UNITED VMS 8.0
Rel 8.0.0.6100
Rel 8.0.0.6100
Latitude / Horizon / Meridian
Table of Contents

1. Introduction ......................................................... 7
2. Product Features ................................................. 8
  2.1 Cyber Security Improvements ................................ 8
    2.1.1 TLS for Edge Devices – Policy .......................... 8
    2.1.2 Applying TLS in Latitude Systems ..................... 8
    2.1.3 System Security Tab ....................................... 9
    2.1.4 Edge Security Tab ........................................ 11
    2.1.5 Edge Device Password Management .................... 12
  2.2 Administration of Users Across Multiple Systems ........ 12
    2.2.1 Global Admin Server ..................................... 13
    2.2.2 Admin Center Entity ...................................... 13
    2.2.3 Global User Group and User Field ..................... 14
    2.2.4 Synchronization ......................................... 15
  2.3 Installation and Upgrade Improvements ..................... 16
    2.3.1 Backward Compatibility ................................ 16
    2.3.2 Improved Installation Process ......................... 16
  2.4 EZ Client Enhancements ...................................... 17
    2.4.1 Support H.264 Streaming in EZ Client Web Interface 17
    2.4.2 Toggling Playback in Multi-Sensor Cameras in EZ Client Web Interface .... 18
    2.4.3 Improved Snapshot Support in EZ Web Client ........ 19
  2.5 Simplified Discovery Process ................................. 20
    2.5.1 Simplified Camera Attachment during Discovery in Latitude .......... 20
    2.5.2 Unified Discovery Process for FLIR Devices ........... 20
    2.5.3 Manual Discovery ...................................... 20
    2.5.4 Horizon/Meridian Manual Discovery .................. 22
    2.5.5 Automatic Discovery ................................... 22
    2.5.6 Horizon/Meridian Automatic Discovery ............... 23
    2.5.7 Improved Discovery Error Messages .................... 24
  2.6 Analytics Setup of FC-ID Cameras in Admin Center ........ 25
    2.6.1 Analytics Setup for FC Series ID in Latitude ........ 26
    2.6.2 Analytics Setup for FC Series ID in Horizon/Meridian ........ 27
  2.7 Support PTZ Tracking on Latitude with Digital Encoders and IP PTZ cameras 27
  2.8 New Licensing Server ....................................... 28
  2.9 Other Enhancements ......................................... 30
    2.9.1 Control of Adaptive Streaming .......................... 30
**List of Figures**

<table>
<thead>
<tr>
<th>Table/figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Current Support for TLS, by Discovery method</td>
<td>8</td>
</tr>
<tr>
<td>Figure 1</td>
<td>System Security Tab - Security Policy</td>
<td>9</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Edge Device Security Policy Options</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Add/Remove TLS Certificate</td>
<td>10</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Replace/Remove TLS Certificate</td>
<td>10</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Password Rules</td>
<td>10</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Password Change Policy</td>
<td>11</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Edge Security Tab - Device Table</td>
<td>11</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Global Admin Center Architecture</td>
<td>13</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Add Global Admin Server</td>
<td>14</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Global Admin Server - Physical View</td>
<td>14</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Global indicator for User Definition</td>
<td>15</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Sync Intervals</td>
<td>15</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Last Sync Time</td>
<td>15</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Sync Now</td>
<td>15</td>
</tr>
<tr>
<td>Figure 15</td>
<td>New settings entry to choose between MJPEG and H.264</td>
<td>17</td>
</tr>
<tr>
<td>Figure 16</td>
<td>EZ Web Client playback of visible scene</td>
<td>18</td>
</tr>
<tr>
<td>Figure 17</td>
<td>EZ Web Client playback of thermal scene</td>
<td>18</td>
</tr>
<tr>
<td>Figure 18</td>
<td>EZ Web Client snapshot downloaded</td>
<td>19</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Attaching cameras to Archivers</td>
<td>20</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Manual discovery - auto detect</td>
<td>21</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Latitude Manual discovery - choosing the right plugin</td>
<td>21</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Horizon/Meridian Manual discovery - auto detect</td>
<td>22</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Horizon/Meridian Manual discovery - choosing the right plugin</td>
<td>22</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Latitude automatic discovery - new unified FLIR plugin</td>
<td>22</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Latitude automatic discovery advanced plugin setting</td>
<td>23</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Horizon / Meridian automatic discovery FLIR plugin</td>
<td>23</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Horizon / Meridian automatic discovery advanced plugin setting</td>
<td>24</td>
</tr>
<tr>
<td>Figure 28</td>
<td>Setting up Analytics Rules</td>
<td>26</td>
</tr>
<tr>
<td>Figure 29</td>
<td>Setting the display parameters</td>
<td>26</td>
</tr>
<tr>
<td>Figure 30</td>
<td>Horizon/Meridian Analytics setup tab</td>
<td>27</td>
</tr>
<tr>
<td>Figure 31</td>
<td>PTZ Tracking Example</td>
<td>28</td>
</tr>
<tr>
<td>Figure 32</td>
<td>Activation key in Admin Center V7.0 and lower</td>
<td>30</td>
</tr>
<tr>
<td>Figure 33</td>
<td>Activation key in Horizon/Meridian Systems</td>
<td>30</td>
</tr>
<tr>
<td>Figure 34</td>
<td>New timer entity in system tree</td>
<td>31</td>
</tr>
<tr>
<td>Figure 35</td>
<td>Timer action - arm camera</td>
<td>31</td>
</tr>
<tr>
<td>Figure 36</td>
<td>FLIR PT-Series HD</td>
<td>34</td>
</tr>
<tr>
<td>Figure 37</td>
<td>Picture-in-Picture display of dual-sensor camera (Thermal is Primary)</td>
<td>34</td>
</tr>
<tr>
<td>Figure 38</td>
<td>FLIR Ariel 3MP Corner Camera</td>
<td>35</td>
</tr>
<tr>
<td>Figure 39</td>
<td>FLIR Quasar 4K Fixed Box Camera</td>
<td>36</td>
</tr>
<tr>
<td>Table 2</td>
<td>Supported Microsoft Windows® Operating System</td>
<td>40</td>
</tr>
</tbody>
</table>
1. Introduction

FLIR is proud to release the next major update to the United VMS family. This United VMS 8.0 major release, available for Latitude, Horizon and Meridian, includes significant new features and benefits for our customers. The release meets new industry trends in technology, adds specific features requested by our customer base, and handles known issues from older versions.

The version includes:

- **Improved Cyber Security with edge device integration**
  - Supports secured connections (TLS) between archiver and cameras
  - Camera password policy – allows users to change default password of one or more cameras from the VMS.
  - Apply security policy by blocking unsecured cameras

- **Enhanced Global Administration**
  - Major improvements in administration of multi-system deployments
  - Automatic management of users across multiple directories
  - Supports central administration of multiple systems in the same organization

- **Installation and upgrade improvements**
  - Backward compatibility- New architecture eases upgrades and allows client & server updates without interruptions to live viewing
  - Improved automation of installation and updates, for greater efficiency and reliability

- **Improved video quality and network bandwidth of EZ Client**
  - Supports H.264 for Proxy with EZ Client web interface functionality

- **Simplified discovery process**
  - Intuitively assign cameras to Archivers upon discovery
  - Provides unified plugin for all FLIR cameras

- **Analytic setup of FC-ID from Admin Center**
  - Configure FC-ID analytic rules directly from the VMS. There is no need to open the camera web page anymore.

