Cisco Kinetic for Cities Safety and Security Solution Design and Implementation Guide

This guide presents the design and implementation details for the Cisco Kinetic for Cities (CKC) Safety and Security (SnS) Solution, which provides real-time video analytics for empty and crowded scenes. Existing and new video surveillance systems can be transformed into proactive and intelligent tools while unifying security and operational efficiency. The response times to incidents are accelerated and the user is assisted in gaining a better understanding of the traffic situation. Video analytics accurately detect events in video streams, instantly inform or alarm operators, and trigger processes by sending this information to the Cisco Kinetic for Cities platform. Cisco Kinetic for Cities Safety and Security, which has an open architecture, can be integrated with leading CCTV camera vendors.

Scope of this Cisco Validated Design

The scope of this Cisco Validated Design (CVD) is limited to the design and implementation details of Safety and Security (SnS) use cases in the context of the Cisco Kinetic for Cities (CKC) Starter Solution. Thus, design needs specific to only the SnS Starter Solution are elaborated at each layer of the network. The components selection at each layer are also restricted to the SnS Starter Solution. The details of backhaul transportation, various architectural models of Cisco Video Surveillance Manager (VSM), and the Data Center internal network design are beyond the scope of this document. We recommend that the Cisco Connected Communities Infrastructure (CCI) solution and CVD be considered for this type of connectivity, see: http://www.cisco.com/go/connected-communities-infrastructure. Monitoring of SnS events from the iOmniscient client is also beyond the scope of this document.

Document Organization

The following table describes the chapters in this document:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Overview, page 2</td>
<td>Describes overview of Cisco Kinetic for Cities and the Safety and Security Solution use cases, unique selling points, and ecosystem.</td>
</tr>
<tr>
<td>Solution Architecture, page 6</td>
<td>Describes the Solution architecture, backhaul network considerations, end-to-end security provisioning, and architectural best practices.</td>
</tr>
<tr>
<td>Privacy Protection, page 20</td>
<td>Reference to privacy protection considerations.</td>
</tr>
<tr>
<td>Performance Measures, page 21</td>
<td>Describes performance measures including time taken for event detection and bandwidth and storage requirements at iOmniscient.</td>
</tr>
<tr>
<td>QoS in the Last Mile and in the Backhaul, page 21</td>
<td>Reference to QoS considerations in the last mile and in the backhaul.</td>
</tr>
<tr>
<td>Solution Components, page 22</td>
<td>Describes Cisco and Third-party solution components.</td>
</tr>
<tr>
<td>Data Center Server Sizing, page 23</td>
<td>Describes the system specifications for VSM and iOmniscient servers.</td>
</tr>
<tr>
<td>Cisco Kinetic for Cities (CKC) Platform, page 24</td>
<td>Describes CKC high-level solution architecture and related features.</td>
</tr>
<tr>
<td>Solution Implementation, page 32</td>
<td>Provides the implementation details of the Cisco Kinetic for Cities (CKC) Safety and Security (SnS) solution for the cloud-based deployment model of the solution.</td>
</tr>
<tr>
<td>Solution Components, page 34</td>
<td>Reference to Solution Components, page 22.</td>
</tr>
</tbody>
</table>
Urban areas across the world are experiencing a rapid growth in population size and density. Today, with less than two percent of world’s landmass, cities are home to more than half of the world’s population. This massive growth of population, along with constrained resources, is posing huge challenges to both city authorities and citizens. Cities consume two-thirds of the world’s energy and account for more than 70% of CO2 emissions. These factors require solutions that offer huge opportunities for information technology. In general, high demand for resources coupled with resource constraints and the increasing need for safety and security call for the digital transformation of cities, popularly coined as Smart Cities. A Smart City is an urban area that uses different types of electronic data collection sensors to supply information for efficiently managing assets and resources.

Smart Cities’ digitization programs span several domains, including Urban Mobility, Safety and Security, Smart Lighting, Connected Traffic, Smart Parking, and Environment. The focus of this design and implementation guide is Cisco’s Smart City Safety and Security (SnS) solution.

This chapter includes the following major topics:

- Cisco Kinetic for Cities, page 3
- Cisco Safety and Security Use Cases, page 3
- Cisco Safety and Security Solution Unique Selling Points, page 4
- Cisco Safety and Security Solution Ecosystem, page 5
Cisco Kinetic for Cities

Cisco Kinetic for Cities (CKC) is Cisco's IoT solution for Smart Cities that addresses various city digitization programs. It brings policy-based control and automation to city infrastructure, such as streetlights, parking sensors, traffic and crowd monitoring, environmental sensors, and video (CCTV) cameras. CKC is a powerful digital platform for aggregating, normalizing, and analyzing the wealth of community data from a myriad of intelligent sensors and city assets. The platform is generic and flexible in its ability to support multiple Smart City domains and onboard any relevant partner. Off-the-shelf CKC comes pre-integrated with a large number of partners across the domains.

Cisco Kinetic for Cities Starter Solutions are bundles or packages that help customers to get started quickly with limited budgets. The Starter Solutions assist customers in achieving the following objectives:

- Start small and quickly and then grow over time to full production-scale deployment.
- Use pre-selected technology partners and pre-defined components, making it easy to deploy.
- Achieve tangible business value in two weeks from the physical installation.
- Define the required hardware/software/services from Cisco and third parties as a single solution.
- Obtain easy access in real time to the platform using a web-based graphical user interface. Figure 1 shows the domains for the current Starter Solution bundles.

The CKC Golden Mile bundle is an aggregate bundle with all the capabilities and options of the combined individual CKC domain-specific Starter Solutions and the ability to select the required attributes and combinations.

Cisco Safety and Security Use Cases

Safety and security video surveillance is a need in diverse environments and use cases. In the section below, "empty scenes" refer to less crowded environments such as parking lots and "crowded scenes" refer to large crowds such as market places and concerts.

The Safety and Security Starter Solution covers the following use cases:

- Object detection:
  - Detection of one or more abandoned objects or objects removed from a crowded or empty scene, including difficult environments such as:
  - Detection of tiny objects, which are difficult even for the human eyes to detect.
  - Detection in low contrast scenes, such as a black bag left on a black background.
  - Possible areas include public/open areas of cities, airports, railway stations, museums, and campuses. Benefits from early and automated detection of incidents that may pose a risk to citizens include allowing the object to be retrieved or destroyed more quickly, object theft/removal detection, automated 24x7 monitoring—lowering costs and improving detection rates and, in general, enabling incidents related to such objects to be managed effectively.
Solution Overview

- Intrusion detection:
  - Detecting abnormal behavior such as people or vehicles traveling in the incorrect direction or entering a restricted zone.
  - Detect and alert intrusion events ranging from something as trivial as parking in a no-parking zone to something more serious like a person walking into the grounds to the White House!
  - Generate alerts when a predefined zone has been entered or exited, by people, vehicles, etc.

- Perimeter protection:
  - Detecting intrusion into the perimeter or boundary of a protected area.
  - An example is generation of alerts when a physical or virtual boundary or perimeter is crossed, such as someone is detected crossing a yellow line and reaching close to the edge of the platform when the train is not at the station.

- Facial Recognition (FR):
  - Matching faces in crowded uncontrolled environments (such as airports, railway stations, and market areas), in challenging environments (such as variable lighting, continuous movements, low resolution, and variable facial angles), against a database (such as blacklisted), and to flag wanted individuals; usually liaising with law enforcement.
  - Matching faces in controlled environments (standing at a counter in high security zones) is a one-to-one facial recognition; usually needed by law enforcement agencies and security check posts.

- Camera video diagnostics:
  - Automatic alerts when cameras are disconnected or out of focus, have been physically moved or tampered with, are providing poor image quality, or if the image quality is poor because of bad weather, variable lighting, or other complex conditions.

Cisco Safety and Security Solution Unique Selling Points

The unique selling points for SnS include the following:

- End-to-end video surveillance solution
- Automated 24x7 video surveillance monitoring—lowering costs and improving detection rates
- Video surveillance in challenging scenarios such as crowded scenes with continuous movements, low resolution images, varying light conditions, low contrast backgrounds, detection of tiny sizes, Facial Detection in varying angles, and detection of left objects half the time hidden in crowd
- Automated video surveillance alerts with the ability to trigger predefined standard operating procedures (SOPs)
- IP67-rated outdoor IP cameras with high-definition, integrated infrared, industry leading image quality, and processing power supporting efficient image compression H.265/H.264
- Cameras supporting dual video streams helpful to accommodate high resolution video recording needs and low resolution video surveillance needs simultaneously
- Plug and Play (PnP) cameras with centralized control and management, supporting multiple video network architectures
- Instantaneous view of event, image, and footage of SnS violations, and support of video wall
- Multi-domain/cross-domain event correlation and policy definitions
- Vendor/technology-independent data normalization, incidents, views, and reports
Solution Overview

- Scalable architecture both in geography size of SnS solution and quantity of cameras
- End-to-end QoS treatment in the owned part of the network
- End-to-end security for the video and control traffic
- Pay-as-you-grow model; pay only for services consumed
- Large multi-domain partner integration base; Cisco-certified partner ecosystem

Cisco Safety and Security Solution Ecosystem

Technology Partners for SnS

Cisco has partnered with iOmniscient for the video analytics capability in its Safety and Security Starter Solution (https://iomniscient.com/). iOmniscient is on the Cisco Global Price List (GPL) via Solutions Plus.

Using its internationally patented technologies, iOmniscient is the technology leader in real-time video analytics with a capability to analyze realistic, complex, and extremely crowded spaces. The company has over 16 years of extensive industry experience, with a presence in more than 30 industries over 14 countries. The company boasts its artificial intelligence-based Nuisance Alarm Minimization System (NAMS) that can eliminate false alarms without compromising detection accuracy. With its global footprint and distributed development and support centers, iOmniscient is able to offer solutions to Cisco partners and customers across the globe.

CKC Licensing Models

- **CKC Cloud-hosted Model**—The digital platform will be deployed on a cloud owned by a Cisco certified cloud partner and will be hosted and managed by Cisco.
- **On-premises Deployment Mode**—The digital platform will be deployed on a data center server or be cloud managed by the customer. The initial deployment will be handled by the Cisco team and thereafter the customer will manage the digital platform on their cloud.

The Starter Solutions are supported only with the CKC Cloud-hosted model.

For general deployments, the CKC platform offers the following subscription categories that customers may choose from based on what best meets their needs:

- **Things as a Service (TaaS)**—Base offering provides data from sensor assets from one vendor within one domain.
- **Domain as a Service (Daas)**—Normalized sensor data across vendors exposed to the platform as APIs.
- **Business as a Service (BaaS)**—Normalized data across domains, enabling contextual relationships between two or more different domains; data also exposed to the platform as APIs.

The required software subscription SKUs (TaaS, Daas, and BaaS for one year) are included in the respective Starter Solution bill of materials (BoM).
Solution Architecture

This chapter includes the following major topics:

- **End-to-End Solution Architecture**, page 6
- **Backhaul Network Considerations**, page 19
- **End-to-End Security Provisioning**, page 20
- **Architectural Best Practices**, page 20

**End-to-End Solution Architecture**

The SnS end-to-end solution architecture is shown in **Figure 2**. The solution is logically divided into four layers: the Street, Backhaul, Data Center, and Cloud layers:

- Lower most is the Street Layer, which hosts cameras and access switches that connect the cameras.
- Backhaul is any public/private transport network connecting the Street Layer and the data center.
- Data center hosts video network management and video visualization systems.
- In turn, the video events and corresponding video snippets from video analytics systems are forwarded to CKC hosted in the Cloud Layer.

**Figure 2** Safety and Security Solution High Level Architecture

IP cameras are connected to the PoE port of an Ethernet switch. The Ethernet switch communicates with the IP camera over a secure socket layer (SSL/TLS) or https and controls its operations.

The Cisco Connected Communities Infrastructure (CCI) solution and CVD is recommended as a suitable network architecture to support IP (CCTV) camera connectivity and connectivity to the Cisco VSM and iOmniscient video services components. For more information, refer to the following URL:

Cameras—the End Devices

Cameras are the end devices in the SnS solution. The performance of the camera is key to how the video analytics functions. Therefore, making the correct choice of camera type, camera placement, and camera settings/configurations is crucial.

Camera Specification

The camera specifications mandatory for SnS functioning are enumerated in Table 1. Note that Table 1 does not list camera features that do not affect SnS functioning directly, such as power source, local storage, multiple-streams, high-resolutions, audio support, and QoS.

Table 1 Camera Specifications for Safety and Security

<table>
<thead>
<tr>
<th>Desired/Mandatory Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum supported resolution (pros and cons with higher resolutions are discussed below)</td>
<td>384x288 1xCIF (0.1 megapixel)</td>
</tr>
<tr>
<td>Video Compression</td>
<td>IP Camera: M-JPEG/JPEG/H.264</td>
</tr>
<tr>
<td></td>
<td>IP Camera: MPEG4 compatible with Real Time Streaming Protocol (RTSP) or Dispersion-shifted Fibers (DSF)</td>
</tr>
<tr>
<td></td>
<td>Analog camera: With Video Server for Digital conversion</td>
</tr>
<tr>
<td>PTZ camera</td>
<td>Fixed cameras are preferred to pan-tilt-zoom (PTZ) cameras</td>
</tr>
<tr>
<td></td>
<td>Continuously moving PTZ cameras can't be used.</td>
</tr>
<tr>
<td></td>
<td>PTZ cameras that are fixed in their home position are acceptable.</td>
</tr>
<tr>
<td></td>
<td>PTZ camera with a pre-defined touring (e.g., 1 pm at preset 1 and 4 pm at preset 2) can be used with scheduled configuration/settings matching the touring schedule.</td>
</tr>
<tr>
<td>Day/Night camera</td>
<td>Infrared or thermal cameras are preferable for night-time surveillance</td>
</tr>
<tr>
<td></td>
<td>Infrared illuminator with auto switch between day and night mode are to be used.</td>
</tr>
<tr>
<td></td>
<td>Thermal cameras detect the infrared radiation emitted by warm objects. Consequently, they are suitable for surveillance over large-areas such as perimeter fences and large factory sites.</td>
</tr>
<tr>
<td></td>
<td>P-Iris: Suitable in varying lighting conditions</td>
</tr>
<tr>
<td>Environmental Certification/Outdoor ready</td>
<td>Appropriate outdoor certified: IP66/IP67 certified</td>
</tr>
</tbody>
</table>

Any Cisco camera meeting the above specifications can be used for the SnS solution. However, the Cisco Video Surveillance 8030 IP Camera (IPC 8030) is tested and offered as part of the SnS Starter Solution.

Camera Placement

This section provides high level guidelines and specifications for camera placement, which plays a key role in any successful video analytics deployment.

The following are general guidelines and key considerations for camera placement:

1. **Camera Height and Mounting**—Mounting cameras at high places will give the software a better chance of accurate detection. However, cameras need to be mounted securely to minimize wind-induced vibration. Camera Vibration will impact reliability.
2. **Camera Angle of View**—Angle should be between 15°-60° from the horizon, while the preferable angle is 45°. The camera should be placed so that the FOV focus covers most of the Area of Interest (AOI), which should be close to the center of image. The object to be detected should occupy most of the field of view. Moving objects should remain within the view at least for 10 frames. The camera should be angled so that rain water does not get onto the lens.

3. **Clear Vision of the Scene (distance of camera from object), obstruction consideration**—Not to be obstructed by walls, light fixtures. Camera must not view through a wire mesh or glass (here glass refers to a glass door/wall, not the glass of the box in case of a box-mounted camera). Camera needs to have lenses with appropriate focal length to clearly see the desired FOV.

4. **Level of Illumination (sufficient light, day/night vision)**—Area must be sufficiently lit. Lighting variation should be minimum. Camera must not receive direct light source (e.g., sun or headlights). If night operation is needed, then the area needs to be lit sufficiently or the camera needs to be a thermal or an infra-red camera.

5. **Correct Size of the Object to be Detected**—The size of the object relies on several factors such as focal length of camera lens and camera resolution. As a guideline, the object should be covering a minimum number 15 to 20 pixels or a minimum 5% of frame/screen height in the video output.