- **Enhanced License Management**
  - New Licensing Server provides flexibility & security for integrators & end-users
  - More flexible & robust administration of licenses

- **Performance Upgrades, improved Robustness and Bug Fixes**
  - Improved handling of video streams on Client machines
  - Better user control over Event handling
  - Elimination of known memory problems after long system uptime sessions
  - Improvements in ONVIF implementation

- **Additional Edge Devices**
  - Several new FLIR and OEM device integrations
2. Product Features

2.1 Cyber Security Improvements

Users are strongly encouraged to take active steps to raise the level of security in their systems. In this release, FLIR has added the ability to secure control communications with edge devices. The release also provides tools for the user to change passwords on edge devices so that manufacturers’ default password are no longer used. These steps will help to close vulnerabilities that might arise if these communications are compromised, which is a particular problem for all systems using components from multiple sources.

Note: In this version TLS support, has been implemented for Latitude only. Horizon and Meridian will support TLS in the future.

2.1.1 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.

Table 1 - Current Support for TLS, by Discovery method

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Discovery method</th>
<th>TLS support</th>
<th>Indication of non-default 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 plugin</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 is supported for: Quasar Gen II cameras, Ariel Gen II cameras and ioi HD cameras. Generation of the TLS certificate should be via the camera web page.
** Changing password is supported for: FLIR thermal 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.

2.1.2 Applying TLS in Latitude Systems

In Latitude, Cyber Security features are now organized in two tabs, allowing users to conveniently set system security policy and manage connections and passwords:

- **System Security Tab** - Sets connection and password policy for edge devices and web clients
- **Edge Security Tab** - Manages edge device connections and password status directly
2.1.3 System Security Tab

The Security Tab, allowing the user to set security policy, has four panels:

![System Security Tab](image)

2.1.3.1 Edge Security Settings

This version adds support for secured connection between cameras and archivers using Transport Layer Security (TLS) for control information (only). The VMS now supports encrypting the control information between Archiver and camera over HTTPS protocol. The user can choose whether to enforce secured connection to all edge devices by blocking unsecured connection. The user can also choose whether to enforce using a trusted certificate.

Three checkboxes allow the user to set security policy for edge devices.

![Edge Device Security Policy Options](image)

**NOTE: Before enabling 'Use secured edge connections'**

Certificates must be loaded in the cameras BEFORE enabling this option. The camera web page should be used to upload certificates or generate self-signed certificates.

Some cameras have an Enable/disable SSL option, which needs to be enabled (e.g. Ariel Gen 2)
2.1.3.2 Web Security

The panel allowing the user to set up and use a TLS certificate for encrypting connections between the system and Web Clients has been moved to this Tab.

Figure 3 - Add/Remove TLS Certificate

Figure 4 - Replace/Remove TLS Certificate

2.1.3.3 User Password Rules

The panel allowing the user to set rules for acceptable password values has been moved to this page.

Figure 5 - Password Rules
2.1.3.4 User Password Change

This panel allows the user to permit or prevent operators changing device passwords.

![Figure 6 - Password Change Policy](image)

2.1.4 Edge Security Tab

The Edge Security Tab presents a table of the edge device connections, showing their security status, and allowing the user to carry out Security actions on individual devices or on groups of devices that support similar actions.

![Figure 7 - Edge Security Tab - Device Table](image)

**NOTE: Before choosing 'Set Security Mode'**

Certificates must be loaded in the cameras BEFORE setting this option. The camera web page should be used to upload certificates or generate self-signed certificates.

Some cameras have an Enable/disable SSL option, which needs to be enabled (e.g. Ariel Gen 2)
The table displays the following:

- The device name
- Whether the device connection to the archiver is secured or not
- If secured, the expiration date of its certificate
- Whether 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 set 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.

A warning message is shown whenever the system includes Quasar Gen Ii and/or IOI-HD units:

![Warning](image)

### 2.1.5 Edge Device Password Management

The following new capabilities have been added to the management of edge devices’ passwords:

- Use Edge security page to change camera password
- Show cameras that still use manufacturer's default password (Not available on cameras discovered with the ONVIF plugin)
- Encrypt camera password in the Directory DB

**Notes:**

1. Changing password is supported for: FLIR core cameras (Thermal cameras, and visible with VMSLib), Quasar Gen I cameras, Ariel cameras, and for units discovered via ONVIF.

2. Default password indication is enabled on all proprietary plugins. It is not available if discovering via ONVIF.

**Limitation:** In this version changing password is not supported for Quasar Gen II and ioi HD cameras.

### 2.2 Administration of Users Across Multiple Systems

In this version we are introducing FLIR’s Global Admin Server, a new server which can be added to Latitude systems. The Global Admin Server is not available with Horizon and Meridian. The Global Admin Feature allows user credentials of selected Users and User Groups to be shared and managed across all of the organization’s systems. This allows maintainability of users across many systems.

Global Admin Server requires an additional license to be added to the Directory.

The benefits of Global Admin Feature include:

- Centralized server entity for user and user group management
- Reduced time previously needed to log into multiple system for administration
- Encourages system growth and deployment

### 2.2.1 Global Admin Server

The Global Admin Server is a central server application that runs on a system which is accessible to all the participating Latitude systems. Each participating system defines the Global Admin Server, its IP address and the frequency for synchronization to it.

![Global Admin Center Architecture](image)

**Figure 8 - Global Admin Center Architecture**

### 2.2.2 Admin Center Entity

The Global Admin Server entity may be added to the Admin Center Physical view.
In the Admin Center, using the Physical View, right-click on the System icon to open the Context menu, and select Add Global Admin Server.

This field allows the configuration of the Global Admin Server including the entity name, network address, username and password and synchronization interval (see section 2.5.3 Synchronization for more information).

**Note**: The default username/password is “admin/[no password]”.

### 2.2.3 Global User Group and User Field

The definition screens for User Groups and for Users exists in Admin Center under Users and Groups on the left hand side. These sections now contain a checkbox allowing the User group or User to be defined as Global.
2.2.4 Synchronization

Once a User or User Group is defined as Global their Login Credentials and Privileges are automatically uploaded to the Global Admin Server.

Each participating Latitude system will receive new and updated user information, which was uploaded to the Global Admin Server from other systems, at the time of synchronization.

Synchronization takes place one of two ways:

- **Synchronization by Intervals**

  Synchronization times can be set within the Admin Center entity to allow for automatic synchronization between each individual Latitude system and the Global Admin Server.

  ![Figure 12 - Sync Intervals](image)

  Last successful synchronization: 1/8/2016 10:39:20 AM

  ![Figure 13 - Last Sync Time](image)

  The last synchronization time is displayed beneath the interval selection.