Besides these generic guidelines, different use cases have specific guidelines. Refer to Forensic Analysis, page 14 for a detailed explanation of the intelligent video analytics packages (iQ-series1) from iOmniscient. Because of the high complexity of video analytics, site survey and camera deployment, guidance by a video analytics photography expert from Cisco/iOmniscient is highly recommended.
**Table 2  Use Case-wise Camera Placement Guidelines**

<table>
<thead>
<tr>
<th>Use Case</th>
<th>iQ-Series</th>
<th>Camera Placement Guidelines (Also refer to Table 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter Protection</td>
<td>iQ-100</td>
<td>The objective of the perimeter protection application is to protect a border that may or may not have a physical fence on it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ideally the cameras should be positioned looking along the perimeter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Each camera should overlap the view of the camera preceding it. This could generate two alarms for a single incident in the overlapped area. However, it will ensure that an event is not missed.</td>
</tr>
<tr>
<td>Minimum Object Size</td>
<td></td>
<td>Objects should be no less than 10% of the height of the camera view.</td>
</tr>
<tr>
<td>Minimum Camera Height</td>
<td></td>
<td>Objects should be no less than 10% of the height of the camera view.</td>
</tr>
<tr>
<td>Camera View</td>
<td></td>
<td>Cameras should be angled between 45 and 60 degrees from the vertical.</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>iQ-100</td>
<td>The height of the intruder should be preferably 10% of the screen height. Trying to detect smaller objects increases the possibility of false alarms since the system cannot differentiate between a person and a small animal. Under normal lighting conditions, a minimum light level of 5Lux from the reflected object should be there.</td>
</tr>
<tr>
<td>Minimum Object Size</td>
<td></td>
<td>Objects should be 10% of the height of the camera view.</td>
</tr>
<tr>
<td>Minimum Camera Height</td>
<td></td>
<td>5 meters to cover 50meters distance.</td>
</tr>
<tr>
<td>Camera View</td>
<td></td>
<td>Cameras should be angled between 45 and 60 degrees from the vertical.</td>
</tr>
<tr>
<td>Object detection (normal and sensitive)</td>
<td>iQ-140 / iQ-180</td>
<td>Camera FOV should be closer to the area of interest. Image contrast between objects to be analyzed and the background should be adequate such that a human can detect an object of any color left in any part of the area of interest.</td>
</tr>
<tr>
<td>Minimum Object Size</td>
<td></td>
<td>10% of the screen height (15-20 pixels needed to understand the object).</td>
</tr>
<tr>
<td>Minimum Camera Height</td>
<td></td>
<td>It can be fixed at different heights (3m, 4m, 5m, 6m) as long as you see objects clear with minimum size 8*8 pixels for iQ-140.</td>
</tr>
<tr>
<td>Camera View</td>
<td></td>
<td>Cameras should be angled between 45 and 60 degrees from the vertical.</td>
</tr>
</tbody>
</table>
Facial Recognition (FR)
iQ-FD + iQ-FR
FR happens by detecting pixels around the eye balls. Thus, the ambience should attract the person to see towards camera.

To prevent a person who is wearing a hat from obscuring his face, the camera should be placed as close to eye level as possible.

Ideally the person to be recognized must always be walking towards the camera. The best systems may tolerate a deviation of around 30% from the frontal position. However, the greater the deviation, the less accurate will the identification be.

25 Pixel distance between eyes is roughly 7–8% of the camera width in the 1 CIF resolution and roughly 4% of the camera width in 4 CIF resolution. Therefore, adjust camera FOV accordingly.

Number of pixels between the eyes depend on the camera resolution, FOV, and the percent of width the eyes occupy in the camera FOV. Thus, variation of any of these factors can vary FR results.

Distance of camera from the face determines the percentage of width eyes occupy in the camera FOV, the higher the distance, the lower the percentage:

1. Cropping the image at the camera to approximately 1MP (1280x960) (or reducing the FOV) to cover the area around the eyes increases the percent of width between eyes in the FOV.

2. The higher the camera resolution, the higher the number of pixels between the eyes. As per iOmniscient guidelines, 25 pixels between eyes can be obtained at a distance of 1m from the face with a 4CIF (704x480) resolution camera.

Cisco’s Cisco Video Surveillance 8030 IP Cameras have a very high resolution (5MP or 2560x1920), adding to this cropping image will provide significant improvements to the distance at which Facial Recognition (FR) can be performed reliably. Simple experimental results in lab have shown that, with cropping, we can achieve an increase from 1.5 to 4.9 meters in the FR distance, an increase of more than 300%.

**Minimum Object Size** 22 pixels between the eyes in case of FR in an uncontrolled environment and 60 pixels between the eyes in case of controlled FR.

**Minimum Camera Height** Camera placed 2–3 meters above the ground.

**Camera View** Faces should be viewed at an angle no greater than 30 degrees

---

Table 2  Use Case-wise Camera Placement Guidelines (continued)

<table>
<thead>
<tr>
<th>Use Case</th>
<th>iQ-Series</th>
<th>Camera Placement Guidelines (Also refer to Table 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facial Recognition (FR)</td>
<td>iQ-FD + iQ-FR</td>
<td>FR happens by detecting pixels around the eye balls. Thus, the ambience should attract the person to see towards camera.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To prevent a person who is wearing a hat from obscuring his face, the camera should be placed as close to eye level as possible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ideally the person to be recognized must always be walking towards the camera. The best systems may tolerate a deviation of around 30% from the frontal position. However, the greater the deviation, the less accurate will the identification be.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>25 Pixel distance between eyes is roughly 7–8% of the camera width in the 1 CIF resolution and roughly 4% of the camera width in 4 CIF resolution. Therefore, adjust camera FOV accordingly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of pixels between the eyes depend on the camera resolution, FOV, and the percent of width the eyes occupy in the camera FOV. Thus, variation of any of these factors can vary FR results.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distance of camera from the face determines the percentage of width eyes occupy in the camera FOV, the higher the distance, the lower the percentage:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Cropping the image at the camera to approximately 1MP (1280x960) (or reducing the FOV) to cover the area around the eyes increases the percent of width between eyes in the FOV.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. The higher the camera resolution, the higher the number of pixels between the eyes. As per iOmniscient guidelines, 25 pixels between eyes can be obtained at a distance of 1m from the face with a 4CIF (704x480) resolution camera.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco’s Cisco Video Surveillance 8030 IP Cameras have a very high resolution (5MP or 2560x1920), adding to this cropping image will provide significant improvements to the distance at which Facial Recognition (FR) can be performed reliably. Simple experimental results in lab have shown that, with cropping, we can achieve an increase from 1.5 to 4.9 meters in the FR distance, an increase of more than 300%.</td>
</tr>
</tbody>
</table>

Note: For a detailed specifications and guidelines, contact iOmnisicent to obtain the Camera Placement Guide.

Camera Settings/Configuration

Cameras can support multiple streams. For information on how different streams can be used for different purposes, refer to Table 5. The desired settings for the camera stream used for video analytics are given below. Templates can be defined with the desired configuration and applied to a group of cameras.

- **Encoding/Codec** – NTSC or PAL
- **Video Codec** – M-JPEG/H.264
- **Video resolution** – Minimum 384x288. Higher resolution increases network bandwidth, storage and video analytics server processing requirements; however, with higher resolution, the FOV in which the objects can be detected can be increased. Refer to Table 2 for use case-wise minimum resolution recommendations.
Frames Per Second (FPS)—Frame Rate refers to the number of frames per unit time. FPS influences the visual perception of continuous motion or smoothness in a scene. For Video Analytics applications, smoothness plays a less significant role. Minimum frame rate requirements vary for different video analytics use cases. Higher frame rates increase CPU load on video analytics servers and can also increase false alarms. Therefore, FPS should be kept to minimum. Motion detection use cases typically need 6fps and non-motion use cases need only 2fps. Refer to Table 3 for use case-wise FPS recommendations.

Table 3 Camera Resolution and FPS Chart

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Minimum Resolution</th>
<th>Minimum Frame Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facial Recognition (uncontrolled)</td>
<td>The software can work at 1xCIF, but the distance at which recognition can be done depends on resolution. Generally use 1 to 2 mp to recognize 5 to 15m, respectively. Camera should have good WDR capability. Min 15mm lens.</td>
<td>No minimum FPS. At one frame needed capturing the face.</td>
</tr>
<tr>
<td>Facial Recognition (controlled)</td>
<td>1mp</td>
<td>No minimum FPS. At one frame needed capturing the face.</td>
</tr>
<tr>
<td>Advanced Objection Detection</td>
<td>1xCIF (0.1 mega-pixel).</td>
<td>2 fps</td>
</tr>
<tr>
<td>Intrusion</td>
<td>1xCIF (0.1 mega-pixel).</td>
<td>6 fps</td>
</tr>
<tr>
<td>Perimeter Protection</td>
<td>1xCIF (0.1 mega-pixel).</td>
<td>6 fps</td>
</tr>
</tbody>
</table>

Bit Rate Mode—Variable Bit Rate (VBR) mode is preferable to optimize average bandwidth requirement and to maintain image quality. VBR typically produces significantly higher quality than CBR at similar bit rates for IP Video Surveillance (IPVS) applications due to less complex scenes (where there is limited motion) in most of the cases.

Bit Rate—Desired bit rate for transmission.

Quality—Preferably set to “High.” This parameter determines which of the two parameters (FR and Resolution) on which to compromise when movements in the scene are high, in order to maintain the desired “Bit Rate.” When movements in the scene are high, video compression efficiency reduces. Therefore, if the “Quality” is set to high, FR is reduced; if Quality is set to “Low,” resolution is reduced; overall, the system tries to maintain the “Desired Bit Rate.”

Video recording—Not needed at the video server, processed video clip recording is done at the video analytics server (iOmniscient).

Triggers from camera—No triggers/events needed to be configured.

Camera analytics—No camera analytics needed.
As mentioned earlier, in case of a multi stream camera, different streams can be used for different purposes. Camera stream configurations for a single and dual stream camera are given in Table 4:

<table>
<thead>
<tr>
<th>Camera type</th>
<th>High resolution—recording needed</th>
<th>High resolution—no recording needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Stream</td>
<td>Configure Stream-1 corresponding to resolution and FPS suitable for video analytics.</td>
<td>Configure Stream-1 corresponding to resolution and FPS suitable for video analytics. Use the same stream for video recording. No need to configure Stream-2.</td>
</tr>
<tr>
<td></td>
<td>Configure Stream-2 with higher resolution and FPS suitable for video recording.</td>
<td></td>
</tr>
<tr>
<td>Single Stream</td>
<td>Configure Stream-1 with higher resolution and FPS suitable for video recording. Use the same video stream for video analytics.</td>
<td>Configure Stream-1 corresponding to resolution and FPS suitable for video analytics.</td>
</tr>
</tbody>
</table>

Access Network Switches

Access network switches provide Power over Ethernet (PoE) power and Ethernet connectivity to the cameras. As per its power specification, the Cisco Video Surveillance 8030 IP Camera requires a PoE+ (802.3at Class 4) power source. It has a power requirement of Max 25.5W. Cisco IE 4000 Industrial Ethernet switches support up to eight POE+ access ports. The switch has a power budget of up to 170W. Thus, up to 6 Cisco Video Surveillance 8030 IP Cameras can be supported per switch.

The Cisco IE 4000 switch supports four Gigabit Ethernet (GE) combo uplink ports, thus supporting up to 4Gbps uplink traffic. Each camera stream can occupy up to 8Mbps. Thus, maximum bandwidth requirement is $= 6 \times 2 \times 8 = 96$Mbps, which is much smaller than one GE, providing enough bandwidth needed for a fully loaded system. The Cisco IE 4000 switches are connected to the backhaul over GE and the traffic is secured.

The access layer switches have the following:

- Fiber and copper Ethernet access ports
- PoE and PoE+ support
- QoS support
- Security support

Backhaul Network

Because of the non-stringent nature of network QoS demands (priority/latency/jitter) for the use cases addressed in this solution, any public/private backhaul meeting the minimum needs can be used. Refer to Backhaul Network Considerations, page 19 for various backhaul network considerations. For network bandwidth calculation, refer to the Cisco Video Surveillance Manager: Design Guide at the following URL:


Cisco Video Surveillance Manager (VSM)

Cisco VSM serves the purpose of camera management, stream management, video conversions, video storage, and video monitoring. Cisco VSM consists of the Media Server, Video Service Operation Manager (VSOM), and Safety and Security Dashboard (SASD). VSOM has two components: the VSOM server and the VSOM client. The video architecture is shown in Figure 3.

- **Media Server**—The Media Server provides video streaming, recording and storage for the cameras and can be hosted in a distributed or central architecture.
Solution Architecture

- **VSOM Server**—The administration and configuration tool that manages all Media Servers in the network and is centrally hosted at the Data Center.

- **VSOM Client**—The browser-based UI for VSOM.

- **Safety and Security Desktop (SASD)**—Tool for viewing video events and live video from multiple cameras.

Cameras are connected to access switches via the Ethernet. Access switches transport the camera traffic via the backhaul to the Media Server. The specific video streams subscribed by the iOmniscient video analytics server (hosted in the same data center) are forwarded by the Media Server to iOmniscient. Similarly, the Media Server also forwards the video streams to video visualization systems like the SASD. The iOmniscient server pushes video analytics alerts to the cloud-hosted CKC. The video snippets corresponding to the alerts are stored by iOmniscient and provided to CKC on demand. The SASD terminal of the Cisco VSM is used to view live/recorded video streams from multiple cameras from multiple sites simultaneously in a single video screen.

**Figure 3 Safety and Security Network Architecture**

Video Network Architecture

A centralized single-tier VSM architecture with Media Servers and storage co-located at the network operating center (NOC), along with the iOmniscient server, are recommended as a general architecture since all video streams to be analyzed have to reach the iOmniscient server. This video architecture is shown in **Figure 3**.

However, in the case of high resolution dual stream cameras, to minimize backhaul bandwidth requirements, one may opt to configure one stream as high resolution for recording and the other stream as low resolution for video analytics. Thus, the high resolution stream can be recorded locally and only a low-resolution/bandwidth stream is transported to a central location for video analytics. In this scenario, a two-tier VSM-architecture with distributed Media Servers located at every cell site for local recording of the high-resolution stream can be adopted.
Note: Most cameras that conform to the Open Network Video Interface Forum (ONVIF) specification will be supported in the system. However, ONVIF conformance does not warrant or guarantee that the camera can be used for analytics.

Before trying to connect the camera stream to the iQ-Series, it is a good idea to test it using the VLC Media Player to confirm that an image can be seen. The VLC player, which is an open source utility, is very useful for confirming that the RTSP stream works.

Forensic Analysis

iQ-Series supports forensic analysis from pre-recorded footage, which can be in the form of image sequence files, video files, 3D-video files, or proprietary VMS archive files.

VMS archive files: Pre-recorded video archives can be fed into the iQ-Series system for analyzing in forensic mode. The external applications that are currently supported in this mode include Cisco VSOM.

Cisco VSM and iOmniscient Interface

All Cisco cameras are managed by Cisco VSM. The cameras are connected to the Media Server and one or more Media Servers are managed by a single VSOM, as shown in Figure 3. All cameras from all Media Servers are visible at the VSOM. iOmniscient can interface with the Media Server directly or via VSOM. However, for a uniform centralized interface, it is preferable to interface with VSOM. Video streams from the camera are sent to iOmniscient via the Media Server. iOmniscient performs video analytics and pushes video analytics events in parallel to both VSOM and CKC. These video analytics events are displayed at the SASD terminal of VSOM. Event handling at the CKC is discussed in Cisco Kinetic for Cities Safety and Security Support, page 17. All related configurations can be done from the iOmniscient client and the VSOM client.

iOmniscient

iOmniscient is the video analytics system. The product from iOmniscient, which is part of the CCK Safety and Security solution, is called the iQ-Series. The following specific iQ-Series licenses/components are part of this Safety and Security Starter Solution:

- **iQ-100**—Perimeter Protection/Intrusion Detection
- **iQ-140**—Object Detection in crowded scene
- **iQ-180**—Object Detection sensitive (detect objects as small as 4x4 pixels)
- **iQ-Infinity**—All functions of iQ-100, iQ-140, and iQ-180
- **iQ-FR**—Facial Recognition

Perimeter Protection and Intrusion Detection differ in terms of the shape to be monitored for access. In the case of Perimeter Protection, the shape typically has very high length and short breadth whereas with Intrusion Detection it could be of any random shape. Both cases fall in the category of very low crowd or open area. The camera features and positioning guidelines vary for the two use cases.

The iQ-180 version of object detection is a super-sensitive version of iQ-140, which is reserved for very special projects where the customer needs to detect very tiny objects in very low contrast areas. For the vast majority of the object detection use cases, iQ-140 is sufficient.

Technically, iQ-180 can detect objects that are 4x4 pixels in size although it is also capable of detecting objects that may be invisible to the human eye. An example would be a black bag on a black floor, hidden by a shadow. Even if the naked eye cannot see the object due to the low contrast, the iQ-180 may still be able to detect it.
iOmniscient offers two types of facial biometric products, which offer different capabilities:

- **Facial Detection iQ-FD**—The iQ-FD Facial Detection System can capture multiple faces in an uncontrolled environment such as in public areas, eliminating the need for physical contact and gives covert ability to an operator to see a person.

- **Facial Recognition iQ-FR**—The iQ-FR Facial Recognition system can compare the images obtained by the iQ-FD system with a database of images and assist in the identification of individuals.