- **Manual Synchronization**

  Synchronization of each system can also be done manually from that systems Admin Center. In order to do so, right-click the Global Admin Server entity in physical view and click Synchronize Now and the system will automatically synchronize with the Global Admin Server.

  ![Figure 14 - Sync Now](image)

**Note:** When information is saved to the Global Admin Server from any participating Latitude system, it will over-write any existing saved data. Therefore, whichever system last updated and saved information to an existing user, will take priority. The most recently saved information will be the only changes pushed to other systems during the synchronization process.

**Best Practice:** Users should perform manual synchronization before doing operations on global entities.

**Important information** – the Global Admin Server has a separate installation and may require a separate/dedicated server to run on. This is a licensed feature.
Global Admin Server Known issues

- In some scenarios, error messages regarding operations on global entities are duplicated.
- It is not possible to set user group as global through the wizard. Possible workaround is to set the user group as global via its general page after creation.
- Global Server’s ‘Test connection’ button will only work when using an empty password. If the default password was modified, a possible workaround is to type the correct password before testing the connection.
- The Global Admin Server should be restarted after installation.
- Users who had Global Admin Server in their system before this release will need to get new licenses that include the Global Admin feature.

Limitations

- Global Admin Server uses port 80; Any other software which uses this port shouldn’t be used on Global Admin Server’s machine.
- Global users should have a unique name within the system; In Global Admin Server, existence of a local user with identical login name to a global user will prevent the import of the global group into the local system and may cause further synchronization issues.

2.3 Installation and Upgrade Improvements

2.3.1 Backward Compatibility

In this version we are introducing necessary changes in our infrastructure to allow future versions to be backward compatible with all software updates within a major version. In addition, the system will support compatibility with one major version backwards; it will allow:

- Clients applications to connect to servers of a different version up to one major version backwards.
- Archivers and other servers should connect to directory server up to one major version backwards.

The main benefit of this feature is to allow customer to upgrade their system in future versions in portions without interrupting live, playback and recording capabilities (excluding the time required to upgrade each server specifically).

Note: Backward compatibility is available starting version 8.0 and onwards. For clarification, version 8.0 is not compatible with version 7.0.

Note: There may be breaking changes in the future which will mean that backward compatibility is not maintained; in this scenario the situation will be the same as today where all servers need to be upgraded to the same version.

2.3.2 Improved Installation Process

In Version 8.0 we have corrected many installation issues in the major install process. The process now checks for many potential errors before starting to extract the installation files, saving time and hard-disk space.

The following fixes were introduced:

- The self-extractor of the software now checks that there is enough space for installation prior to extracting the software. The installer checks that there is a minimum of 20GB available space on C:\ drive.
The “installation cache folder” was moved from: C:\Windows\Downloaded Installations to a new location in program data: C:\ProgramData\FLIR\VMSInstallCache
The self-extractor now checks if the cache folder of previous version is available. If the folder is missing, installation cannot proceed and the self-extractor will abort before the extraction. An error message notifying the user of the issue is displayed advising the user to contact FLIR support.
A message was added notifying the user that the “installation cache folder” should not be deleted
If the user starts the self-extractor a second time the self-extractor will re-use the same folder and will not self-extract to a different location as in the past.
A fresh installation will check for previous installations and any old cache folders. If any old cache folders or old installations are found the installer deletes them.
When uninstalling, the installer ensures that no files are left over from the installation. Any locked files will be marked for deletion and will be deleted after next computer reboot. Note: this happens behind the scenes without notifying the user.
If a different flavor of United VMS is already installed the self-extractor aborts before starting to extract files.

2.4 EZ Client Enhancements

2.4.1 Support H.264 Streaming in EZ Client Web Interface

Video streaming in H.264 is now supported by EZ Client, which enables improved video quality and network bandwidth. While streaming H.264, the transcoder is used as a proxy.

The user can choose to use H.264 or transcoded MJPEG streams. A new setting entry was added to switch between H.264 and MJPEG streaming. The user’s choice will be saved in user’s Cookies on his workstation so that he can change it only once.

The default setting depends on his browser – in Chrome the default will be H.264, in Internet Explorer and Edge browsers the default will be MJPEG.

```
Figure 15 - New settings entry to choose between MJPEG and H.264
```

H.264 streaming is supported with the following browsers:

- Chrome 54 and higher on Windows OS, MAC OS and Android tablets. **Chrome is the recommended browser for EZ Client.**
- Microsoft Internet Explorer 11 or higher, and Edge browser 25 or higher.
- Opera 43 or higher (Windows OS)

For all other browsers, EZ Client supports MJPEG transcoded stream

**Note:** In the following scenarios, EZ Client video will still be transcoded to MJPEG:

- Video with analytics OSD
Product Features

- Video that was not originally H.264 compression
- Video with privacy masking
- Browsers which do not support MSC and H.264 or when codecs are missing
- Live from PTZ camera in Edge and IE
- Resolution higher than 1080p in Edge and IE
- Midas and Panasonic cameras
- Resolution above HD 1080p in Windows 7

Known issues:

- Client performance might decrease, especially on weak workstations or tablet and high resolution streams. This is due to the client being responsible for decoding the H.264 stream.
- Latencies observed (in Opera and Chrome) are usually in the range of 300-400ms but can be below 150ms in certain cases.
- At high resolution and some cases H.264 does not play well on IE and Edge (e.g. high resolution, in Win8.1 and 10); if user experience is not good, the user should switch to MJPEG (using the switch available in the settings). This needs to be done once. The system will then keep the setting.

2.4.2 Toggling Playback in Multi-Sensor Cameras in EZ Client Web Interface

EZ Web Client now supports toggling of playback as well as live video between thermal and visual scenes on multi-sensor cameras.

![Figure 16 EZ Web Client playback of visible scene](image16)

![Figure 17 EZ Web Client playback of thermal scene](image17)

Applies to: all multi sensor cameras (PT-Series, A310-PT Series, D-Series, PT-HD-Series)

Firmware version: all.
2.4.3 Improved Snapshot Support in EZ Web Client

Snapshots are now automatically saved in the Downloads folder on the user’s workstation. There is no need to manually download the snapshot.

For an H.264 stream, the snapshot is taken in the workstation running the EZ Client. This makes the snapshot immediate and more accurate. This change means that there is no need to go to the notification center to download the snapshot, it is downloaded automatically and immediately.

Note: for video transcoded to MJPEG the snapshot is still captured on the server, but is immediately downloaded to the Downloads folder on the user’s workstation.

Figure 18  EZ Web Client snapshot downloaded
2.5 Simplified Discovery Process

2.5.1 Simplified Camera Attachment during Discovery in Latitude

We have improved the interface for attaching cameras to Archivers during the Discovery process in Latitude. You can easily attach cameras to Archivers, and see clearly the cameras and the Archivers to which they are attached.