Facial Recognition requires the camera to be connected to face gallery. If the Facial Recognition Server is installed locally to IQ Server, the connection between the camera and Facial Recognition Server is done automatically by the IQ Server; otherwise, if the remote Facial Recognition Server is used, the camera is to be connected to the Facial Recognition Server manually.

The IQ-Series and corresponding licenses are bundled based on the desired use cases and corresponding sensitivity/intelligence level needed for detection. The iQ-Rating chart summarizes the iQ types and their capabilities. Higher sensitive detections need higher CPU so making the correct product choice is important.

### iOmniscient Licensing Model

iOmniscient products are licensed per camera stream and per iQ-product type. As mentioned, some product types include multiple detections that are shown in Figure 4. As mentioned earlier, the products included in the SnS starter solutions are iQ-100, iQ-140, iQ-180, iQ-Infinity, and Facial Recognition.

![Figure 4 iOmniscient iQ Rating Chart](image-url)
Solution Architecture

Consideration for AOI and Filters

Area of Interest (AOI) eliminates unnecessary processing for uninterested areas in the camera view. Filters can be set within each AOI. Filters, which define what to look for in order to raise alerts, include different types (such as color, size, human, and aspect ratio) that can be defined. Filters that are too broad raise false alarms and those that are too narrow miss alarms. For example, a too small size filter will raise false alarms and a too big size filter will mask real alarms. The size of an object corresponds to its distance from the camera. A general rule of thumb is to have a 20% margin; a smaller filter is 20% less than the minimum size and larger filter is 20% higher than the maximum size.

Model tracking matches specific models and filters, for example, for humans distinguished from animals and vehicles. The human filter itself can have different views (side, top, diagonal) and takes into account aspect ratio, size, and speed of the object for detection. Based on the need, alarms can be generated on humans or others.

Dynamic Configuration and NAMS

The iOmniscient system is equipped with a Nuisance Alarm Minimization System (NAMS), which provides robust operation in its environment with minimal false alarms. Dynamically, the conditions of background and light can be detected and different configurations suiting the current scene can be applied by iOmniscient, thus improving detection.

NAMS can be configured to remove noise such as small moving objects and changes in the background due to stopped moving objects, and can be adjusted for light intensity. Advanced motion detection helps tuning for cases that are very sensitive to lights, having a lot of shadows, and vibrations.

Event Notifications

iOmniscient can do web streaming for analytics events to multiple external receivers such as CKC and Cisco VSM Soft Trigger. The URLs for image and video snippets corresponding to the reported alarm are embedded in a XML and pushed via web protocols. The receiver can play/view the embedded image/video. The identity of the camera stream generating the event, event-type, time, filtered area with coordinates, etc., are provided in the event for the receiver to correlate. The video and image files are stored at the iOmniscient server for a configured period. For a FR-only image, alarm notification provides only the URL. Pre- and post-alarm footage length can be adjusted.

Cisco VSM displays the events in the SASD terminal and CKC displays it in the CKC client views.

iQ Health Check

Different conditions such as tampering, blackout, camera disconnection, and low lighting contrast can be detected and events are generated.

Use Case Specific Guidelines

For default/recommended values of specific configurations corresponding to each use case, refer to Solution Implementation, page 32 and the iQ Series User Help Manual v4.7 at the following URL:


Important configurations include selecting product type, AOI, filters, NAMS, detection time, and advanced alarm settings.

For iQ-140 theft detection in a busy scene, the monitored object can be obscured up to 50% of the detection time, thus avoiding false alarms. The minimum size of the object depends on the iQ product type discussed earlier.

iQ-FD and iQ-FR Specific Guidelines

Multiple faces can be detected simultaneously in a crowd/uncontrolled environment as long as the faces are seen with the desired clarity. Higher resolutions increase the chance to detect faces at a longer distance. The recommended Cisco 8030 is a 5MP camera, which boosts the system’s Facial Recognition capability at a long distance. However, resolution should be set to a desired minimum to minimize CPU load. Several FR-related specific configurations are detailed in the iQ Series User Help Manual v4.7.

The iOmniscient system can detect known faces and raise alarms. The detected faces are matched with a database and the matched faces are notified through alarms. The alarm includes a URL for the found face snapshot.
Enrolling faces can be done from recorded videos, still images, or live. Enrolling multiple faces of a single person from a multiple angle can aid better accuracy. Auto and manual enrollments are possible; manual should be used when a controlled enrollment is needed. Options include One-to-Many, Many-to-One, Many-to-Many. The threshold for match can be set and tuned for better accuracy.

**Note:** Refer to the [iQ Series User Help Manual v4.7](#) for filters and other configurations and tunings specific to FD and FR.

At iOmniscient, it is recommended to keep the archive period to a minimum 15 days or more as per the specific requirements of the deployment:

- Match confidence value indicates confidence of a correct match.
- Match value indicates the accuracy of match.

High resolution Facial Recognition with the Static Face Search Engine (SFSE) library is possible. This is an application for a controlled environment with a higher accuracy of match. It works with face image databases of higher resolution 300x300 pixels as opposed to a 96x96 pixel legacy database. This works best when the image comes from a photograph or when the person faces the camera with a very low deviation angle.

### Cisco Kinetic for Cities Safety and Security Support

CKC is the Cisco’s Smart City umbrella application that supports several Smart City domains, providing a vendor and technology neutral unified view, storage, and interface. CKC supports the Safety and Security domain.

The iOmniscient analyzes live video streams from multiple cameras and forwards events to CKC for viewing and processing. Events are sent as XML documents containing event details and event image/video URLs, as shown in Figure 5 and Figure 6. The CKC presents the received events at different levels of zoom-in and summarizations. To minimize cluttering of events, several event filters are providers (Region, Domain, and Event-type). The operator can view the video footage/image by clicking on the events displayed at the CKC.

**Types of events include:**

- **Camera health events:**
  - Cameras disconnected, not responding busy, out of focus, low contrast poor image, tampered

- **Facial Recognition events:**
  - Person identified / face match found

- **Object detection events:**
  - Abandoned object, object missing

- **Intrusion detection events**
  - Intrusion detection

iOmniscient sends events to both CKC and SASD in parallel. Events and embedded event video footage can be viewed from both of their terminals. Live/recorded video stream from any desired camera can also be viewed at the SASD terminal and with CKC using the optional Video Dashboard capability.

Pre and post-event video clip size can be configured at iOmniscient for recording. Based on the configuration iOmniscient records, the images and video clips pertaining to events. The video/image shown at CKC by clicking on the event is fetched from iOmniscient. On the other hand, VSM stores video continuously. The video shown at SASD is fetched from VSM, thus the size of the video clip to be viewed can be changed dynamically.

For each alarm received at CKC, alarm life cycle is defined and alarm workflow/SOP can be configured. The operator can use pre-defined SOPs such as SMS or e-mail, or define a custom SOP of their choice. The operator can also escalate an event by raising its severity.
Solution Architecture

Figure 5  XML Notification for Facial Recognition Event

```xml
  <AlarmCamera>
    <CameraID>5</CameraID>
    <ServerID>Id</ServerID>
    <ProductType>2</ProductType>
    <CameraDescription>Counter-1 FR Camera</CameraDescription>
    <ImgDescription/>
    <Ly>
      <Latitude>1</Latitude>
      <Longitude>1</Longitude>
    </Ly>
  </AlarmCamera>
  <MatchedPerson>
    <Recog_Output_Rank>1</Recog_Output_Rank>
    <Person_ID>2283</Person_ID>
    <FirstName>2017 12 20 14 23 06 116</FirstName>
    <LastName>1-7</LastName>
    <PersonImage/>
    <ConfidenceLevel>High</ConfidenceLevel>
    <CategoryType>Not Specified</CategoryType>
    <MatchValue>0</MatchValue>
    <GalleryName>Default</GalleryName>
    <GalleryId>1</GalleryId>
    <PersonImageUrl>http://IP Address:8899/images/10873436_1712181301_13520_12283.jpg</PersonImageUrl>
    <Phone/>
    <Email/>
    <Comments/>
    <DriverLicense/>
  </MatchedPerson>
  <MatchedPerson>
    <Recog_Output_Rank>2</Recog_Output_Rank>
    <Person_ID>2214</Person_ID>
    <FirstName>2017 12 20 14 34 206</FirstName>
    <LastName>1-7</LastName>
    <PersonImage/>
    <ConfidenceLevel>Medium</ConfidenceLevel>
    <CategoryType>Not Specified</CategoryType>
    <MatchValue>0.605796602140187</MatchValue>
    <GalleryName>Default</GalleryName>
    <GalleryId>1</GalleryId>
    <PersonImageUrl>http://IP Address:8899/images/10873436_1712181301_13520_2234.jpg</PersonImageUrl>
    <Phone/>
    <Email/>
    <Comments/>
    <DriverLicense/>
  </MatchedPerson>
</Alarm>
```
Backhaul Network Considerations

Video analytics can be done at the edge by the camera or done centrally. The video analytics that can be done in a distributed manner are often limited due to the processing capacity at the edge of the camera. On the other hand, complex video analytics can be done at a central location. Thus, central video analytics on near real-time live streams are common for Smart City use cases and are the ones supported by the SnS Starter Solution and CKC.

In the former case, the media server and video storage are often positioned near the camera location and, in the latter, they are collocated centrally at the data center. The latter one (i.e., the central analytics model) requires the video stream to be transported to the central location; therefore, backhaul needs to have the desired bandwidth. In our design, the video stream to be analyzed by the video analytics engine has to reach the central location at all times in real time. Therefore, the Media Server, VSOM, and storage are preferably located at the central location, co-located with the iOmniscient server.

For the Safety and Security use case targeted in the SnS starter solution, near real-time video analytics itself meets the desired objectives of latency and jitter. However, QoS marking and desired bandwidth allocation are recommended at each node/hop to avoid packet loss and disruptions. The entire end-to-end network management and data path are to be secured.

As mentioned in Cisco Safety and Security Use Cases, page 3, the focus of this guide is video analytics events management; therefore, the details of video network architecture are beyond the scope of this document.
Privacy Protection

End-to-End Security Provisioning

Camera Authentication—All cameras are 802.1x authenticated by the AAA server at the central location. Camera stream forwarding and recording happens after successful authentication. Authentication is repeated at configurable interval typically once a day. The camera keeps retrying until authentication is successful. Port security is enabled on all access layer switches to restrict the number of devices connecting a port. VLANs limit the size of a broadcast domain, assist in management of sub-networks, and help apply differential service levels for different traffic classes. As per the standard VLAN recommendation, separate VLANs should be used to segregate management traffic, IPVS video traffic, and the rest of the traffic across the network (access, core, and data center). Refer to Solution Implementation, page 32 for a sample configuration.

- Communication between VSOM and iOmniscient is secured using HTTPS/TLS.
- Communication between iOmniscient and CKC is secured using HTTPS/TLS.
- Live camera streams from the Media Server are sent to iOmniscient encrypted within the VPN tunnel.

Architectural Best Practices

It is recommended to adhere to the following architectural best practices:

- Follow use case-specific recommended camera models and deployment guidelines.
- Limit video resolution and frame rate to the minimum required.
- Segregate video traffic with separate VLANs.
- Use secured channel of communication at every layer, including between iOmniscient and CKC.
- Refer to Caveats, page 86.

Privacy Protection

Several applications and federal laws might enforce privacy protection while doing video surveillance. The privacy mask can be configured at iOmniscient to blur human faces in a scene. In conjunction with the human filter, the privacy mask will provide more accurate results.
Performance Measures

This chapter includes the following major topics:

- **Time Taken for Event Detection**, page 21
- **Bandwidth and Storage Requirements at iOmniscient**, page 21

**Time Taken for Event Detection**

The live video stream is fetched by iOmniscient. Video analytics performed at real-time and events are pushed to CKC and VSM. Therefore, overall event detection delay is comprised of propagation delay + compute delay. Considering that bandwidth and compute are provisioned as per the specification, the event detection delay should be in the range of a sub-second to a few seconds.

**Bandwidth and Storage Requirements at iOmniscient**

Table 5 lists the bandwidth and storage requirements at iOmniscient.

<table>
<thead>
<tr>
<th>Number of cameras</th>
<th>Resolution</th>
<th>Frame rate</th>
<th>No. of events per day (recording length 30 sec per day)</th>
<th>Compression</th>
<th>Storage in GB per day</th>
<th>Network bandwidth in Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>640x360 (0.2MPx)</td>
<td>2</td>
<td>500</td>
<td>H.264 High quality</td>
<td>0.03</td>
<td>0.016</td>
</tr>
<tr>
<td>1</td>
<td>640x360 (0.2MPx)</td>
<td>6</td>
<td>500</td>
<td>H.264 High quality</td>
<td>0.2</td>
<td>0.05</td>
</tr>
</tbody>
</table>

Considering 10,000 camera streams, 500 events per day, and event clips retaining period 15 days: Storage requirement at iOmniscient: 4500 GB = 4.5TB.

The following online calculator was used to compute storage and bandwidth requirement:

- [https://www.cctvcalculator.net/en/calculations/bandwidth-calculator/](https://www.cctvcalculator.net/en/calculations/bandwidth-calculator/)

Alarm grouping can be enabled, which will suppress duplicate alarms videos.

**QoS in the Last Mile and in the Backhaul**

The video traffic is the source for detecting Safety and Security incidents. Therefore, these video streams must be given proper QoS treatment to ensure low latency and proper bandwidth allocation along the path. This starts with marking these video streams with class CS5 (DSCP 40) at the camera. CS5 is the recommended class marking for IPVS traffic.

Again, at the ingress of the uplink, the switch port receiving traffic from camera should tag all IPVS traffic with IPVS VLAN and mark all video traffic on the specified IPVS VLAN as CS5 (Broadcast Video). At the egress of the access switch to which the camera is connected, configure high priority queuing for all CS5 traffic with guaranteed bandwidth allocation. As per standard QoS guidelines, it is recommended to limit the maximum reserved bandwidth to 30%.

Thus, 30% of the available uplink bandwidth can be reserved for video traffic and configure exceed action as “drop.” For example, this translates to 300Mbps on a 1Gbps uplink and 1.2Gbps on a 4Gbps uplink.
In Access Network Switches, page 12, it is shown that maximum 96Mbps uplink bandwidth is needed from a Cisco IE 4000 switch for the entire video traffic. Thus, the allocated bandwidth will ensure no overflow.

As mentioned earlier, the Safety and Security application does not impose strict latency or jitter requirements as near real time (not real time) video analytics events and the corresponding video are sufficient to serve the desired purpose. However, for a good user experience, the following are the recommended guidelines:

- **Latency**—As a general guideline, Cisco recommends one-way network latency for both image and command should not exceed 150ms when UDP is the transport protocol in order to provide an acceptable quality of experience to viewing clients. For TCP, the round-trip time (RTT) should not exceed 50ms.

- **Jitter**—Cisco recommends that the mean jitter threshold should not exceed 2ms, in order to ensure a good user experience.

No QoS can be guaranteed when the traffic passes through public Internet. However, when enterprise backhaul is used as transport from Cisco IE 4000 to the Data Center, the QoS can be guaranteed. It may be noted that although CKC is cloud hosted, it has minimal impact on QoS since live video stream terminates at the Media Server and iOmniscient server hosted in the Data Center. Only events and on-demand recorded video clips are forwarded to the CKC from the Data Center.

### Solution Components

This chapter includes the following major topics:

- **Cisco Components, page 22**
- **Third-Party Components, page 23**

### Cisco Components

Table 6 shows the Cisco products used in CKC Safety and Security Starter Solution.

#### Table 6  Cisco Components in the CKC SnS Starter Solution

<table>
<thead>
<tr>
<th>Cisco Products</th>
<th>Model and Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Camera</td>
<td>CIVS-IPC 8030</td>
<td>Outdoor dome HD camera with 5 MP resolution, with infrared night vision. Supports H.265, H.264, or MJPEG compression.</td>
</tr>
<tr>
<td>Cisco Industrial Ethernet Switch (NB is recommended, but is not included in the SnS Starter Solution BOM)</td>
<td>IE-4000-4T4P4G-E</td>
<td>Ruggedized Industrial Ethernet Switch</td>
</tr>
<tr>
<td>CKC</td>
<td>2018 Version (auto-upgraded cloud version)</td>
<td>--</td>
</tr>
</tbody>
</table>
Data Center Server Sizing

Table 6  Cisco Components in the CKC SnS Starter Solution (continued)

<table>
<thead>
<tr>
<th>Cisco Products</th>
<th>Model and Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CKC Cloud</td>
<td>CKC version 4.0 and associated activation licenses</td>
<td>Cisco Kinetic for Cities</td>
</tr>
<tr>
<td>CKC Safety and Security as-a-service</td>
<td>Service license for CKC 4.0</td>
<td>Safety and Security module</td>
</tr>
<tr>
<td>UCS servers</td>
<td>CPS-UCSM4-1RU-K9</td>
<td>UCS servers for VSM and iOmniscient</td>
</tr>
<tr>
<td></td>
<td>UCSC-C220-M4S</td>
<td></td>
</tr>
</tbody>
</table>

Third-Party Components

Table 7 shows the Cisco products used in CKC Safety and Security Starter Solution:

Table 7  Third Party Components in the Cisco CKC SnS Starter Solution

<table>
<thead>
<tr>
<th>3rd Party Products</th>
<th>Model and Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOmniscient System</td>
<td>4.6.3</td>
<td>iQ-Infinity, iQ-100, iQ-140, iQ-180 and iQ-FR</td>
</tr>
</tbody>
</table>

Data Center Server Sizing

The SnS data center hosts the VSM server and iOmniscient servers. This section gives the system specifications for VSM and iOmniscient servers. CKC is a cloud-hosted platform, managed by the Cisco CKC operations team; therefore, no specification is provided.