![Figure 19 Attaching cameras to Archivers](image)

2.5.2 Unified Discovery Process for FLIR Devices

In United VMS 8.0, all supported FLIR edge devices are discovered through a single Discovery plug-in. This unifies all FLIR cameras under one plugin: Thermal cameras, Quasar, Ariel, etc. This greatly simplifies the user’s setup process. The user is not required to know the exact model of when discovering FLIR cameras. The FLIR plugin automatically determines the type of camera and applies the correct discovery parameters. The unified plugin also allows the user to use the edge devices’ password from a single entry which applies to all FLIR cameras discovered at that time.

Using default parameters, the unified plugin will automatically detect each type of camera and assign the correct parameters for that type. By selecting individual product types, it also allows the advanced user to use different parameters for each plugin if required.

2.5.3 Manual Discovery

This release includes a new drop-down list for the Product Type. It is now possible to select the Auto Detect option to automatically detect the device. The user only needs to set the IP address of the unit and let the system auto-detect the type of camera. One can change the username and password for the unit if they are not the default values. The user can still access the separate camera plugins.
Figure 20  Manual discovery - auto detect

Figure 21  Latitude Manual discovery - choosing the right plugin
2.5.4 Horizon/Meridian Manual Discovery

The same was applied to Horizon/Meridian manual discovery, below are screenshots of the Horizon/Meridian manual discovery.

![Horizon/Meridian Manual discovery - auto detect](image1)

![Horizon/Meridian Manual discovery - choosing the right plugin](image2)

2.5.5 Automatic Discovery

In Automatic discovery, it is now possible to select the FLIR plugin which supports all the individual plugins. The system still applies the individual settings for each plugin, and the user can change default settings if needed.

![Latitude automatic discovery - new unified FLIR plugin](image3)
The same was applied to Horizon/Meridian automatic discovery, below are screenshots of the Horizon/Meridian automatic discovery.

Figure 25  Latitude automatic discovery advanced plugin setting

Figure 26  Horizon / Meridian automatic discovery FLIR plugin

2.5.6 Horizon/Meridian Automatic Discovery

The same was applied to Horizon/Meridian automatic discovery, below are screenshots of the Horizon/Meridian automatic discovery.
Limitations

Legacy Pro Line, Legacy Pro Line A and TRK4000D cannot be discovered while adding unit manually and product type is 'Auto Detect'. For edge devices of these types the user will need to choose the correct plugin (Legacy Pro Line, Legacy Pro Line A and IOI respectively).

2.5.7 Improved Discovery Error Messages

As part of ongoing improvements to robustness and supportability we have made improvements to the error messages in manual discovery.

The following new error messages -

- For unit previously discovered in the system –
  "Unit already been discovered in the system. Please review the Discovery page for unattached units or check for it on your existing Archivers."

- When trying to discover a unit with the wrong plugin -
  "Unit does not match the selected product type, please try a different product type. In case FLIR unit is to be discovered, auto-detection option could be used."

- When the unit MAC address cannot be read -
  "Unable to retrieve the unit’s MAC address, Please check that the unit’s firmware is up to date or contact the manufacturer."

- When the unit FW cannot be read -
  "Unable to retrieve the unit’s firmware version, Please check that the unit’s firmware is up to date or contact the manufacturer."

- When it is impossible to establish the model number of the unit
  "Unable to retrieve the unit’s model number, Please check that the unit’s firmware is up to date or contact the manufacturer."
2.6 Analytics Setup of FC-ID Cameras in Admin Center

Latitude, Horizon and Meridian VMS systems now allow the user to fully configure Analytics rules for FC-Series ID Thermal cameras through the Admin Center.

The user can choose whether to configure the analytics via his Admin Center or through the web. When the “Use configuration from” switch is set to “System” analytics are copied from the camera to the VMS and all settings are accessible via Admin Center, any setup done via the camera web will be overridden by the VMS. When the switch is set to “Web”, the screen will show the current settings that were created using the camera’s web interface and they cannot be edited and hence shown as disabled.

Analytic setup in System mode is recommended, it introduces a new and intuitive user experience to configure the analytic setup with FC Series ID, and saves the user the need to access the camera web page.

In addition, it enables users to preserve all settings of the camera in the VMS, therefore providing a settings backup which can be used in case of camera replacement.

- On authentication error –
  
  "The username and/or password is invalid, Please correct and try again. "

- When the hostname cannot be resolved –
  
  "Unable to resolve the hostname that was entered, Please check the hostname and confirm with your IT department that the configured DNS servers are reachable. Alternatively use an actual IP address instead."

- When there is a network connectivity issue or unknown network –
  
  "Unit address is not in any of the networks to which this Archiver is connected, Please attach the relevant network to this Archiver and try again. "

2.6 Analytics Setup of FC-ID Cameras in Admin Center

Latitude, Horizon and Meridian VMS systems now allow the user to fully configure Analytics rules for FC-Series ID Thermal cameras through the Admin Center.

The user can choose whether to configure the analytics via his Admin Center or through the web. When the “Use configuration from” switch is set to “System” analytics are copied from the camera to the VMS and all settings are accessible via Admin Center, any setup done via the camera web will be overridden by the VMS. When the switch is set to “Web”, the screen will show the current settings that were created using the camera’s web interface and they cannot be edited and hence shown as disabled.

Analytic setup in System mode is recommended, it introduces a new and intuitive user experience to configure the analytic setup with FC Series ID, and saves the user the need to access the camera web page.

In addition, it enables users to preserve all settings of the camera in the VMS, therefore providing a settings backup which can be used in case of camera replacement.
2.6.1 Analytics Setup for FC Series ID in Latitude

The Admin Center user uses a simple mouse gestures to draw outlines for the camera’s multiple Intrusion Zones and virtual Tripwires, and can also indicate Masking areas, as part of the camera setup process.

Intrusion Zone and Tripwire definitions can include details such as classification of object types, and movement direction, allowing the camera to respond to specific stimuli, and display accordingly.

**Figure 28 - Setting up Analytics Rules**

**Figure 29 - Setting the display parameters**

**Applies to:** all FC-Series ID cameras

**Firmware version:** V2.03.P01 and up
2.6.2 Analytics Setup for FC Series ID in Horizon/Meridian

Horizon and Meridian VMS systems support the same setup capabilities, meaning that even users of the smaller VMS solutions have access to these capabilities.

![Horizon/Meridian Analytics setup tab](image)

**Figure 30 - Horizon/Meridian Analytics setup tab**

2.7 Support PTZ Tracking on Latitude with Digital Encoders and IP PTZ cameras

PTZ Tracking provides support for linking an analytics encoder and a PTZ camera. The user sets up customized rules and criteria on the encoder to define a perimeter and what to detect. The encoder is then associated with a PTZ camera (‘binding’).

In United VMS 8.0, the Latitude system supports this capability using digital encoders and high-performance IP PTZ cameras. When the encoder is armed, if a moving object is detected, the
encoder controls and moves the PTZ camera to autonomously track and zoom in on the detected object.

This version fully supports PTZ Tracking on FLIR PT-Series, PT Series HD, and A310pt cameras. PTZ Tracking requires binding the cameras in FLIR Latitude with a TRK encoder.

**TRK Firmware version:** 2.2.0.13 and up.

### 2.8 New Licensing Server

A new licensing server is introduced with this version. The licensing server is a third-party software product by the name of Software Potential.

The process of generating and installing a new license, as well as updating a license is like the current process with some changes described below.

1. Upon first login to Admin Center the **Install license** screen opens
2. Paste the activation key received from FLIR operations in the **Activation Key** box (as marked in the figure below) then press **Generate Request**
3. Save the request file on your workstation
4. Go to the licensing customer portal ([https://srv.softwarepotential.com/Portal](https://srv.softwarepotential.com/Portal)), to the **New Device** section and browse to the request file.
5. Once the request file is present an **Activate** button appears. Click on it and follow the instructions to save the license file on your workstation.
6. From the license installation window browse to the file location and open the license file
7. Click the **Install License** button to install the license
Important note: When upgrading an existing system to version 8.0 a new license is needed. A version 8.0 license can be obtained from FLIR operations using the system’s activation key. Please ensure that you have obtained a V8.0 license or have the system’s activation key before upgrading.
Having the old Activation Key available is useful. The existing activation key can be obtained from Admin Center 7.0 dashboard, or from the Systems Settings page.

On Horizon/Meridian systems, the current Activation Key can be found on the Settings Page / Licensing Tab

Note: The new licensing server is used for systems of version 8.0 and higher. United VMS versions being upgraded but still below 8.0 (i.e. from 6.3 to 7.0) will still operate off the previous licensing server.

2.9 Other Enhancements

2.9.1 Control of Adaptive Streaming

Each Archiver can now have a general setting that switches Adaptive Streaming on or off. Previously it was possible to switch Adaptive Streaming on and off for each camera from Control Center. This now adds the ability to the Administrator on-site to disable Adaptive Streaming on all the cameras of an Archiver together.

The default behavior is to use adaptive streaming.

To implement this functionality please contact FLIR Support.
2.9.2 Active Directory Performance Improvements

The implementation of Active Directory (AD) in the VMS was affected by the number of users defined in AD and caused slow loading for organizations with a large numbers of users. In this version this process has been improved, resulting in significantly reduced processing time for importing Users and User Groups.

The implementation of Active Directory (AD) in the VMS was affected by the number of users defined in AD and caused slow loading for organizations with a large numbers of users. In this version this process has been improved, resulting in significantly reduced processing time for importing Users and User Groups.

2.9.3 Add Arm/Disarm by Schedule

Latitude VMS now supports a new action of Arm/Disarm and a new timer that supports Arm/Disarm of cameras. The timer includes a timer elapsed event which can trigger an action to Arm/Disarm the camera.

![New timer entity in system tree](image1)

![Timer action - arm camera](image2)

**Figure 36** New timer entity in system tree

**Figure 37** Timer action - arm camera

**Applies to:** all ioi devices, FC-Series ID (from firmware version V2.03).
Firmware version: all

Important note: when upgrading to 8.0, if the system was already installed with the Triggered Events Plugin in version 7.0 the plugin should be uninstalled before the upgrade.

2.9.4 Rebranding FLIR Cloud Services
We have rebranded the cloud services and changed the URL to: http://vmscloudservices.flir.com/
There should be no service interruption or changes in user experience.

2.9.5 SDK Improvements
The FLIR Enterprise mobile app was improved by adding RTSP API which enables it to get H.264 streams via RTSP. This is currently developed only for the mobile middleware.
This will enable mobile app to get H.264 live video stream.

2.9.6 DNA Support
This version will include the new DNA version 2.1.3.15. This DNA version introduces support to all new cameras listed in this Release Notes.
The exact details can be found in the DNA Release Notes.
3. Robustness

The following improvements have been made:

3.1 Improved support of Video Streams on Client machines

In earlier versions, users on Client machines would often see messages indicating video failure, even though they may not experience any disturbances in the video stream. This is due to the default short rendering timeout. In this and future versions, the video rendering timeout can be adjusted, which reduces instances of this problem.

The default value is 5 seconds.

To implement this functionality please contact FLIR Support.

3.2 Improved Event Passing in EDB

The system allows filters to be set up between EDBs, in order to reduce the number of events passed across the system. To assist users who wish to get all events passed without filtering, the system now allows event filtering between EDBs to be turned on or off via EDB’s config file.

By default the event filter is on so that only relevant events are passed between EDBs.

To implement this functionality please contact FLIR Support.

3.3 Memory Leaks – ART and Transcoder

Two ART memory leak problems have been identified and resolved:
- Sony Gen1 camera
- Adaptive streaming

A memory leak in the Transcoder that only arose after several weeks in use was traced and corrected.

3.4 Continuous Uptime leading to Overflow Exception

Systems that were continuously in operation for over 50 days were exhibiting an Overflow Exception. This has been corrected.

3.5 Issues with Unclosed CCTV Keyboard

Users with CCTV keyboards instances that were not closed after use were experiencing a gradual drop in Frame Rates. This has been corrected.

3.6 Improved ONVIF implementation

In order for the Pelco D6230 to be discovered, a small change to the system was required.
4. Edge Device Enhancements

In this version, we have added support for new FLIR edge devices

4.1 New FLIR PT-Series HD Multi-Sensor Camera

Support was added for the new FLIR PT-Series HD camera.

The FLIR PT-Series HD is a dual-sensor, pan-tilt camera system that provides superior, long-range perimeter intrusion detection and integrates with FLIR United VMS.

![FLIR PT-Series HD](image)

Figure 38: FLIR PT-Series HD

Integration of this camera in United VMS is designed to take advantage of the camera's capabilities, while simultaneously providing the operator with an interface that is easy to use.

The camera is shown in the navigation tree as two separate scenes – one for the visible spectrum camera, and one for the thermal spectrum camera. The scene being used for the primary view is highlighted, and the user can toggle views by clicking on the navigation tree entry.

The display in the Viewing Window provides a picture-in-picture view. The user can also toggle between cameras by clicking in the secondary picture.

The size and position of the secondary is variable – the user can click and drag to change these.

![Picture-in-Picture display of dual-sensor camera (Thermal is Primary)](image)

Figure 39 - Picture-in-Picture display of dual-sensor camera (Thermal is Primary)
4.2 New FLIR Ariel Corner Camera

Support was added for the Ariel 3MP Corner Camera, which features a specialized lens providing ceiling-to-floor and wall-to-wall field of view, packaged with a unique corner-shape form factor.

![FLIR Ariel 3MP Corner Camera](image)

*Figure 40: FLIR Ariel 3MP Corner Camera*

![Corner Camera View](image)

*Figure 41 - Corner Camera View*
4.3 New FLIR Quasar Fixed Box Camera

Support was added for the new FLIR Quasar 4K fixed box multiple-resolution camera. The Fix Box camera can be switched from 4K daytime mode to 1080p lowlight / nighttime mode for optimum performance in high-traffic areas.

![FLIR Quasar 4K Fixed Box Camera]

Figure 42: FLIR Quasar 4K Fixed Box Camera

4.4 Support Analytics Events via ONVIF

In this version we have enhanced our ONVIF support by adding support of analytics events via ONVIF.

The new events supported are:

- Tripwire detection
- Intrusion detection

This was added to the already-supported Motion detection and Tamper (scene change and lens cover) events.