The iQ Series User Help Manual v4.7 gives different minimal server configurations for different sizes of the network and use case requirements. Most suitable for the SnS Starter Solution is the specification for a network of 4 FR and 22 iQ-infinity. The configuration and the recommended server model are listed in Table 8:

Table 8  Server Specifications

<table>
<thead>
<tr>
<th>Server (VSOM + Media Server + SASD)</th>
<th>Component</th>
<th>Minimum</th>
<th>Recommended Server Model</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>CPU</td>
<td>CPU: 2.4 * Intel Xeon-6 core E5-2620 (15Mcache, 2GHz)</td>
<td>UCSC-C220-M4S</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Memory: 8GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hard Disk: 1<em>240GB 6</em>500GB SATA2 7200 rpm</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- OS: 64bit Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSM (VSOM + Media Server + SASD)</td>
<td>CPU</td>
<td>CPU: 2.4 * Intel Xeon-6 core E3-2620 (15Mcache, 2GHz)</td>
<td>CPS-UCSM4-1RU-K9</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Memory: 16GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hard Disk: 4TB SAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- OS: Windows-10, 64 bit OS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cisco Kinetic for Cities (CKC) Platform

This chapter includes the following major topics:

- Cisco CKC High-Level Solution Architecture, page 24
- Cisco Kinetic for Cities Salient Features, page 25
- Tenants, Regions, Domains, and Access Control, page 26
- Portal Tabs, page 27
- Policies and Events, page 28
- System Messages, page 29
- Safety and Security Reports, page 30
- Internationalization Support, page 30
- CKC Safety and Security Northbound API, page 30

Cisco CKC is a centralized integrated Internet of Things (IoT) platform for City Infrastructure and Services management. A multitude of vendors and solution providers often provide city infrastructure such as streetlights, parking lots, safety and security infrastructure, waste management, and environmental monitoring. CKC, as a centralized platform, interfaces with each of these vendors and solution providers and provides a uniform vendor-neutral cross-domain monitoring and management system.

Each solution domain consists of a range of sensors, a secured interface to communicate with the sensors, a mechanism to collect and collate information at a central location, and a central information events and policy management system.

The core functionality of the CKC platform includes:

1. Interface to multi-domain, multi-vendor, multi-technology, multi-interface sensors, devices, and apps.
2. Domain-wise data normalization to a standard data model.
3. Monitoring and controlling of the derived information using the CKC Dashboard and other CKC apps (including third-party applications and analytics apps integrated with CKC via its northbound APIs).
4. A platform for intra-domain and cross-domain correlation and policies.
5. Normalized data models exposed via northbound APIs to business apps.

Cisco CKC High-Level Solution Architecture

Figure 7 shows the high-level solution architecture of CKC. The building blocks include:

- Various domain interfaces
- A real-time engine to collect, normalize, time-series, and store data
- Domain/vertical applications
- Dashboard
- Mobile apps and NBI to third-party apps
Further details and descriptions of the Cisco Kinetic for Cities 4.0 (CKC 4.0) solution and architecture can be found in the CKC 4.0 Business Decision Makers (BDM) deck at the following URL:

- https://salesconnect.cisco.com/open.html?c=fc093f72-bec4-491c-97a7-3975d676dafd

**Note:** SalesConnect information is only available to Cisco Channel Partners and Cisco personnel with a valid Cisco Connection Online (CCO) login. Customers and other interested parties should contact their local Cisco distributor or Cisco Account Manager for additional details.

### Cisco Kinetic for Cities Salient Features

The salient features of the CKC solution include:

1. City-wide solution for multi-domain applications
2. Wide range of supported domains
3. Large number of off-the-shelf partner integrations for each domain, covering various geographies across the world
4. Partner and technology-independent normalized information model across the domain
5. Intra- and cross-domain event correlation and policy enforcement
6. Cross-domain policy-based automation
7. Highly scalable architecture, including compute, data storage, and network capability
8. Cloud-based deployment model
9. Support for user-friendly and customizable dashboards and third-party apps
10. Northbound API exposing both real-time and historical information
11. Out of the box and customizable reports
Tenants, Regions, Domains, and Access Control

Tenants

A tenant is typically a city managed by a customer who is given access to the different infrastructures of the tenant based on the license. Based on the request from the customer for a specific City/Tenant with associated geographic locations, the Cisco Cloud Ops team provisions the same.

Defining Regions within a Tenant

The administrator can define multiple sub-regions within the Tenant’s overall region (that is, City). A sub-region is any random area, overlapping/non-overlapping, within the parent region. A user can be assigned with one or more sub-regions, as shown in Figure 8.

Multi-Domain

Each tenant is provisioned with a set of domains, as per the customer requirement, controlled by the customer license. Assume a multi-tenant customer with two tenants: tenant-1 and tenant-2. As per license, the customer can have different domains for different tenants. For example:

- Domain-1 (only Lighting) can be configured for tenant-1.
- Domain-1 and Domain-2 (Lighting and SnS) can be configured for tenant-2.

CKC Users and Role-based Access Control (RBAC)

CKC is a multi-user and multi-role platform in which multiple users and multiple roles can be created. Roles are groups with a variety of access permissions. Each user can be assigned a set of one or more roles. Broadly speaking, roles have two major categories: operators and administrators:

- Operators have access to operational functionality. Operations are grouped by domains and each domain has an operations group, for example, Parking Operator, Lighting Operator, Environment Operator, and Safety and Security Operator.

- In addition to the functionality of the operator, administrators have rights for administrative functionality such as managing users, assigning roles to users, enabling policy modules, and assigning regions to users. These operator and administrator groups are defined by Cisco Cloud Ops.

Each user can be assigned with one more roles/groups and one or more regions/sub-regions, as shown in Figure 8.

- If one or more sub-regions under a parent region are assigned to a user, the sub-regions (and not the parent region) appear in the drop-down menu.

- If a parent region is assigned and no sub-regions are assigned under the parent region, then the parent region appears in a drop-down menu in the region section.
Figure 8  Users and Role Based Access Control (RBAC)

For Figure 8, which illustrates the flexibility of any user being assigned to any role(s) for any region(s), users are described below:

- User-1 is an administrative user having access to Sub Region-1 for all operator functionality.
- User-2 is a parking operator for Sub Region-1.
- User-3 is a parking operator for Sub Region-2.
- User-4 is a multi-domain operator managing lighting and SnS for Sub Region-1 and Sub-Region-2.

After logging in, users can view the dashboard. From the user’s access-dependent menus, which display in the dashboard, they can select a region from the allowed list of regions to monitor and perform desired operations. All regions assigned to a user are within a single Tenant. Therefore, no user can access any kind of data across the tenants.

To manage the access permissions, the Cisco Cloud Ops team creates an initial set of logins. The CKC Hosting Partner or Customer, using an admin login having user-management permission, can then add subsequent users. The combination of the above capabilities provides RBAC, with “Role” definitions based on the User Group to which a user belongs. User management can also be done through NB integration. User account creation, associating user account to a group and set of locations, can all be done using appropriate Northbound API.

See CKC Safety and Security Northbound API, page 30 for a detailed description of NB interface and operation.

Portal Tabs

The CKC portal provides a multi-tab interface. Upon login, a user can view the CKC portal with tabs and menus based on their access rights discussed earlier. A quick access to a summary view of overall system status and frequently viewed infrastructure is provided. Various prominent tabs and their purpose are described below:

- **Regions**—A drop-down menu that displays various regions within the tenant for which the logged in user has access rights. All tabs within the portal reflect information of the selected region.

- **Dashboard**—A custom-built view that can be defined/updated by the user. The user can configure the dashboard to include one or more pre-defined widgets. Typically, domain-specific widgets are available for each domain, which gives an overview of the domain. The user can select multiple widgets to appear on the dashboard.
Cisco Kinetic for Cities (CKC) Platform

- **Map View**—The map view of the selected region where one or more domain module-map-layers can selectively be superimposed on the geographic map through a multi-level selection. Several such map-layers can be superimposed simultaneously on the selected geo-map.

- **Alerts**—Displays the alert information for different modules/domains. The user can select a pre-defined filter to restrict the list of alerts displayed.

- **Policies**—Lists the current custom and default policies present in the system. The user can create new policies and alter existing policies based on access-rights. More details are available in Policies and Events, page 28.

- **Events**—Access to view and manage event-based actions or conditions that trigger specific actions. More details are given in System Messages, page 29.

- **Reports**—Access for selecting pre-defined report-widgets and viewing the reports online at various zoom-levels.

- **SOP**—Standard Operating Procedures are workflows, which can be scheduled by operator on receipt of an alert to be initiated following an incident or event.

### Policies and Events

The Policies and Events pages provides access to tools for user management of any policy type. Details related to policy and events feature are described below.

**Policies**

A policy is a set of rules that control the behavior of infrastructure items. Each policy has a set of conditions that activate the behavior it provides.

Although platform features can be controlled manually from the user interface, their operation is often automated by means of policies. A policy is a set of rules that automatically modify the behavior of the city infrastructure. For example, an Operator might define policies that implement the following kinds of automated behaviors:

1. Increase street lighting to enhance safety when occupancy increases and dim lights to save energy when occupancy drops beneath a specific threshold.

2. Change the pricing or availability of metered parking spaces in order to accommodate a public event.

Four kinds of polices supported by CKC are listed below in ascending order of priority. Higher priority policy can override lower priority policy.

1. **Default**—The default behavior that is always in effect until a higher priority policy type supersedes it. For example, the default parking policy might make a particular parking space always available at a price of one dollar per hour, but a time-based policy could modify that pricing or availability at specific times of day or on specific days of the week.

2. **Time-based**—The policy is activated by a time-based condition. For example, a time-based policy might supersede the default policy to raise the price of parking from 7 AM to 7 PM on business days and to allow free parking on Sundays and holidays. Another variant of duration-based policy is that which imposes a two-hour maximum on the amount of time a user can occupy a parking space.

3. **Event-based**—This policy is activated based on a sensor input. For example, when a parking space is occupied, parking fees can apply or a parking violation alarm can be raised.

4. **Manual-override**—The policy is overridden manually by an operator or by an administrator. For example, an operator might manually enforce a no parking zone policy to facilitate road repairs.

Policies can be Default Policies (out-of-the-box policies defined within CKC) or Custom Policies. Here “Default” refers to pre-defined/out-of-the-box policies within CKC, not the “default behavior policy” described above. Custom policies are defined by the user.
Default Policy/Out-of-the-Box Policy

Default policies include a list of predefined policies for each domain.

Custom Policy

Custom policies can be defined by the operator in XML or text file format. Sample custom policy templates can be obtained from the Cisco partner or from the Cisco Cloud Ops team. Creating a policy does not apply it. The policy must be associated with one or more locations that it governs. For example, a parking policy might be applied to all parking spaces in the city, to specific parking lots, or even to only specific spaces.

Events

An event defines a set of conditions that can be used to trigger an action. The action could be generating a system message or triggering an event-based policy. The Events page provides tools for creating and managing events. A single event can invoke multiple policies (lighting, traffic, parking). But each policy works with exactly one module. In other words, events are cross domain whereas policies apply to a single domain.

In the case of the SnS domain, events such as Suspicious-Object-Found can be assigned to an AOI. A cross-domain action such as Flash-Light is associated to the event. Similarly, a Person-Identified event can be associated to another cross domain action Light-Nearby-areas.

System Messages

Notifications, Alerts, and Alarms are referred to as System Messages. Various incidents within the CKC infrastructure generate System Messages. System Messages are visible within the Dashboard and CKC Mobile Apps. Of these, Notifications are only informational messages and no action is possible.

- Notifications—Informational Messages
- Alerts—System-actionable Incidents
- Alarms—External Incidents
- Viewing Unread System Messages
- Sorting and Filtering System Messages

Incidents within the CKC infrastructure generate Notification, Alert, and Alarm messages that are visible within the CKC UI and the Enforcement Officer Mobile App.

Notifications—Informational Messages

A Notification is a real-time informational message that the CKC itself generates. For example, whenever a vehicle enters or leaves a parking place, the sensor in that location generates a notification. You can ignore notifications without consequence because the primary purpose of a notification is to generate raw data for reporting purposes.

Each new notification is visible under the Notifications icon immediately upon generation. The bell icon in the CKC UI banner displays the number of unread notifications. Clicking the bell displays the most recent notifications and resets the counter.
Alerts—System–Actionable Incidents

An Alert identifies an incident that is actionable within the CKC infrastructure. For example, a parking violation generates an alert that an enforcement officer can use to issue a parking ticket from the mobile app. Alerts are actionable within the CKC user interface according to a specific workflow that marks the alert into different states such as:

1. New
2. Acknowledged
3. Resolved

Alarms—External Incidents

An Alarm identifies a significant incident that cannot be resolved within the CKC itself. For example, a failed streetlight can be tracked in the CKC UI, but the incident cannot be resolved without the intervention of personnel or systems external to the CKC Platform. Alarms are displayed in the notification panel with a distinct icon.

Alarms have a different icon than informational notifications or alerts. As described earlier, Events are multi-domain policies, not System Messages. Table 9 summarizes these aspects.

Table 9 System Messages and Events

<table>
<thead>
<tr>
<th>Category</th>
<th>Notifications</th>
<th>Alerts</th>
<th>Alarms</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation path</td>
<td>Notification dialog</td>
<td>Alerts tab</td>
<td>Notification dialog</td>
<td>Events tab</td>
</tr>
<tr>
<td>Actionable</td>
<td>No</td>
<td>Yes</td>
<td>By agents external to CKC</td>
<td>No</td>
</tr>
<tr>
<td>Icon</td>
<td><img src="image" alt="Warning" /></td>
<td><img src="image" alt="Information" /></td>
<td><img src="image" alt="Notification" /></td>
<td>N/A</td>
</tr>
</tbody>
</table>

Safety and Security Reports

Safety and Security reports are multi-level drill-down reports supported by CKC. SnS event reports such as Object Detection and Intrusion Detection reports provide yearly summary (average) reports, which can be drilled down for monthly, daily, and hourly report views.

Internationalization Support

Any operator or administrator user can select the preferred language for CKC dashboard display. All menus, sub-menus, drop-down menus, and labels are displayed in the preferred language. The user can switch language of choice anytime. The choice of languages for a Tenant is provisioned by the Cisco Cloud Ops team. English is supported by default. Any other language can be supported based on the business case.

CKC Safety and Security Northbound API

To access the Northbound API, the Northbound app need to obtain an OAuth2 authentication token by logging in with an existing client-id, client-secret, and user account credentials. The client-id and client-secret are provided by the CKC Cloud Ops team. All authorizations of the user login used for getting an OAuth2 token are applicable to subsequent operations done using the obtained OAuth2 token. Different categories of Northbound API include the Core Services API,
Real-Time Engine API, Time-Series Engine API, and Policy API. Table 10 briefly summarizes these categories.

Table 10  CKC Northbound API Description

<table>
<thead>
<tr>
<th>API Category</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Services API</td>
<td>These API are common to all domains. This includes API for authentication/authorization, user/group, and location management.</td>
</tr>
<tr>
<td>Real-Time Engine API</td>
<td>This has API to obtain real time domain specific information. Different APIs are available for different domains. Both read and write operations are possible using the appropriate API.</td>
</tr>
<tr>
<td>Time Series Engine API</td>
<td>Time Series API has a domain-specific API to retrieve historic data from the system.</td>
</tr>
<tr>
<td>Policy API</td>
<td>This includes API to define new policies (Trigger and Action) and to find and delete existing policies.</td>
</tr>
</tbody>
</table>
Solution Implementation

This chapter, which provides the implementation details of the Cisco Kinetic for Cities Safety and Security Solution for the cloud-based deployment model of the solution, as discussed in Solution Architecture, page 6, includes the following major topics:

- Implementation Overview, page 32
- Implementation Scope, page 32
- Solution Topology, page 33

Figure 9, which shows the complete flow of the implementation, is referred to throughout the remainder of this document:

Figure 9  Cisco Kinetic for Cities (CKC) Safety and Security Solution Implementation Flow

Implementation Overview

The implementation details of the CKC Safety and Security Solution include system topology, components, and networking for the solution deployment along with integration of Cisco Video Surveillance Manager (VSM) and the iOmniscient Video Analytics Server (IQ-Server) with its components in the Data Center, City, and the Streets layers of the system architecture. Integrating CKC with iOmniscient Video Analytics Server for Safety and Security use case provisioning along with system caveats are also discussed.

Implementation Scope

The Cisco Kinetic for Cities Safety and Security Solution CVD consists of the Design chapters, which provides the overall guidance for the system design, and these Implementation chapters. Refer to Cisco Safety and Security Use Cases, page 3 for the scope of this document.

The scope of this solution implementation is limited to Safety and Security Solution deployment, which is based on the Cisco Video Surveillance Manager and iOmniscient Video Analytics solution integration and its use cases with a cloud-based instance of CKC, as defined in the Starter Solutions BoM.
The detailed implementation of the core network or other infrastructure services in the City and Data Center layers of the design is beyond the scope of this document. For more details on the recommended architecture and best practices for the design and deployment of a Smart City network, please refer to the Cisco Connected Communities Infrastructure solution and CVD at the following URLs:

- [https://salesconnect.cisco.com/#/program/PAGE-15434](https://salesconnect.cisco.com/#/program/PAGE-15434)

**Note:** The SalesConnect information is only available to Cisco Channel Partners and Cisco personnel with a valid Cisco Connection Online (CCO) login. Customers and other interested parties should contact their local Cisco distributor or Cisco Account Manager for additional details.

### Solution Topology

This section covers the CKC Safety and Security solution network topology, solution components, and the Layer 2 and Layer 3 reference configuration of the system for the deployment model discussed in *End-to-End Solution Architecture*, page 6.

*Figure 10* shows the CVD network topology for the CKC Safety and Security solution in the Street, City, and Data Center or Internet Services layers of the solution architecture.

**Figure 10**  
Cisco Kinetic for Cities Safety and Security—Solution Network Topology

**Note:** The solution topology in *Figure 10* is an example deployment model for the Safety and Security Solution with a wired backhaul network at the Street and City layers of the system architecture, as defined in the Design chapters of this document. A reference implementation of wired Ethernet backhaul network for the solution topology in *Figure 10* is covered in this document. Detailed implementation of the other backhaul network infrastructure such as wireless and cellular is out of the scope of this document.
Solution Components

Street Layer

In this deployment, Cisco IP Camera endpoints (Cisco Video Surveillance 8030 IP Camera) connect to the Cisco Industrial Ethernet 4000 Series (Cisco IE 4000) switches in the Street Layer. Cisco IE 4000 switches in the Street Layer provide power to the IP Camera through Power-over-Ethernet (PoE).

Industrial Ethernet switches (Cisco IE 4000) provide a power and uplink network access to Cisco IP Cameras in the wired backhaul network and provide network access to Cisco Video Surveillance Operations Manager and Media Server in the data center.

City Layer

Cisco IE 4000 switches in the Street Layer aggregate to Cisco ASR 920 switches and Cisco Catalyst 4500-X distribution switches in the City layer. Network traffic from ASR 920 switches is aggregated at the Catalyst 4500-X switch and forwarded to the Data Center Layer.

Internet and Data Center Layer

Internet Service Providers (ISPs) for the Cities provide Internet services through which the CKC Cloud application is accessed for viewing the different incident alerts that are raised from the iOmniscient Video Analytics server (IQ-Server) on the Street Layer camera feeds. Integration of CKC and the iOmniscient IQ-Server is done at this layer for the end-to-end Safety and Security use cases and functionalities, as described in the Design chapters of this document.

Solution Components

Refer to Solution Components, page 22 for the list of Cisco and third-party devices used this solution.

Note: Backhaul wired networking devices (Cisco IE 4000, Cisco Catalyst 4500-X, etc.) used in the deployment diagram in Figure 9 are example backhaul network infrastructure devices for the Cities wired Ethernet network backbone and are not covered in the Starter Solution BoM.

Solution Networking

The SnS solution deployment should deploy on separate logical networks (VLANs) for people/end devices at the Street Layer and network infrastructure devices management. It is a best practice recommendation to use separate VLANs for camera traffic and its management application traffic (VSM, IQ-Server, etc.) at the data center.

This section summarizes an example logical network (VLAN) configuration, IP addressing, and DHCP pools for the CKC SnS Solution network. Table 11 is an example list of VLANs implemented for this system validation.

Table 11 Example of Solution Networking (VLAN Segmentation)

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Purpose</th>
<th>Network/Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>350</td>
<td>Video Analytics Camera Endpoints (IPVC8030)</td>
<td>172.16.128.0/26</td>
</tr>
<tr>
<td>400</td>
<td>Device Management VLAN</td>
<td>172.16.20.0/24</td>
</tr>
<tr>
<td>700</td>
<td>Data Center VLAN</td>
<td>172.16.25.0/24</td>
</tr>
</tbody>
</table>

Note: The VLANs shown in Table 11 are only the examples that are used in this solution validation. VLAN numbering and system networking may vary based on your actual deployment.
Table 12 is an example of DHCP pools that need to be created in the system:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Pool Network</th>
<th>Excluded Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Pool for Camera endpoints IP addressing</td>
<td>172.16.128.0/26</td>
<td>172.16.128.1-172.16.128.10</td>
</tr>
</tbody>
</table>

Configure Solution Networking

This chapter provides the implementation of VLANs and Layer 3 logical interfaces on network devices at each layer of the Cities Safety and Security Solution network topology, as shown in Figure 9, includes the following major topics:

- **Street Layer, page 35**
- **City Layer, page 37**
- **Internet Services/Data Center Layer, page 43**

Street Layer

This section provides the implementation of Industrial Ethernet access switches in the Street Layer of the Safety and Security Solution network topology, as shown in Figure 9.

Cisco Industrial Ethernet Switch (Cisco IE 4000)

These Cisco Industrial Ethernet switches are acting as access layer switches and providing wired internet access and PoE power to Cisco cameras in the Safety and Security solution. This section covers the implementation of Cisco IE 4000 switches that are shown in the Access/Street Layer of the Solution Network Topology in Figure 11.

Figure 11  Cisco IE 4000 Configuration Flow for Cities Safety and Security

Configuring Network Layer 2 and Layer 3

This section defines the implementation of VLANs on the Cisco IE 4000 switch. The following VLANs are required on the Cisco IE 4000 switches:

- **VLAN 350**—Camera VLAN
- **VLAN 400**—Management VLAN

1. Configure VLANs, which must be created on the Cisco IE 4000 switches:

   ```plaintext
   Cisco IE 4000-1(config)#vlan 350
   Cisco IE 4000-1(config)#vlan 400
   end
   ```

   **Note:** Repeat the step on all Cisco IE 4000 switches in the deployment based on the system networking configuration for your deployment. The above example configuration shows the Cisco IE 4000 switches configuration for the network topology in Figure 9.
Configure Solution Networking

2. Assign the ports to which cameras will be connected to the VLAN created in Step 1. For example:

   ```
   interface range GigabitEthernet 1/9 - 16
   switchport mode access
   switchport access vlan 350
   spanning-tree portfast
   
   Repeat this step for each Cisco IE switch in the Street Layer.
   ```

3. Configure the trunk ports at the uplinks. For example:

   ```
   interface range GigabitEthernet 1/1 - 2
   description ##TO Uplink##
   switchport mode trunk
   switchport trunk allowed vlan 350,400
   
   Repeat this step for each Cisco IE switch in the Street Layer on the appropriate ports.
   ```

Configuring Resilient Ethernet Protocol

The Resilient Ethernet Protocol (REP) is used to implement high availability at the Street Layer and involves the Cisco IE 4000 switches. REP provides a way to control network loops, handle link failures, and improve convergence time. It controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment.

A REP segment is a chain of ports connected to each other and configured with a segment ID. Refer to the topology diagram in Figure 9 to understand the REP segments configured in Cities Safety and Security. For more information about REP, REP segments, and their configuration, refer to REP at the following URL:


Complete the following steps to configure REP in Cisco IE 4000 switches:

1. Configure REP admin VLAN 400 on the global configuration. VLAN 400 is used for REP control plane communication:

   ```
   rep admin vlan 400
   ```

2. Assign the ports to rep segment 200 as per topology <topology no>:

   ```
   interface GigabitEthernet1/1
   rep segment 200
   
   interface GigabitEthernet1/2
   rep segment 200
   ```

3. Verify the REP topology by issuing the command given below:

   ```
   show rep topology
   ```

Note: Repeat the step on all Cisco IE 4000 switches in the deployment based on the system networking configuration for your deployment. The above example configuration shows the Cisco IE 4000 switches configuration for the network topology, as shown in Figure 9.
Configure Solution Networking

Configuring Quality of Service for Video

QoS refers to the ability of a network to provide improved service to selected network traffic such as video in case of Cities Safety and Security. In order to implement QoS, a class-map and a policy-map is created to classify traffic and to apply a policy to the traffic respectively. To learn more QoS and its configuration, refer to Configuring Quality of Service for Video, page 37.

Complete the following steps to configure QoS on Cisco IE 4000:

1. Create class map to match the video traffic:

   ```
   class-map match-any video
   match ip dscp 40
   ```

2. Create policy-map with this class-map for egress traffic to prioritize video traffic:

   ```
   policy-map video_prefer
   class Video
   priority
   police cir 300000000
   ```

3. Apply the policy on the egress interfaces:

   ```
   interface range GigabitEthernet1/1-2
   service-policy output video_prefer
   ```

City Layer

This section provides the implementation of the core/backbone network switches in the City layer of the Safety and Security solution network topology shown in Figure 12:

Configuring Aggregation Router ASR 920

Figure 12  City Layer Configuration Flow for Cities Safety and Security

Configuring Network Layer 2 and Layer 3

On the ASR 920, Ethernet Virtual Connection (EVC) service instances need to be configured in order for a port to carry Ethernet traffic. For details on configuring ASR 920 with EVC, please refer to the guide at the following URL:


For interfaces connected to Catalyst 4500-X switches, one ASR 920 service instance for EVC is configured to forward the traffic from the VLANs 100-900 in the network to the uplink switch 4500X.

For example, refer to the configuration below to configure service instance 100:

```
service instance trunk 100 ethernet
   encapsulation dot1q 100-900
   rewrite ingress tag pop 1 symmetric
```
Configure Solution Networking

```plaintext
bridge-domain from-encapsulation
!
!
interface TenGigabitEthernet0/0/12
description ##To-CAT4500 ##
service instance trunk 100 ethernet
  encapsulation dot1q 100-900
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation

interface TenGigabitEthernet0/0/13
description ##To-ASR-2##
no ip address
service instance trunk 100 ethernet
  encapsulation dot1q 100-900
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
!

Similarly, complete the configuration on the ASR 2 and 3.

Configuring Resilient Ethernet Protocol

ASR 920-1 is part of the following two REP segments:

- Segment 100 = Te0/0/12 and Te0/0/13
- Segment 200 = GigabitEthernet0/0/0

**Figure 13  REP Segments on ASR 920**

The bottom segment is for aggregating the traffic coming from the Street Layer and the top segment is for traffic going to the City layer. Segment Topology Change Notification (STCN) messages are sent from Segment 200 to Segment 100; all sub-REP rings should follow the same pattern.

1. Configure REP admin VLAN 400 on the global configuration. VLAN 400 is used for REP control plane communication:

   rep admin vlan 400

2. Configure REP segment 100 on Te0/0/12 and Te0/0/13:

   interface Te0/0/12
description ##To-CAT4500(1)##
   rep segment 100

   interface Te0/0/13
description ##To-ASR920(2)##
   rep segment 100
Configure Solution Networking

3. Configure REP segment 200 edge port on interfaces going toward Cisco IE 4000:

**ASR-920-1**

```plaintext
interface GigabitEthernet0/0/0
   description ##To-Cisco IE 4000(1)##
   rep segment 200 edge primary
```

**ASR-920-2**

```plaintext
interface GigabitEthernet0/0/0
   description ##To-Cisco IE 4000(3)##
   rep segment 200 edge
```

4. Configure REP STCN on all Edge interfaces on ASR-920 going toward Cisco IE 4000. STCN is configured for notifications to be sent from sub-segments to the main Segment 100:

```plaintext
interface GigabitEthernet0/0
   rep stcn segment 100
```

**Note:** The preceding configuration must be applied to other ASR 920 switches in the network.

5. Configure Load Balance in sub-segments primary edge ports comprised of Cisco IE 4000 subtended to ASR 920 switches. Video VLANs travel in clockwise direction and non-video VLANs travel in counter-clockwise direction. Video traffic in the VLAN 350 is configured to be allowed on the ASR 920 primary edge port on the REP segment 200, as shown in Figure 13:

```plaintext
interface GigabitEthernet0/0/0
   description ##To-Cisco IE 4000(1)##
   rep preempt delay 15
   rep block port id 0001BC16658A3100 vlan 350
```

Configuring Quality of Service for Video

This section describes QoS configurations on the ASR 920 as defined in this architecture's QoS design.

1. Create class-map to match the video traffic:

```plaintext
class-map match-all video
   match ip dscp 40

policy-map preserve
   class video
      set ip dscp 40
```

2. Create policy-map at the egress to allocate 30% of the bandwidth to the video traffic:

```plaintext
policy-map video_prefer
   class video
      bandwidth percent 30
```

3. Apply the egress and ingress policies on the appropriate egress and ingress interfaces:

```plaintext
interface TenGigabitEthernet0/0/13
   !
   service-policy input preserve
   !
interface TenGigabitEthernet0/0/12
   !
   service-policy output video_prefer
   !
```
Configure Solution Networking

Core/Aggregation Cisco Catalyst 4500-X Switch

The Figure 10 deployment model shows that the Cisco IE 4000 access switches are connected to the core/aggregation network switches.

The Catalyst 4500-X switch is used as an aggregation switch in the City layer. Network traffic from ASR 920 switches is aggregated at the Catalyst 4500-X switch and forwarded to the Data Center Layer. Several tasks are required to configure a Catalyst 4500-X. Figure 14 shows the work flow. Cisco Catalyst 4500-X switches are deployed in a pair, which provides network core, aggregation services, and Layer 3 routing functionalities for the Wi-Fi endpoints in the access layer. This section covers the implementation of the Cisco Catalyst 4500-X switch in the CKC Safety and Security Solution City layer.

Figure 14 4500X Configuration Flow for Cities Safety and Security

Configuring Network Layer 2 and Layer 3

This section defines the implementation of VLANs and Layer 3 logical interfaces on the Cisco Catalyst 4500-X switch.

1. Configure VLANs, which must be created along with port assignments on the Cisco Catalyst 4500-X switches:

   CSS-DS4500X-1(config)#vlan 350,400,700
   CSS-DS4500X-2(config)#vlan 350,400,700

2. Create the Layer 3 SVI for data VLANs. The example configuration below shows SVIs for the data VLANs and network management VLAN on the Cisco Catalyst 4500-X switches:

   CSS-DS4500X-1:
   
   interface Vlan350
       ip address 172.16.128.3 255.255.255.0
   
   interface Vlan400
       ip address 10.1.20.3 255.255.255.0
   
   interface Vlan700
       ip address 172.16.25.3 255.255.255.0

   CSS-DS4500X-2:
   
   interface Vlan350
       ip address 172.16.128.4 255.255.255.0
   
   interface Vlan400
       ip address 10.1.20.4 255.255.255.0
   
   interface Vlan700
       ip address 172.16.25.4 255.255.255.0

3. The Catalyst 4500-X is configured with two port-channels. One has member links to each Nexus 5000 switch, and the other has member links to the other Catalyst 4500-X for HSRP:

   interface Port-channel1
       description ##To-CAT4500(2)##
       switchport
Configure Solution Networking

```
switchport mode trunk
!
interface TenGigabitEthernet1/1
  switchport mode trunk
  channel-group 1 mode active
!
interface TenGigabitEthernet1/2
  switchport mode trunk
  channel-group 1 mode active
!
interface Port-channel2
  description #To-Nexus#
  switchport
  switchport trunk allowed vlan 300,400,700
  switchport mode trunk
!
interface TenGigabitEthernet1/3
  switchport trunk allowed vlan 300,400,700
  switchport mode trunk
  channel-group 2 mode active
!
interface TenGigabitEthernet1/4
  switchport trunk allowed vlan 300,400,700
  switchport mode trunk
  channel-group 2 mode active
```

4. Enable Rapid per-VLAN Spanning Tree:

```
spanning-tree mode rapid-pvst
```

5. Configure DHCP server for the cameras:

```
ip dhcp pool Camera_POOL
  network 172.16.128.0 255.255.255.192
  default-router 172.16.128.1
```

Note: It is recommended to use a centralized, enterprise-class Dynamic Host Configuration Protocol (DHCP) server to provide IP addresses to camera endpoints in the network. However, a local router-based DHCP server was used as an example implementation for solution validation.

Configuring Resilient Ethernet Protocol

1. Configure admin vlan for REP:

```
rep admin vlan 400
```

   This command specifies the VLAN that REP should be used to communicate to the other devices on the same segment.

2. Go into the respective interfaces and define the segment and the role of the interface and load balance traffic as Video VLAN. Video VLAN travels clockwise; non-video VLAN travels counter clockwise in the segment. The configuration is as follows:

   4500X-1:

```
interface TenGigabitEthernet1/5
  description #To-ASR920-1#
  rep segment 100 edge primary
  rep preempt delay 15
  rep block port id 0030B4C72260004C vlan 350
```
Configure Solution Networking

4500X-2:

```plaintext
interface TenGigabitEthernet1/5
description ##To-ASR920-3##
rep segment 100 edge
```

Configuring HSRP

The Catalyst 4500-X switch is the gateway for the access points and camera in Street Layer; therefore, HSRP is configured to provide redundancy at Layer 3. The HSRP configuration for the two switches follows:

On 4500X-1:

```plaintext
interface Vlan350
standby 11 ip 172.16.128.1
standby 11 priority 110
standby 11 preempt
```

On 4500X-2:

```plaintext
interface Vlan350
standby 11 ip 172.16.128.1
```

Configuring Quality of Service for Video

This section describes QoS configurations on the Catalyst 4500-X as defined in this architecture’s QoS design. Complete the following steps:

1. Create the class-map to classify video traffic:

   ```plaintext
class-map match-all video
   match ip dscp 40
   !
   