**Note:** ONVIF protocol support for these events can vary between camera manufacturers. The fix is relevant only to cameras that expose the following ONVIF event topics:

"tns1:RuleEngine/LineDetector/Crossed" and "tns1:RuleEngine/FieldDetector/ObjectsInside"

4.5 New Supported 3rd Party Cameras

This version supports the following edge devices (for full list of supported cameras, please check the Supported Edge Device List):

- FLIR N247B3
- AXIS Q6055
- AXIS Q3708 with single channel license
- AXIS P3707 with single channel license
# 5. Fixed Issues

All the cases described in the table below were fixed in V8.0.

<table>
<thead>
<tr>
<th>CR ID</th>
<th>Description</th>
<th>Support Ticket</th>
</tr>
</thead>
<tbody>
<tr>
<td>43696</td>
<td>Discovery windows is closed even when set in the option to stay open after discovery/add-on was fixed</td>
<td>73706</td>
</tr>
<tr>
<td>43498</td>
<td>Archiver stop functioning (cameras become inaccessible) due to a memory leak, and only a reboot of the Archiver resolves the issue</td>
<td>71773</td>
</tr>
<tr>
<td>43647</td>
<td>Fixed issue where ONVIF based FLIR fixed cameras with digital PTZ were discovered as regular PTZ cameras even though they did not have a PTZ engine.</td>
<td></td>
</tr>
<tr>
<td>43208</td>
<td>Fix for jerky video with Bosch cameras</td>
<td>70969</td>
</tr>
<tr>
<td>41316</td>
<td>Unable to get video via transcoder when connected from gateway on the same server machine (also from web client from remote machine).</td>
<td>66166</td>
</tr>
<tr>
<td>40694</td>
<td>Export failure when trying to export from dvt file</td>
<td>64722</td>
</tr>
<tr>
<td>42280</td>
<td>Latitude installer allows multiple process to run simultaneously issue was fixed. Now only a single instance of Latitude installer can run.</td>
<td>67798</td>
</tr>
<tr>
<td>42058</td>
<td>Application error in Admin Center relating to Moxa output pin setup was fixed.</td>
<td>67356</td>
</tr>
<tr>
<td>43692</td>
<td>GIS map is not functioning after EOL for the &quot;Google Earth&quot;</td>
<td>73282</td>
</tr>
<tr>
<td>43366</td>
<td>In a silent install popup messages appear</td>
<td>71843</td>
</tr>
<tr>
<td>42974</td>
<td>Fixed initialization issues for Pelco Spectra IP D6220</td>
<td>70109</td>
</tr>
<tr>
<td>42806</td>
<td>Add &quot;Force adding description on clear&quot; to the content covered by copy configuration.</td>
<td>69779</td>
</tr>
<tr>
<td>42771</td>
<td>Map Script – Correcting problem with the value of the Property 'ChangeAllToUnfocus' (was null or undefined)</td>
<td>68904</td>
</tr>
<tr>
<td>42608</td>
<td>Fixed issue where it was not possible to save preset on Sony SNC-WR632 firmware 2.5 / 2.6.6</td>
<td>69093</td>
</tr>
<tr>
<td>42576</td>
<td>Video Hiccup while viewing Hikvision and Grunding cameras from Latitude</td>
<td>68525</td>
</tr>
<tr>
<td>42541</td>
<td>Fixed issue where non-admin users received an error message while login to Control Center after upgrade</td>
<td>68329</td>
</tr>
<tr>
<td>41307</td>
<td>Fix time formatting on email received due to the action &quot;send email&quot;</td>
<td>66215</td>
</tr>
<tr>
<td>41127</td>
<td>Cannot Discover DVtel 9420 camera</td>
<td>65938</td>
</tr>
<tr>
<td>41156</td>
<td>Unable to discover American Dynamics (Illustra 625) camera via ONVIF</td>
<td>65695</td>
</tr>
<tr>
<td>40992</td>
<td>Adding Second stream of Pelco TXB-N causes unit to become inaccessible</td>
<td>65008</td>
</tr>
<tr>
<td>40704</td>
<td>Unit Online set with scheduled recording profile is not recording.</td>
<td>65216</td>
</tr>
<tr>
<td>40668</td>
<td>Incident Creation is not working for a scene with linked audio out</td>
<td>63477</td>
</tr>
<tr>
<td>40660</td>
<td>No PTZ control on remote client using Keyboard</td>
<td>62540</td>
</tr>
<tr>
<td>CR ID</td>
<td>Description</td>
<td>Support Ticket</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>40624</td>
<td>Cannot discover the Sony RZ30</td>
<td>64897</td>
</tr>
<tr>
<td>43355</td>
<td>QCCconfig.dll detected as virus by anti-virus software</td>
<td></td>
</tr>
<tr>
<td>43682</td>
<td>QCC does not work on Windows 10</td>
<td>72715</td>
</tr>
<tr>
<td>44423</td>
<td>Fixed issue with request file for V8.0 license is not generated</td>
<td></td>
</tr>
<tr>
<td>44366</td>
<td>Fixed issue where the video stream is restarting upon a change in external workspace.</td>
<td>74930</td>
</tr>
<tr>
<td>35387</td>
<td>Fixed issue where high quality video from Sony Gen 5 and Gen 6 cameras is not stable</td>
<td></td>
</tr>
<tr>
<td>44387</td>
<td>Fixed issue of frequent video failure messages on client machine</td>
<td>73778</td>
</tr>
<tr>
<td>44425</td>
<td>Fixed memory leak (in ART) with Sony Gen1 camera</td>
<td></td>
</tr>
<tr>
<td>44455</td>
<td>Fixed issue of overflow exception after the OS having uptime of 50 days</td>
<td>74418</td>
</tr>
<tr>
<td>44198</td>
<td>Fixed issues that layouts opened using a CCTV keyboard are not closed and eventually causing frame rate to drop</td>
<td>74684</td>
</tr>
<tr>
<td>44462</td>
<td>Fixed issue where Pelco D6230 was not discovered using ONVIF</td>
<td></td>
</tr>
<tr>
<td>43424</td>
<td>Fixed Transcoder memory leak</td>
<td>71618</td>
</tr>
<tr>
<td>44479</td>
<td>Fixed issue where events were not passed between EDBs.</td>
<td>75264</td>
</tr>
<tr>
<td>44478</td>
<td>Fixed memory leak in ART in adaptive streaming.</td>
<td>72962</td>
</tr>
<tr>
<td></td>
<td></td>
<td>75353</td>
</tr>
<tr>
<td></td>
<td></td>
<td>75272</td>
</tr>
<tr>
<td></td>
<td></td>
<td>75327</td>
</tr>
<tr>
<td></td>
<td></td>
<td>75383</td>
</tr>
<tr>
<td>42605</td>
<td>Fixed issue where a standard user cannot login to CC and AC when DVTEL services are running on the same machine</td>
<td>68750</td>
</tr>
<tr>
<td>43889</td>
<td>Transcoder log is being flooded with too many lines of the same warning</td>
<td>75937</td>
</tr>
</tbody>
</table>
# 6. Known Issues