   2. Create policy-maps using the above created class-map to preserve the DSCP marking for the ingress and allocate 30% to video for the egress traffic:

   ```plaintext
   policy-map preserve
   class video
   set dscp 40
   policy-map video-prefer-egress
   class video
   bandwidth percent 30
   
   3. Apply the policies on the appropriate egress and ingress interfaces:

   ```plaintext
   interface Port-channel1
   service-policy input preserve
   service-policy output video-prefer-egress
   
   interface TenGigabitEthernet1/2
   service-policy input preserve
   service-policy output video-prefer-egress
   ```
Internet Services/Data Center Layer

Configuring Data Center Switch Nexus 5672

The configuration steps on the Nexus switch, as per the architecture, are shown in Figure 15:

Figure 15  Nexus Switch Configuration Flow for Cities Safety and Security

Configuring Network Layer 2 and Layer 3

This section defines the implementation of VLANs and the creation of Layer 3 logical interface on a Nexus switch pair:

1. Configure VLANs, which must be created along with ports assignment on both Nexus N5K-C5672UP switches, for example:

   CWIFI-NEX5672UP-1(config)# vlan 350,400,700

2. Create Layer 3 SVI interfaces:

   interface Vlan350
   ip address 172.16.128.5/24
   interface Vlan400
   ip address 172.16.20.5/24
   interface Vlan700
   ip address 172.16.25.5/24

Configure vPC

1. Enable features on the Nexus 5000 in configuration mode:

   feature lacp
   feature vpc

2. Configure the Management port on both Nexus pairs:

   interface mgmt0 /* on N5K-1 */
   ip address 1.1.1.1/30
   interface mgmt0 /* on N5K-2 */
   ip address 1.1.1.2/30

3. Configure the vPC peer-keepalive link in the vPC domain using a management network connection:

   N5K-1:

   vrf context management
   vlan 350,400,700
   vpc domain 90
   role priority 100
   peer-keepalive destination 1.1.1.2
N5K-2:

vrf context management
vlan 350,400,700
vpc domain 90
role priority 110
peer-keepalive destination 1.1.1.1

4. Configure port channels for vPC on Nexus 5000 switches:

interface port-channel7
    description UCS13 : VPC7
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    no negotiate auto
    vpc 7

interface port-channel8
    description ASA : VPC8
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    spanning-tree port type network
    no negotiate auto
    vpc 8

interface port-channel17
    description UCS11 : VPC17
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    speed 10000
    vpc 17

interface port-channel80
    description ASA2 : VPC80
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    spanning-tree port type network
    no negotiate auto
    vpc 80

interface port-channel101
    description Cat45001 : vpc101
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    spanning-tree port type normal
    no negotiate auto
    vpc 101

interface port-channel102
    description cat45002 : vpc102
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    spanning-tree port type normal
    no negotiate auto

5. Configure port channels for vPC Peer link on both Nexus 5000 switches:

interface port-channel4096
    description vPC PEER LINK
    switchport mode trunk
    switchport trunk allowed vlan 350,400,700
    vpc peer-link
    spanning-tree port type network
    no negotiate auto
6. Configure port channel member links on both Nexus 5000 switches:

**N5K-1:**

```plaintext
interface Ethernet1/1
  description vPC Peer link
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 4096 mode active

interface Ethernet1/2
  description vPC Peer link
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 4096 mode active

interface Ethernet1/3
  description cat45001 : po101
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 101 mode active

interface Ethernet1/4
  description cat45002 : po102
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 102 mode active

interface Ethernet1/7
  description Po7 : UCS
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  channel-group 7

interface Ethernet1/8
  description Po8 : ASA
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  speed 1000
  channel-group 8 mode active

interface Ethernet1/9
  description Po80 : ASA2
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  speed 1000
  channel-group 80 mode active
```

**Note:** The configuration is shown as plain text without the typical indentation used in actual configuration files.
Configure Solution Networking

N5K-2:

interface Ethernet1/1
  description vPC Peer link
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 4096 mode active

interface Ethernet1/2
  description vPC Peer link
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 4096 mode active

interface Ethernet1/3
  description cat45001 : po101
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 101 mode active

interface Ethernet1/4
  description cat45002 : po102
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  spanning-tree port type network
  channel-group 102 mode active

interface Ethernet1/7
  description Po7 : UCS
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  channel-group 7

interface Ethernet1/8
  description Po8 : ASA
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  speed 1000
  channel-group 8 mode active

interface Ethernet1/9
  description Po80 : ASA2
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  speed 1000
  channel-group 80 mode active

interface Ethernet1/17
  description Po17 : UCS11
  switchport mode trunk
  switchport trunk allowed vlan 350,400,700
  channel-group 17

Note: Verify the configuration using the following commands on both Nexus 5000 switches. The CLI commands are:
  show vpc, show vpc consistency-parameters <> , and show port-channel summary.
Configuring HSRP

The Nexus 5000 pair is configured with HSRP for the four Layer 3 SVIs created previously. This redundancy keeps Layer 3 Virtual IP (VIP) address available even if one Nexus box goes down. VIP will also be the default gateway for VLAN 400 and 700.

Configure the Hot Standby Router Protocol (HSRP) parameter under the SVI interface:

**N5K-1:**

```
interface Vlan350
    hsrp 8
    preempt
    priority 110
    ip 172.16.128.2

interface Vlan400
    hsrp 2
    preempt
    priority 110
    ip 172.16.20.1

interface Vlan700
    hsrp 5
    preempt
    priority 110
    ip 172.16.25.1
```

**N5K-2:**

```
interface Vlan350
    hsrp 8
    ip 172.16.128.2

interface Vlan400
    hsrp 2
    ip 172.16.20.1
interface Vlan700
    hsrp 5
    ip 172.16.25.1
```

**Note:** Use the `show hsrp brief` command to verify the active and standby switch.

Configuring Quality of Service for Video

The Nexus 5000 switch at the Data Center Layer also provides QoS features to classify the video traffic, prioritize the traffic flow, and provide congestion avoidance through egress queuing. The ingress traffic to Nexus 5K is classified using ingress classification policies and egress queuing is applied for video traffic to guarantee bandwidth and priority queuing for egress traffic, as defined in the architecture's QoS design considerations.

**Note:** The Nexus 5000 switch supports three QoS policy types: Network QoS, Queueings, and QoS. For detailed information on QoS and configuration syntax examples, refer to the following link:

Configure Solution Networking

The following steps describe the QoS implementation in the architecture’s data center Nexus switch:

1. Configure class-map to classify the video traffic:

   ```
   class-map type qos match-all video
   match dscp  40
   ```

2. Create policy-map for ingress and egress traffic to preserve the DSCP marking and to prioritize video traffic:

   ```
   policy-map type qos preserve
   class video
   set dscp  40
   ```

   ```
   policy-map type qos video_prefer_egress
   class video
   ```

   ```
   policy-map type queuing video_prefer_egress
   ```

   ```
   policy-map type queuing video_prefer_traffic
   ```

   ```
   class type queuing video
   priority
   bandwidth percent 30
   ```

3. Apply the policy on the appropriate ingress and egress interfaces:

   ```
   interface port-channel101
   service-policy type qos input preserve
   ```

   ```
   interface port-channel17
   service-policy type queuing output
   ```

   ```
   video_prefer_egress
   ```

Cisco ASA Firewall

In this architecture, ASA acts as a firewall and provides secure network access. Traffic flowing between networks passes through the ASA firewall. Also, traffic generated from all end devices (cameras) going to the data center, from the data center going to the Internet and return traffic for it passes through the firewall.

The ASA is configured to operate as follows:

- Firewall Mode: Routed
- Context: Single

However, in order to enable high availability on the ASA pair, as well as to enhance the throughput of the ASA pair, the ASAs are configured to be a part of a cluster. Clustering allows multiple ASAs to be grouped together as a single logical device.

Configuring Cisco ASA Firewall

**Figure 16  ASA Firewall Configuration Flow for Cities Safety and Security**

**Configuring Port-Channel**

A port-channel interface connects to the demilitarized zone (DMZ) network to provide Internet access to various devices in the system. During testing, the interface, called the DMZ Interface, is assigned a static IP address provided by the lab admin.
Configure Solution Networking

This interface is assigned the lowest security level because it is the least trusted interface. Its interface configuration is:

```plaintext
interface Port-channel2
  nameif DMZ-Interface
  security-level 0
  ip address 173.39.13.86 255.255.255.248
```

Before configuring clustering, we will configure only the port-channels.

**Note:** Do not configure the IP address and other interface details before configuring clustering. Configure only the port channel configuration.

The port-channel configurations:

```plaintext
interface GigabitEthernet1/0
  channel-group 1 mode active
  no nameif
  no security-level
  no ip address

interface GigabitEthernet1/1
  channel-group 1 mode active
  no nameif
  no security-level
  no ip address

interface GigabitEthernet0/2
  channel-group 2 mode active
  no nameif
  no security-level
  no ip address

interface GigabitEthernet0/3
  channel-group 2 mode active
  no nameif
  no security-level
  no ip address

interface GigabitEthernet1/2
  channel-group 3 mode on
  no nameif
  no security-level
  no ip address

interface GigabitEthernet1/3
  channel-group 3 mode on
  no nameif
  no security-level
  no ip address
```

**Note:** The port-channel interface for the Cluster Control Link (CCL) has to be created on each member separately. LACP may be used for quicker failure detection or static “on” mode for less complexity. The example above uses the “on” mode.

Configure Adaptive Security Appliance (ASA) Clustering

This architecture uses the Adaptive Security Appliance (ASA) platform’s clustering feature in order to enable scalability in addition to high availability. ASAs in a cluster will yield a performance of approximately:

- 70% of the aggregated throughput
- 60% of the number of concurrent connections
- 50% of the connection rate in connections per second
Configure Solution Networking

**Note:** Before starting the configuration, ensure that you have console access to both the ASAs.

The two ASAs in this architecture are configured as an ASA cluster with the following configuration:

- On each device, a minimal bootstrap configuration is configured, including the cluster name, cluster control link interface, and other cluster settings.
- The Spanned EtherChannel interface mode has been used in this architecture.

To understand the interface modes available and their features, refer to the following link:


Run the following command:

```
cluster interface-mode spanned check-details
```

The running configuration on the ASA is checked for incompatible commands and a warning prompt will indicate conflicts and available options.

**Note:** Do not bypass the check and force the mode change.

After reviewing the incompatible commands in the previous step, force the interface mode to Spanned-EtherChannel mode using the following command:

```
cluster interface-mode spanned force
```

In order to convert all the port-channels to spanned-EtherChannels, add the following command to the Port-Channel interface configuration:

```
interface Port-channel1
  description To N5K
  lacp max-bundle 8
  port-channel span-cluster
  no nameif
  no security-level
  no ip address
```

Add the commands to all the port-channels that have been configured to be data interfaces; that is, Port-channel1 and Port-channel2.

**Note:** Do not configure the CCL - Port-channel3 as a spanned-EtherChannel. Configure the ASA that will become the master of the cluster:

```
cluster group cwifi
  key <cluster-key> -> Optional
  local-unit asa1
  cluster-interface Port-channel5 ip 99.99.99.1 255.255.255.0
  priority 1
  health-check holdtime 3
  lacp system-mac auto system-priority 1
  mtucluster 1600
  enable
```

Since all units in the cluster have the same configuration as others and actively pass traffic, in the event of a unit failure, connectivity is maintained through the cluster thanks to connection information being replicated to at least one other unit in the cluster. Each connection has a replicated connection residing on a different cluster unit and takes over in case of a failure. This ensures that practically no traffic disruption occurs when one unit in the cluster fails. To add the second unit to the cluster, the Port-Channel for the CCL needs to be created on it and the following commands need to be configured:
Configure Solution Networking

```plaintext
cluster group cwifi
key *****
local-unit asa2
cluster-interface Port-channel5 ip 99.99.99.2 255.255.255.0
priority 100
enable

Note: Add the slave unit to the cluster after completing all configuration on the master since the slave will replicate the configuration from the master.

Configure Interfaces

VLAN sub-interfaces provide access to different components in the network, such as the data center and management network. Sub-interfaces based on VLANs are configured on the Port-Channel; each is given a unique name and an appropriate security level.

A VLAN and sub-interface configuration for management network access follows:

```plaintext
interface Port-channel1.400
vlan 400
nameif Management
security-level 100
ip address 172.16.20.9 255.255.255.0
```

The following is a VLAN and sub-interface configuration for data center access on the firewall:

```plaintext
interface Port-channel1.700
vlan 700
nameif DataCenter
security-level 90
ip address 172.16.25.2 255.255.255.0
```

The following is an interface configuration for the ISP/DMZ interface:

```plaintext
interface Port-channel2
lacp max-bundle 8
port-channel span-cluster
no nameif
no security-level
no ip address

interface Port-channel2.254
vlan 254
nameif DMZ-Interface
security-level 0
ip address 173.39.13.86 255.255.255.248
```
Configure Solution Networking

Other Settings

Other basic settings need to be added, such as the following:

- Hostname
- Routing

Hostname

The following is the hostname used in this guide:

```bash
hostname ASA5545-2009
```

Routing

In order for iOmniscient to be able to reach the Internet, the static route is configured as follows:

```bash
route DMZ-Interface 0.0.0.0 0.0.0.0 173.39.13.81 1
```

Network Address Translation

Network objects simply specify the networks or host IP addresses used in Network Address Translation (NAT) statements. Network objects make configurations more readable. The network object that we have used is as follows:

```bash
object network iOmni
host 172.16.25.22
```

NAT Statements

Our configuration uses the following NAT statement to translate the source IP address of iOmniscient from UCS to the DMZ-interface:

IP address:

```bash
object network iOmni
nat (UCS,DMZ-Interface) static interface 3-78
```
Onboarding a New Cisco Video Camera (IP Camera 8030)

The Cisco Video Surveillance 8030 (indoor/outdoor) IP Cameras are high-definition, full-functioned video endpoints with industry-leading image quality and processing power. To find out more about the camera, refer to the “Overview” section of the Cisco Video Surveillance 8020/8030 IP Camera Reference Guide at the following URL:


**Note:** It is recommended to enable the 802.1x authentication method for Cisco Video Surveillance 8030 IP Cameras in the network for network and device security. However, this implementation does not cover 802.1x for the purpose of solution validation. Refer to the following document for more details on 802.1x Port-based authentication of cameras in the network:


The following section describes the initial installation of Cisco Video Surveillance 8030 IP Cameras:

1. Refer to the “Performing the Initial Setup of the IP Camera” section of the Cisco Video Surveillance 8020/8030 IP Camera Reference Guide at the following URL:

2. Log in to the camera and select the enable QoS/DSCP. Enter 40 as the **DSCP** value, as shown in Figure 17:

![Figure 17 Enabling DSCP Marking for Camera Traffic](image)

In addition to the above mentioned steps, the following steps are recommended on Cisco Video Surveillance 8030 IP Cameras for the Facial Recognition feature:

1. From **Configuration**, navigate to **Media > Video** and click **Mode**. Select the **5 Megapixel** radio button, as shown in Figure 18 (if not already selected).
2. Next select **Stream 2** by clicking on the viewing window and selecting the **Stream 2** from the drop-down menu.

3. Next adjust the border to crop the view to focus on the desired area and resolution 1280X960, as shown in Figure 19. Finally click **Save**.

---

**Figure 18** Enabling 5 Megapixel Mode

**Figure 19** Cropping the View to 1280 x 960
Physical Camera Placement

For information on camera placement, please refer to Camera Placement, page 7.

Installation of Cisco Video Surveillance Solution

Cisco VSM is a comprehensive system for video surveillance needs. This system enables the network and security teams to collaborate effectively in a highly scalable environment combining both video and network techniques to optimize the experience. Cisco Video Surveillance Operations Manager (VSOM) provides a highly secure web portal to configure, manage, display, and control video in an IP network, and allows an easy management of a large number of security assets and users, including media servers, cameras, encoders, and event sources. To read more about Cisco VSM, refer to the “Cisco Video Surveillance Manager” data sheet at the following URL:


This chapter includes the following major topics:

- Installation of Cisco Video Surveillance Manager on the UCS Platform, page 55
- Installation of Cisco Safety and Security Desktop (SASD), page 55
- Configuring Video Surveillance Manager for Cities Safety and Security, page 56
- Obtaining the Video Wall on SASD for Cities Safety and Security, page 61

Installation of Cisco Video Surveillance Manager on the UCS Platform

Refer to the steps in the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms, Release 7.x for installing Cisco VSM on the UCS platform at the following URL:


Installation of Cisco Safety and Security Desktop (SASD)

A Cisco Safety and Security Desktop (SASD) is a full-featured monitoring application that provides access to the cameras and video from a single Operations Manager. Cisco SASD is used in Cities Safety and Security to monitor live or play back recorded video in single- or multi-pane views based on camera and to monitor and manage alerts and events in association with cameras. To read more about Cisco SASD, refer to the Cisco Video Surveillance Manager Safety and Security Desktop User Guide at the following URL:


This section includes the steps for installing the Cisco SASD.

Refer to the “Installing the Cisco SASD Application Suite” section of the Cisco Video Surveillance Manager: Install and Upgrade Guide, Release 7.7 and higher.
Configuring Video Surveillance Manager for Cities Safety and Security

This section details how VSM is configured in Cities Safety and Security. Configuring VSOM for Cities Safety and security involves the following major steps:

1. Creating a template for the cameras
2. Adding the camera with this template

Creating a Template

Create the template for the cameras using the following steps:

1. In the Camera menu, choose Template.
2. From the left panel, choose Add.
3. In the General tab, enter the template name, location, and model name (an example is shown in Figure 20):

![Figure 20 Example of Creating a Template](image-url)
In the **Streaming, Recording and Events** tab, enable the 24 x 7 recording for Video Stream A, retaining the recording for 1 day, as shown in Figure 21:

**Figure 21 Streaming, Recording and Events Tab**

For Stream A and B, click **Custom** and enter the values. Click **Set**. Figure 21 shows an example. Refer to Table 13 for the recommended values.

**Note:** In our setup, we have recorded the Video Stream A with a resolution of 1920 X 1080. Video Stream B is of a lower resolution and is used for analytics purpose. Alternatively, either of the streams can be used for analytics and recording purposes.

For using Facial Recognition, we recommend using HD resolution for accuracy. Using a higher resolution can increase the chance to detect faces in longer distance, but this will also cause higher CPU usage. Faces can be detected with as low as 4CIF because the iQ System requires 22–25 pixels between the eyes to recognize the person, but the person needs to stand as close as a 1 meter distance for a low resolution to be recognized.

**Figure 22 Custom Settings Example**
4. Finally click **Create**. The created template should appear on the left under the list of templates, as shown in Figure 23.

**Figure 23  Created Template Displays on the Left**

The recommended profile for running it in the best possible way for this setup includes a FPS value of 8.

**Table 13  Resolution with Recommended Bit Rate**

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Bit-Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>4CIF</td>
<td>1000</td>
</tr>
<tr>
<td>1MP</td>
<td>1000</td>
</tr>
<tr>
<td>1920X1080</td>
<td>2000</td>
</tr>
</tbody>
</table>
Figure 24 shows the template settings that are necessary for the Facial Recognition feature:

**Figure 24  Template Settings for Stream 2 of Facial Recognition Cameras**

![Custom Quality Setting]

**Note:** Using a high frame rate causes a lag in the video feed observed on iOmniscient. Although different products in the iQ-Series require different frame rates, it can be broadly said that the iOmniscient detection algorithms are required to analyze a minimum of 6fps. On the other hand, few products are only required to analyze a minimum of two (2) frames per second. The minimum FPS settings are the default frame rates set under the Frame rate setting of the iOmniscient; therefore, a template FPS value of 8 is recommended as the setting for running the cameras.

To understand more in depth about the recommended frame rate setting for running the cameras, please refer to the “Frame Rates” section of the *iQ Series User Help Manual v4.7*. 

Adding Cameras

Add the cameras using the following steps:

1. Under the **Camera** menu, select **Camera** and click **Add** from the left window.
2. Enter the details as shown in Figure 25 and then click **Add**.

**Figure 25  Example of Adding a Camera in VSOM: Camera Details**

3. Once the camera is added, verify the status of the added camera as shown in Figure 26.

**Figure 26  Example of Adding a Camera in VSOM: Verifying Camera Status**
Obtaining the Video Wall on SASD for Cities Safety and Security

1. Run the SASD application by clicking the shortcut from the desktop.
2. Enter the server IP, username, and password.
3. Click Login.
4. Click the Video tab and select the camera for which the feed has to be seen.
5. Drag and drop the camera to the wall to see the video feed from the camera, as shown in Figure 27:

Figure 27 Viewing Video on SASD Wall

This completes the configuration of VSOM and SASD.
Installation of iOmniscient Video Analytics

iOmniscient provides intelligent video analytics/surveillance. In Cities Safety and Security, the iOmniscient analytics is used to generate alerts when an unwanted event happens in the area under surveillance. To read more about iOmniscient, refer to iQ-Smart City Security - Safety - Service: A guide on how to maximize the value of your investment in a Smart City System at the following URL:


This chapter includes the following major topics:

- Installation of iOmniscient Video Analytics Server, page 62
- Configuring Object Detection Sensitivity on the Camera, page 63
- Configuring Video Surveillance Manager for Cities Safety and Security, page 64
- Scheduling iQ-Server Restart, page 64
- Configuring iOmniscient to Send Public IP in the Alert instead of the Private IP, page 69

Installation of iOmniscient Video Analytics Server

Refer to the Installation subsection in the “Getting Started” section of the iQ Series User Help Manual v4.7.

Configuring iOmniscient Video Analytics Server for Cities Safety and Security

To set up the Cisco Camera in the IQ Client, complete the following steps:

1. To add a camera, right-click **Server** and select **Add Camera**, as shown in **Figure 28**.

![Figure 28 Example of Adding a Camera in iOmniscient](image)

2. Select product type, input camera name, select video input type as **VMS Protocol**, and select brand name as **Cisco VSM 7x**.

3. Click the folder icon to input channel details, enter the Cisco server IP, enter the proxy name (with which the camera is created in the Cisco VSM server), enter the Cisco server username, password, and stream number, and then click **OK**.
Installation of iOmniscient Video Analytics

Figure 29 Example of Adding a Camera in iOmniscient

4. Proceed with Camera Enable and select the drive. Additionally, check the Variable resolution if configuring the camera for Facial Recognition.

5. Now you can set up an Area of Interest (AOI). For information on how to do this, refer to the Areas (of Interest) section of the iQ Series User Help Manual v4.7.

6. If you do not wish to create an AOI at this time, click Start.

7. On the right pane, click Live View. You should be able to see the live feed from the camera in the right pane (also referred to as main panel).

8. Click Apply and then click OK. A dialog box will display.

9. Click Yes.

Figure 30 Completing the Addition of a Camera in iOmniscient

Configuring Object Detection Sensitivity on the Camera

This section will cover how to add a camera and enable the Object Detection feature on it.

1. Add the camera by following Steps 1 to 4 of Configuring iOmniscient Video Analytics Server for Cities Safety and Security, page 62 and then choosing IQ-180 as the product type.

2. Click Start in the left panel.

3. In the right panel, click Live View. You should be able to see the live feed from the camera in the main panel.
Installation of iOmniscient Video Analytics

4. Enter the area name in the Area name section of the right pane and then click New.

5. Draw the Area of Interest by dragging and drawing a rectangle/polygon. Refer to the Areas (of Interest) section of the iQseries help guide for more in depth steps.

6. From the list of products, click the Object Detection checkbox.

7. Finally click Apply and then click OK.

The other features can be added in a similar way. To see more in-depth steps to add the features/product to the camera, refer to the product-specific settings in the iQ Series User Help Manual v4.7.

Configuring Video Surveillance Manager for Cities Safety and Security

The alerts sent by the iOmniscient system can also be received and viewed at the SASD. Refer to the “Setup Cisco Soft Trigger 7.x” section to set up VSOM to receive the alert. Also, refer to the “Setup notification on IQ Server” section to set up IQ Server to send the alerts to VSOM.

Scheduling iQ-Server Restart

In order for the iQ-Server to receive constant video feed, an automatic restart of the iQ-Server must be scheduled. This can be performed by completing the following steps:

1. Ensure that you have the IQService.bat file obtained from iOmniscient.

2. From Control Panel > System, select Security. Click the Schedule Task under Administrative Tools. Refer to Figure 31:

Figure 31  Scheduling iQ-Server Restart
3. Click **Create Basic Tasks**, as shown in **Figure 32**.

**Figure 32  iIQ Server Restart: Creating a Basic Task**

4. Enter the details as shown in **Figure 33**:

**Figure 33  iQ-Server Restart: Details**

5. After entering the details under **Name** and **Description**, click **Next**.

6. Select the **Daily** option under **Trigger** and then click **Next** again, as shown in **Figure 34**:

**Figure 34  Scheduling iQ-Server Restart: Selecting Trigger**
7. Enter the time **23:00** and the daily recurrence should be **1**. Then click **Next**, as shown in **Figure 35**.

**Figure 35  Scheduling iQ-Server Restart: Schedule**

![Create Basic Task Wizard]

8. Select **Start a Program** for the **Action**, and then click **Next**, as shown in **Figure 36**:

**Figure 36  Scheduling iQ-Server Restart: Selecting an Action**

![Start a Program Selection]
9. Browse and select the file path for the iQservice.bat file provided by iOmniscient and then click **Next**, as shown in Figure 37. Refer to References, page 87 for the content of the iQservice.bat.

**Figure 37  Scheduling iQ-Server Restart: Program Script**

Note: If any queries occur with the script file, iOmniscient help must be sought.

10. Click **Finish**. A Windows scheduler task will be created for the restart process every day at 23:00, as shown in Figure 38.

**Figure 38  Scheduling iQ-Server Restart: Finishing**
11. After clicking **Finish**, the task scheduler main window will display. Check for the task that you created with your customized name (in this case, we have created an IQ Server Restart) and double-click it. The **iQ-Server Restart Property Dialog Box** will display. Then select the **Run whether the user is online or not** option and click **OK**, as shown in **Figure 39**.

**Figure 39  Scheduling iQ-Server Restart: Security Options**

![Create Basic Task Wizard](image)

**Note:** Due to the restart of the IQ Server, the feed/analytics will pause for the duration of the restart.

**Note:** In the above configuration, the IQ Server is configured to restart at 23:00 Hrs. However, any other timing can be chosen alternatively, as per requirements.
Configuring iOmniscient to Send Public IP in the Alert instead of the Private IP

By default, the iOmniscient server sends the internal IP of the server in the alert URL that are sent to the CKC. In order for iOmniscient server to send a public IP in the alerts, the following steps must be followed:

1. Navigate to Preferences and select Server Settings.
2. In the Server Settings menu, click Product Specific and choose Alarm Streaming, as shown in Figure 40:

![Figure 40 Configuring iQ-Server to Send Public IP in the XML Alerts](image)

3. Enter the Public IP in the IP address box and port 80, as shown in Figure 40.
4. The alert sent will now have the public IP in the Image Alert and Video Alert URL.

Integration of CKC with iOmniscient Video Analytics Server

This chapter includes the following major topics:

- CKC Configuration Prerequisites, page 70
- Registering CKC Callback URL on iOmniscient Application, page 71

CKC Safety and Security solution use cases are implemented by integrating the Cisco Kinetic for Cities Cloud application instance with the iOmniscient Video Analytics Server on the City Data Center. This is achieved by configuring:

1. CKC Safety and Security (SnS) extension for iOmniscient Provider
2. CKC Callback URL registration on iOmniscient IQ-Server
CKC Configuration Prerequisites

**Note:** It is assumed that the customer already has a CKC instance/tenant provisioned to implement the Safety and Security domain in that existing CKC tenant/instance. If not, it is crucial to get the CKC tenant/instance created first with the help of Cisco CKC Cloud Operations team before configuring the Safety and Security domain in that CKC tenant/instance, as stated in this section.

The Cisco CKC Cloud Operations team configures the CKC Safety and Security Extension for integrating the CKC tenants with the iOmniscient Video Analytics server for end-to-end solution use cases. Therefore, the following details from the iOmniscient application server are provided to the CKC Operations team to configure the SnS extension.

### iOmniscient Video Analytics Application Server ID

1. Public IP (NAT) address of the iOmniscient application server instance at City network.

2. Camera ID and name as configured in the iOmniscient application along with camera location name and lat/long values.

*Table 14* provides an example of iOmniscient application details at the City network to be shared with the CKC Operations team for the SnS extension configuration.

<table>
<thead>
<tr>
<th>Server ID</th>
<th>TCP Server Host, Port</th>
<th>Public IP address of the iOmniscient Server which is reachable from CKC application on cloud</th>
<th>Camera Name</th>
<th>Camera ID</th>
<th>Use Case</th>
<th>Location Name</th>
<th>Latitude/ Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>12349876</td>
<td>173.39.15.80, 80</td>
<td></td>
<td>8030_5stream1</td>
<td>0</td>
<td>Suspicious Object (Object Detection)</td>
<td>BGL12-lab</td>
<td>12.001234/ RET 77.456789</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030_6 stream1</td>
<td>1</td>
<td>Suspicious Object (Object Detection)</td>
<td>BGL12-corridor</td>
<td>12.001235/ RET 77.456780</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030_6stream2</td>
<td>2</td>
<td>Suspicious Object (Object Detection)</td>
<td>BGL12-breakout</td>
<td>12.001236/ RET 77.456781</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030_7stream1</td>
<td>3</td>
<td>Intrusion Detection</td>
<td>BGL11-lab</td>
<td>12.001237/ RET 77.456782</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030_7stream2</td>
<td>4</td>
<td>Intrusion Detection (Perimeter Protection)</td>
<td>BGL11-corridor</td>
<td>12.001238/ RET 77.456783</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030_4stream2</td>
<td>5</td>
<td>Intrusion Detection</td>
<td>BGL11-breakout</td>
<td>12.001239/ RET 77.456784</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030_8stream1</td>
<td>6</td>
<td>Person Identified (Facial Recognition)</td>
<td>BGL12-Lobby</td>
<td>12.001230/ RET 77.456785</td>
</tr>
</tbody>
</table>

**Obtaining the iOmniscient Application Server ID**

Complete the following steps to obtain the iOmniscient Application Server ID:

1. On the iOmniscient Server (IQ-Server) Windows System, open a Windows command prompt from the application start menu.

2. Enter the command `sqlcmd` on the user command prompt:

   ```
   C:\Users\admin>sqlcmd
   ```
3. Enter the following SQL command to retrieve the server ID from the system database:

```
1> select [serverid] from [iqsys].[dbo].[systemstatic]
2> go
serverid
----------
12349876
(1 rows affected)
```

4. Note this server ID for configuring CKC SnS Extension. Enter **quit** to exit from SQL command prompt.

Registering CKC Callback URL on iOmniscient Application

An HTTPS callback URL provided by the CKC Operation team is configured on the iOmniscient application server to validate and register the CKC URL to receive incident alerts raised upon video feed analysis from the iOmniscient application.

**Note:** Make sure to get the CKC Callback URL from the CKC Operations team after configuring the CKC instance SnS extension for integration with iOmniscient server.

The iOmniscient Application Server (IQ-Server) pushes the alarms raised upon the occurrence of the incident to the CKC SnS Extension. The CKC extension engine processes the alarms received from IQ-Server. CKC dashboard notifies the alarms as “Notification” messages and “Alerts” for each use case incident, i.e., Suspicious Object, Intrusion, Person Identified, etc.
Complete the following steps to register the CKC POST URL on the iOmniscient Application Server (IQ-Server):

1. On the iOmniscient Client (IQ-Client) Windows System, from **IQ-Server Name > Camera Name** in the left pane, select the camera name for which alarms are to be pushed to CKC, from the left pane view.