<table>
<thead>
<tr>
<th>CR ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43615</td>
<td>WebClient - Image is frozen for Panasonic models on win7</td>
</tr>
<tr>
<td>43638</td>
<td>FW issue affects analytics setup - Tripwire direction setting is not applied to the camera</td>
</tr>
<tr>
<td>44017</td>
<td>After upgrade from 7.0 Admin Center requires license for each directory on the system, when logging in to Admin Center a message to install license due to an unlicensed FOD will be displayed</td>
</tr>
<tr>
<td>44053</td>
<td>Transcoder – a memory leak may cause the transcoder to crash sometimes, it will restart again but may require the user to choose streams again to view on Web Client</td>
</tr>
<tr>
<td>44090</td>
<td>When there is no primary Directory in the system yet, and the client tries to connect, the login will fail with a message: 'Client version is newer than server....'; this will only be displayed while the server is unlicensed</td>
</tr>
<tr>
<td>44097</td>
<td>Web Client Playback starts over every time the user navigates to a different tab and back to client</td>
</tr>
<tr>
<td>44111</td>
<td>Live streams in high resolution will accumulate a delay, which at some point will cause the stream to restart. In Web Client</td>
</tr>
<tr>
<td>44100</td>
<td>A scene that had privacy mask defined on will always play in MJPEG in the Web Client, even after the mask is removed</td>
</tr>
<tr>
<td>43932</td>
<td>Edge Security – if the unit is rediscovered its security settings will revert back to default</td>
</tr>
<tr>
<td>43869</td>
<td>When licensing a system with Failover Directory, the license cannot be installed on an offline FOD</td>
</tr>
<tr>
<td>44002</td>
<td>FW issue - FC-ID - Automatic calibration isn't successful.</td>
</tr>
<tr>
<td>44004</td>
<td>FW issue - Admin Center - FC-ID - Setting &quot;Masking Area&quot; will not disable intrusion detection in the marked area</td>
</tr>
<tr>
<td>43996</td>
<td>FW issue - FC-ID - Opposed to camera settings (&quot;No Boxes&quot;) when saving a change in VMS two boxes appear for 1 minute</td>
</tr>
<tr>
<td>43990</td>
<td>When upgrading to V8.0 'SkinsPack' windows is displayed for each patch removal</td>
</tr>
<tr>
<td>44317</td>
<td>Cloud services are not available with this version</td>
</tr>
<tr>
<td>44316</td>
<td>SafRun service does not start automatically on Windows 10 after upgrade to Anniversary/Creators</td>
</tr>
<tr>
<td>45017</td>
<td>If a customer had the Time Triggered Events Plugin installed in version 7.0 he needs to uninstall the plugin before upgrading to 8.0.</td>
</tr>
</tbody>
</table>
7. New Installations and Upgrades

7.1 Supported Upgrade Path for 8.0

Direct upgrade to V8.0 is available from the following versions:

- United VMS 7.0.0.57xx
- United VMS 6.4.0.68xx

7.2 Supported Operating Systems

The following operating systems are supported and can be used for running Latitude:

*Table 2 - Supported Microsoft Windows® Operating System*

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 Professional SP1 - 64 bit</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows 8 Pro - 64 bit</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows 8.1 Pro- 64 bit</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Windows 10 Pro – 64 bit – plan to deploy Horizon and Meridian with Win 10</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Server 2008 R2 SP1 - 64 bit</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Server 2012 - 64 bit (Standard and DataCenter editions)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Server 2012 R2 - 64 bit (Standard and DataCenter editions)</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Notes:

1. 32 bit systems are not supported with 8.0
2. In case upgrade is required from non-supported OS, please refer to 8.0 Installation instructions and clarifications document
8. Additional Resources

For more information about the VMS system, visit http://www.flir.com/security/display/?id=73645

9. Windows Updates

Note: The VMS Windows services must be stopped prior to applying Windows updates
Latitude is certified with all the Microsoft Updates available up until April 1, 2017.
Check for the latest Microsoft updates.

10. Disclaimer

By providing this document, FLIR Systems, Inc. is not making any representations regarding the correctness or completeness of its contents.

© FLIR Systems, Inc. 2017. All rights reserved.
Appendix A. Supported Languages

<table>
<thead>
<tr>
<th>Supported use with non-English language</th>
<th>Latitude</th>
<th>Meridian</th>
<th>Horizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>AdminCenter</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ControlCenter</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-English keyboard input</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Latitude:**

1. **OS**
   - It is recommended to install Latitude services on English OS even if using client applications in other languages.
2. **Admin Center**
   - Latitude Admin Center does support various non-English languages. This can be changed in the config file at `<Installation Folder>\AdminCenter under the section "<Localization>"`
3. **ControlCenter**
   - ControlCenter does support non-English languages. This can be changed in the ControlCenter config file at `<Installation Folder>\ControlCenter under the section "<Localization>"`.

**A.1. Horizon/Meridian:**

1. **OS**
   - Horizon and Meridian are appliances that are sold as-is. Therefore, FLIR does not support changing the languages in the OS. There is the potential for it to cause issues. However, you can add a keyboard input for another language and type in that language.
2. **Admin Center**
   - Horizon/Meridian Admin Center has no support for non-English languages. Note: While Admin Center does not support such function, one is able to type in a different language into Admin Center. For example, if one would like to name cameras in a non-English language, this is supported. Please note that right-to-left languages may skew the positioning of certain components (i.e. logical Id).

**A.2. ControlCenter**

- ControlCenter (being a unified application) does support non-English languages and FLIR does support this. This can be changed in the ControlCenter config file at `<Installation Folder>\Control Center under the section "<Localization>"`. 
A.3. Changing the User Interface Language When a System is Already Installed

Latitude AdminCenter and the FLIR Unified ControlCenter supports multiple languages. By activating the desired language, these applications are conveniently displayed in the localized user interface of your choice. The selection of the user language can be done during the installation phase or manually if the system is already installed (see procedure below).

The following languages are supported: English, Hebrew, Spanish, Russian, Italian, Japanese, Chinese, French and Portuguese.

Procedure to manually change the user interface language:

1. Each of the following files needs to be edited:
   i. `<Installation Folder>\AdminCenter\AdminCenter.exe.config`
   ii. `<Installation Folder>\ControlCenter\ControlCenter.exe.config`
   iii. `<Installation Folder>\Directory\Directory.exe.config`

2. Note: In the case where only ControlCenter is being changed, only edit the ControlCenter.exe.config.

3. Open the files using a text editor, such as Notepad or WordPad.

4. Search for the following string: `add key="Language" value="en"

5. Replace the value en with the value of the desired language:

<table>
<thead>
<tr>
<th>Language</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>en</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja</td>
</tr>
<tr>
<td>Hebrew</td>
<td>he</td>
</tr>
<tr>
<td>Chinese</td>
<td>zh-CN</td>
</tr>
<tr>
<td>Spanish</td>
<td>es</td>
</tr>
<tr>
<td>French</td>
<td>fr-FR</td>
</tr>
<tr>
<td>Russian</td>
<td>ru</td>
</tr>
<tr>
<td>Portuguese</td>
<td>pt-BR</td>
</tr>
<tr>
<td>Italian</td>
<td>it-IT</td>
</tr>
</tbody>
</table>

5. Save the files and launch the FLIR application displaying the localized user interface.
Appendix B.

B.1. Installing a new Latitude system

Please follow the pre-requisite instructions from the *Latitude-8.0-Installation-and-Clarifications* before starting this installation.