2. Navigate to the **Notification > XML** tab in the right panel, as shown in Figure 41:

**Figure 41  iOmniscient Client Camera Configuration Window**
3. Enter the CKC Callback URL in the **IP Address** field (highlighted in the red rectangle) and **Port number** (80), as shown in Figure 42. Then click **Test Connection**. After a successful test connection, the **Sending Test Event Done** message must display.

**Figure 42** iOmniscient Client Camera Configuration Window for CKC Integration
4. Click **Save**. The CKC extension callback URL must appear in the right panel, as shown in Figure 43 (highlighted in the red rectangle):

**Figure 43 Registered CKC Callback URL on iOmniscient Camera Configuration**

The above steps complete the integration of the CKC Cloud application with the iOmniscient Video analytics application server (IQ-Server) on the City Data Center.

**Cisco Kinetic for Cities Provisioning**

This chapter includes the following major topics:

- Configuring CKC Users and Roles, page 75
- Safety and Security Use Cases, page 77
- Configuring Safety and Security Reports, page 86

Safety and Security solution use cases are enabled on CKC by provisioning CKC with specific functionality for Tenants, Domains, Policy, Reporting, and Device Engines. The CKC software platform has Create, Remove, Update, and Delete (CRUD)-based functionality that relates to a standard software platform.

The configuration of tenants, domains per tenant, and CKC tenant operator user are performed by the CKC operations team on the cloud CKC instance using administrator/super user rights.

**Note:** Safety and Security solution use case navigation on CKC dashboard is generally performed using the CKC Operator user role. If you need to configure additional users, you would need CKC administrator user credentials for your tenant provided by the CKC operations team.
Configuring CKC Users and Roles

By default, the CKC operations team creates a user with operator rights for you to log on to the CKC dashboard to see domain-specific features/use cases enabled for that tenant. If additional users are required to be created, you must log in as the CKC administrator user with privileges to create/modify/delete users for a tenant. For step-by-step instructions on creating/modifying/deleting users, refer to the “Creating Users” section in the CKC Dashboard Administrator Guide provided by the CKC Operations team.

Figure 44 shows an example list of users created for a region in CKC tenant:

![Figure 44 Adding and Updating New Users with CKC Dashboard Administrator Login](image)

Configuring CKC User Roles and Regions

User roles determine tabs and domains access permissions for the user logging on to CKC Dashboard. Creation of new roles and access permission configuration is performed by the CKC Operations team as per your requirements. For more details on roles, refer to the “Role Assignment” section of the CKC Dashboard Administrator Guide provided by the CKC Operations team.
Figure 45 shows an example role assignment for the “blroperator” user:

**Figure 45  Example User Role Assignment**

Once the administrator has created the user and mapped them to a User Role, they can then provide the hierarchical access for different locations present in the CKC for the same tenant. Depending on the position or location, the user profile can be assigned a specific location so that only the assigned location is accessible when the user is logging in with those credentials. Location in this context refers to the position of a tenant, as shown in Figure 46. Assign Location to a tenant is used in CKC dashboard to position a location (region defined) within a Tenant.

For more details on region mapping to the users of a tenant, refer to the “Location Assignment” section in the CKC Dashboard Administrator Guide provided by the CKC Operations team. Figure 46 shows an example region mapping or location assignment for a tenant user:

**Figure 46  Mapping Location to Tenants and Regions for Administrator User Profile Management**
Safety and Security Use Cases

This section covers the steps to navigate the CKC dashboard to obtain the details of the following Safety and Security (iOmniscient provider) use cases implemented on the CKC 4.0 release:

1. Suspicious Object Detection Alerts and Notifications configured per camera on the Street Layer
2. Intrusion/Perimeter Protection incident alerts and notifications configured per camera on the Street Layer
3. Person Identified Alerts and notifications using iOmniscient Facial Recognition analytics configured per camera

Getting Suspicious Object Detection Notification and Alerts

CKC Safety and Security solution use cases depend on the video stream from the Cisco IP Cameras on the City Street Layer. The iOmniscient iQ-Server in the City Data Center receives the live video stream of the camera via Cisco VSM. The IQ-Server analyzes the live video feed for the configured analytics feature and raises real time incident alarms to CKC.

The CKC dashboard provides notification of configured incident alarms along with alerts for the City Operator to act upon. Alerts are displayed on the CKC dashboard Map View on a per-camera basis based on the camera’s latitude/longitude values available in the alarms from the IQ-Server.

After integrating the CKC with the IQ-Server, the different incident notification and alerts are available in the CKC dashboard upon the occurrence of the incident(s).

Complete the following steps to navigate to Notification messages on the CKC dashboard:

1. Log in to the CKC dashboard as an Operator user (e.g., blroperator).
2. Click the Notification icon in the right top corner on the CKC dashboard. You will see a list of notifications received by CKC from different providers configured on that tenant, as shown in Figure 47:

Figure 47  CKC Dashboard Notification of Suspicious Object Detected on a Camera

The white rectangle in Figure 47 indicate a Suspicous Object notification received from the iOmniscient IQ-Server.
Complete the following steps to navigate **Suspicious Object Detection Alerts** on Map View:

1. Navigate to Map View > Module Layers > Safety & Security > Suspicious Object. You see a Map View with the details of all available cameras in the configured region, as shown in Figure 48:
2. When a camera is selected, the corresponding camera is highlighted in the Map View screen on the left. Figure 49 shows the Suspicious Object alerts on the Map View for Cameras in a region (example, Bangalore).

**Figure 49   CKC Dashboard Map View for Suspicious Object Detected for a Camera**

Complete the following steps to navigate to Safety and Security Alerts on the CKC dashboard:

1. Navigate to Alerts and select Safety & Security from the Module drop-down menu. You will see a list of all Alerts available for all cameras in the configured region, as shown in Figure 50:

**Figure 50   CKC Dashboard Alerts View for Suspicious Object Alerts**

2. Click the Alert image window to open/download a video clip of the Suspicious Object detected in a browser window.
Getting Intrusion Detection Notification and Alerts

Complete the following steps to navigate to Notification messages on the CKC dashboard:

1. Log in to the CKC dashboard as Operator user (e.g., blroperator).

2. Click the Notification icon in the right top corner on the CKC dashboard. You will see a list of notifications received by CKC from different providers configured on that tenant, as shown in Figure 51:

![Figure 51 CKC Dashboard Notification of Intrusion Detected on a Camera](image)

The white rectangle in Figure 51 indicate an Intrusion notification received from the iQ-Server.
Complete the following steps to navigate to Intrusion Detection Alerts on Map View:

1. Navigate to Map View > Module Layers > Safety & Security > Intrusion. You will see a Map View with the details of all available cameras in the configured region, as shown in Figure 52.

Figure 52  CKC Dashboard Map View for Intrusion Detected in a Region
2. When a camera is selected, the corresponding camera is highlighted in the Map View page on the left. Figure 53 shows the Intrusion alerts on the Map View for Cameras in a region (example: Bangalore).

**Figure 53** CKC Dashboard Map View for Intrusion Detected on a Camera Video

Complete the following steps to navigate to Safety and Security Alerts on the CKC dashboard:

1. Navigate to Alerts, and select Safety & Security from the Module drop-down menu. You will see a list of all Alerts available for all cameras in the configured region, as shown in Figure 54:

**Figure 54** CKC Dashboard Alerts View for Intrusion Detection Alerts

2. Click an Intrusion Alert image window to open/download the Intrusion event image in a browser window.
Obtaining Person Identified (Facial Recognition) Notification and Alerts

Complete the following steps to navigate to **Notification** messages on the CKC dashboard:

1. Log in to CKC dashboard as an Operator user (e.g., blroperator).

2. Click the **Notification** icon in the right top corner on the CKC dashboard. You will see a list of notifications received by CKC from different providers configured on that tenant, as shown in **Figure 55**:

**Figure 55**  CKC Dashboard Notification of Person Identified (Matched) on a Camera

The white rectangle in **Figure 55** indicates a Person Identified notification received from the iOmniscient IQ-Server.
Complete the following steps to navigate to **Intrusion Detection Alerts** on **Map View**:

1. Navigate to **Map View > Module Layers > Safety & Security > Person Identified**. You will see a **Map View** with the details of all available Cameras in the configured region for which alarms are raised, as shown in **Figure 56**:

![Figure 56 CKC Dashboard Map View for Person Identification in a Region](image-url)
2. When a camera is selected, the corresponding Camera is highlighted in the Map View page on the left. Figure 57 shows the Person Identified alerts on Map View for Cameras in a region (ex: Bangalore).

Figure 57  CKC Dashboard Map View for Person Identification on a Camera

Complete the following steps to navigate to Safety and Security Alerts on the CKC dashboard:

1. Navigate to Alerts > Safety & Security from the Module drop-down menu. You will see a list of all Alerts available for all cameras in the configured region, as shown in Figure 58:

Figure 58  CKC Dashboard Alerts View for Person Identification Alerts

2. Click a Person Identified Alert image window to open/download the matched person image in a browser window.
Caveats

Configuring Safety and Security Reports

This section covers the implementation of Safety and Security events and reports that are supported in CKC Dashboard Release 4.0.

Getting Object Detection and Intrusion Detection Reports

CKC helps enable customers to discover data patterns that were previously hidden through discovery, comparison, and correlation of data across various domains. You can generate an Object Detection and Intrusion Detection Event report that shows the average number of incidents at a given time for a region or point of interest sampled every minute for the day, week, month, or year.

Refer to the “Reports” and “Generating Reports,” and “Other Reports” sections in the Cisco Kinetic for Cities Dashboard User Guide for the step-by-step instructions on generating reports for the Safety and Security solution.

Caveats

Table 15 covers the list of open issues in the system and workarounds.

Table 15 Caveats and Workarounds

<table>
<thead>
<tr>
<th>Open Issues</th>
<th>Work around</th>
</tr>
</thead>
<tbody>
<tr>
<td>The image of the identified person in the FR alert cannot be obtained in a new browser window upon clicking the alerts on CKC dashboard if both the image and video URL box are checked against in the configuration to send an alert to CKC dashboard.</td>
<td>When configuring iOmniscient to send FR alerts to CKC, make sure to check against the image URL only. The video URL checkbox must remain unchecked on iOmniscient configuration.</td>
</tr>
<tr>
<td>Cameras, once added in iOmniscient system, receive a camera ID in the order of sequence in which they are added. Deleting a camera causes the corresponding ID to be deleted from the list of camera IDs, thus resulting in a non-consecutive list of camera IDs. Moreover, as CKC configs are based on camera IDs, a change in the camera IDs would have to be followed with a subsequent changes in the CKC configs. Therefore, to avoid this, deleting a camera is not recommended.</td>
<td>Once a camera is added, it should not be deleted. If required to add a different camera in its place, the Settings section of the same camera ID can be modified to replace the existing camera with a new one or the camera can be stopped.</td>
</tr>
<tr>
<td>Video feed from cameras in iOmniscient stop after nearly three days of continuous running of the IQ-server.</td>
<td>Configure a windows scheduler to restart the iQ-server automatically every day. For the detailed steps, refer to the Scheduling iQ-Server Restart, page 64.</td>
</tr>
<tr>
<td>Safety and Security average incident counts report (Object Detection &amp; Intrusion) on the CKC dashboard is referenced from the UTC time zone although it is queried for report from tenant’s local time zone. Therefore, there is a mismatch of how the data is reported in the Combo chart graph view.</td>
<td>Northbound API (NB API) for Safety and Security. ROI reports should be queried to get the valid data for the local time zone as needed. For example, if the tenant is in India Standard Time (IST) time zone, the NB API query to get the report data from data engine should be UTC+5.30 hours to get valid data for the local time zone.</td>
</tr>
<tr>
<td>The camera names on the CKC map view representation show an extremely long name that is not meaningful, therefore, making it difficult to isolate a particular camera.</td>
<td>Not Available</td>
</tr>
<tr>
<td>CKC dashboard live alarms are available with a limited lifespan on the CKC dashboard and alarms of past 24 hours are unavailable.</td>
<td>Not Available</td>
</tr>
</tbody>
</table>
References

The following documentation is referred to or used in this document:

- **Cisco Kinetic for Cities Dashboard User Guide**:  

- **Cisco Kinetic for Cities Dashboard Admin Guide**:  

- **Cisco Digital Network Architecture for Cities solution documents**:  

- **Catalyst 4500 Series Switch Software Configuration Guide, IOS XE 3.9.xE and IOS 15.2(5)Ex**:  

- **iQ Series User Help Manual v4.7**:  

- **iOmniscient Camera Placement Guide**:  
  - This guide can be obtained directly from iOmniscient.

The `iQservice.bat` file must be obtained from iOmniscient team; for reference, the following is the content of the file:

```
md c:\iOmniscient  
echo;>>c:\iOmniscient\Servicelog.txt  
echo %date% %time% Stop IQService >>c:\iOmniscient\Servicelog.txt  
taskkill /IM alertserver.exe /F /T >>c:\iOmniscient\Servicelog.txt  
timeout /t 10  
echo %date% %time% Start IQService >>c:\iOmniscient\Servicelog.txt  
net start IQsysServices >>c:\iOmniscient\Servicelog.txt
```

The above file must be saved as a batch file and used in the Step 8 of **Scheduling iQ-Server Restart, page 64**.

- **Cisco Kinetic for Cities DevNet**:  

- **Thing-Query-Language (TQL)**:  

**Note**: Some of the information listed above is only available to Cisco Channel Partners and Cisco personnel with a valid CCO login. Customers and other interested parties should contact their local Cisco distributor or Cisco Account Manager for additional details.
## Glossary

Table 16 is the list of acronyms and initialisms used in this document.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOI</td>
<td>Area of Interest</td>
</tr>
<tr>
<td>ASA</td>
<td>Adaptive Security Appliance</td>
</tr>
<tr>
<td>BaaS</td>
<td>Business as a Service</td>
</tr>
<tr>
<td>BoM</td>
<td>bill of material</td>
</tr>
<tr>
<td>CCL</td>
<td>Cluster Control Link</td>
</tr>
<tr>
<td>CIF</td>
<td>Common Interchange Format</td>
</tr>
<tr>
<td>CKC</td>
<td>Cisco Kinetic for Cities</td>
</tr>
<tr>
<td>CRUD</td>
<td>Create, Remove, Update, and Delete</td>
</tr>
<tr>
<td>CVD</td>
<td>Cisco Validated Design</td>
</tr>
<tr>
<td>DaaS</td>
<td>Domain as a Service</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarized zone</td>
</tr>
<tr>
<td>DSF</td>
<td>Dispersion-shifted Fibers</td>
</tr>
<tr>
<td>EVC</td>
<td>Ethernet Virtual Connection</td>
</tr>
<tr>
<td>FD</td>
<td>Facial Detection</td>
</tr>
<tr>
<td>FoV</td>
<td>Field of View</td>
</tr>
<tr>
<td>FPS</td>
<td>Frames Per Second</td>
</tr>
<tr>
<td>FR</td>
<td>Facial Recognition</td>
</tr>
<tr>
<td>GPL</td>
<td>Cisco Global Price List</td>
</tr>
<tr>
<td>HSRP</td>
<td>Cisco Hot Standby Router Protocol</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPVS</td>
<td>IP Video Surveillance</td>
</tr>
<tr>
<td>NAMS</td>
<td>Nuisance Alarm Minimization System</td>
</tr>
<tr>
<td>NAT</td>
<td>network address translation</td>
</tr>
<tr>
<td>NOC</td>
<td>network operating center</td>
</tr>
<tr>
<td>ONVIF</td>
<td>Open Network Video Interface Forum</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>PTZ</td>
<td>pan-tilt-zoom</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-based Access Control</td>
</tr>
<tr>
<td>REP</td>
<td>Resilient Ethernet Protocol</td>
</tr>
<tr>
<td>RTSP</td>
<td>Real Time Streaming Protocol</td>
</tr>
<tr>
<td>RTT</td>
<td>round-trip time</td>
</tr>
<tr>
<td>SASD</td>
<td>Cisco Safety and Security Dashboard</td>
</tr>
<tr>
<td>SFSE</td>
<td>Static Face Search Engine</td>
</tr>
<tr>
<td>SnS</td>
<td>Safety and Security</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>secure socket layer</td>
</tr>
<tr>
<td>STCN</td>
<td>Segment Topology Change Notification</td>
</tr>
<tr>
<td>TaaS</td>
<td>Things as a Service</td>
</tr>
<tr>
<td>VBR</td>
<td>Variable Bit Rate</td>
</tr>
<tr>
<td>VIP</td>
<td>Virtual IP</td>
</tr>
<tr>
<td>VSM</td>
<td>Cisco Video Surveillance Manager</td>
</tr>
<tr>
<td>VSOM</td>
<td>Cisco Video Service Operation Manager</td>
</tr>
</tbody>
</table>
Glossary