1. Copy the software installation packages to the local hard drive of the server.
2. Note: Prior to the installation, make sure that the InstConfig.INI file, which should be included in the installation package provided by FLIR, is available in the same directory as the installation executable file.
3. Double click the Latitude_8.0.0.exe file or for operating systems with User Access Control activated, right-click the file and select Run as administrator.
4. If a Microsoft Windows security prompt appears, confirm to run the file by clicking Yes to run it.
5. Wait while the Self Extracting Installation files process runs and Configuring Installer process completes.
6. The installation will present the pre-requisites installation dialog if pre-requisites items are needed to be installed. Click Install to continue.
7. A progress indicator and status shows the progress of the item installations. After installation of the individual requirements, the Latitude 8.0 Installation Wizard Welcome screen appears.

For the initial Latitude 8.0 Installation Wizard screens, do the following:

1. In the Welcome screen, click Next.
   - The License Agreement dialog box appears.
     - Read the license agreement, click I accept the terms in the license agreement, to confirm you agree, and then click Next.
2. A Location screen is shown, indicating the destination directory.
   - Click Next to use the default current destination folder (installation path)
     - or-
     - To change the default, click Change, enter the path in the Folder name field, and click OK.
3. In the Latitude 8.0 Installation Wizard, click Next.
   - The Language Selection dialog box appears.
     - Click Next
     - or-
     - To select a language other than English, click the Language menu and select the language from the available language options and then click Next.
   - The Setup Type dialog box appears. The different installation options are described in the next four sections.

B.2. Upgrade instructions

Upgrading from previous versions is performed using the same installation package as the fresh installation.

The current release supports the following direct upgrade paths:

Upgrade from 6.4 (6.4.0.68) – Requires a new license
Upgrade from 7.0 (7.0.0.57) – Requires a new license
**Important note**: before starting with the upgrade ensure that you have the systems activation key and have obtained a V8.0 license from FLIR operations.

It is important to consult the Latitude-8.0-Installation-and-Clarifications document prior to the upgrade to ensure that all pre-requisites have been fulfilled.

### B.2.1 Upgrade Steps for Latitude

1. The following procedures must be fulfilled prior to upgrading to Latitude NVMS 8.0:
2. Login to Admin Center, System Settings, License and extract the system Activation key.
3. Note: you will need to send the activation key to FLIR Operations get the new V8.0 license.
4. Make sure that the Installation folder created by the previous Latitude build is still in the folder C:\Windows\Downloaded Installations. If this directory was previously deleted for any reason, then contact FLIR Technical Support before carrying out the upgrade, so that the required information can be replaced.
5. Port availability – The Latitude Installation process assumes that certain specific ports are available. Please see the required ports list in the "Default Latitude Port Settings" section of the 8.0 installation instructions and clarifications document. Should any of the listed ports not be available, then your System Administrator should make suitable adjustments in consultation with FLIR Technical Support.
6. Make sure you have available license for Latitude 8.0. Note that any upgrade from a previous version to Latitude 8.0 will require a new license to be installed for every directory server in the system. Note: In order to upgrade from a previous version, you must have a valid SSA.
7. Make sure you have access to the Internet to activate and download the license file.
8. Apply latest Windows updates.
   **CAUTION**: To avoid improper or failed installation, assure that all Windows updates are run **before** and **not during** the Latitude installation process. Please be sure to reboot the machine if required.
   **Note**: The Latitude services must be stopped prior to applying Windows updates
9. Close Latitude clients and all unnecessary applications before running the upgrade
10. When planning to upgrade to the next version, you should consult the “Expected Scenarios and Best Practice” section in the 8.0 Installation instructions and clarifications document.
11. Backing up Existing Systems and Database. The upgrade procedure includes an option to back up the databases. It is highly recommended to select this option.

To obtain the update executable follow one of the steps below:

2. If the desired update version number is not available on the website, please contact support at +1 888 388 3577

It is recommended to deploy this VMS update on all machines – servers, clients and SDK applications.

**Run Upgrade Procedure from a previous version**

1. Copy the software installation packages to the local hard drive of the computer.
   The installation files are extracted to a temporary folder, (this may take a few minutes).
2. The Welcome screen appears.
   Click Next
   The Language Selection dialog box appears.
3. Select the language to be used when working with the Latitude system, and then click Next.
   The System Configuration Backup dialog box appears.
   **Note**: FLIR strongly recommends backing up the application configuration and databases.
4. Accept the default backup path or click Change to use a different backup path. 
   Click Next.
5. The Ready to Upgrade the Program dialog box appears.
6. Click Next to begin the upgrade process of the software.
7. The installation of the required pre-requisites (needed for upgrade) begins.
   The Upgrading Latitude screen appears.
   The Installation wizard shows the status of the components and displays a progress bar.
   Once the installation process is complete, the Installation Wizard Completed dialog box appears.
8. Click Finish.

Notes:

1. SDK applications must be closed manually.
2. Close the client applications before running the installation package.
3. The Windows services will stop for the installation, after the installation is finished, windows services will be launched automatically.
4. Admin Center and Control Center won’t start automatically.
5. Upgrade the server side of the system, starting with the Directory server if not an all-in-one system.

Once the server upgrade concludes, open Control Center over a remote client workstation and connect to the server. You may be prompted to upgrade to the new version. If so, the new version will be downloaded over the network and installed automatically.

B.2.2 Upgrade Steps for Horizon/Meridian

1. A new license should be requested from FLIR operations before the upgrade.
2. Close the client applications before running the installation package.
3. Stop FLIR services and install Windows updates.
4. Obtain the most recently released software file from FLIR Operations or FLIR Enterprise Support.
5. Start by upgrading the server side of the system.
6. Open the containing folder and find Horizon_8.0.0.exe or Meridian_8.0.0.exe
7. Double click the .exe and allow the software to extract the FLIR Installer.
8. Please keep in mind that FLIR services will stop during this upgrade. Therefore, all cameras will be temporarily offline and will not continue recording until the completion of the upgrade.
9. If not already installed, once the package is extracted, the Microsoft .NET 4.5.2 installer will begin. Follow the steps on the screen.
10. Please be patient, as this process can take 15-20 minutes
11. If prompted by the Installer, please allow the server to reboot. The Installer will launch upon login.
12. Continue to follow the prompts on the screen as they appear. Additional reboots may be required.
13. When the Installer completes, open ControlCenter to re-license your server.
14. Once server upgrade has concluded, open ControlCenter over a remote client workstation and connect to the server. You will be prompted to upgrade to the new version. After accepting, the new version will be downloaded over the network and installed automatically without requiring any further input.