Cisco Physical Security Operations Manager 6.1

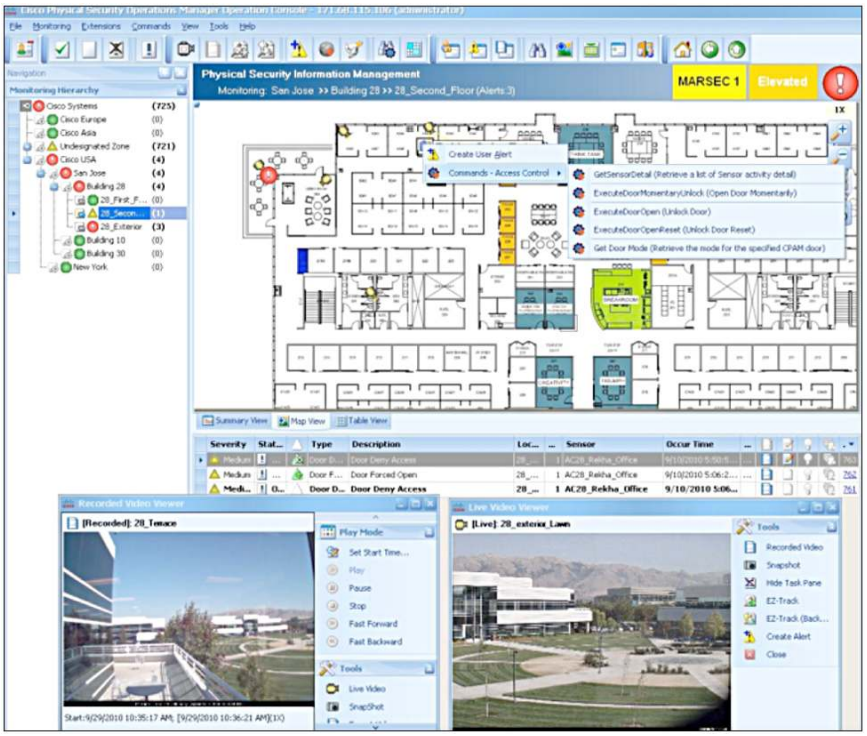
The Cisco® Physical Security Operations Manager is a scalable command-and-control-style operator console. It unifies management and operation of Cisco Video Surveillance Manager, Cisco Physical Access Manager, and the Cisco IP Interoperability and Collaboration System (IPICS).

The Physical Security Operations Manager integrates security alarms and events from multiple sources, consolidates device management into a single location, and displays information on easy-to-use and intuitive maps. It provides efficient data visualization and allowing easy access to live and stored video and access-controlled doors (Figure 1).

Powered by a sophisticated business logic engine, the Physical Security Operations Manager allows users to create custom workflows to support use cases that cross all product domains. It helps mitigate risk across an enterprise, by providing actionable intelligence, speeding security incident resolution, and reducing security operations costs.

The Cisco Physical Security Operations Manager is available as software that can be installed on Cisco Unified Computing System™ (UCS) C and B series.

Figure 1. Cisco Physical Security Operations Manager



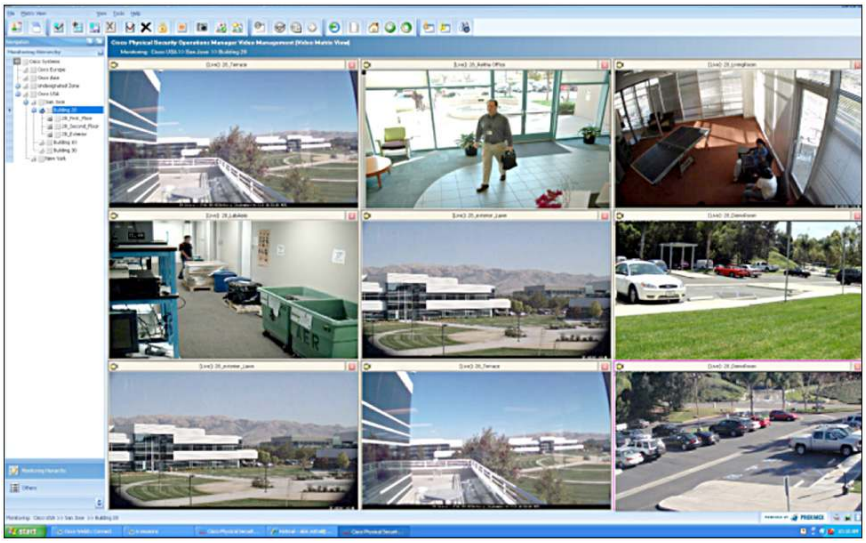
Important Features

Centralized Monitoring and Control of Thousands of Cisco IP Cameras and Access Control Devices

The Cisco Physical Security Operations Manager provides the scalability required to monitor thousands of IP cameras streaming video through multiple Video Surveillance Managers deployed in a distributed environment. It offers a variety of features, including:

- **Interactive geospatial maps and tree,** with a complete view of facilities, sensors, and alarms in an easy-to-use, intuitive graphical interface. Operators navigate the interactive map by clicking on security zones and areas or by using the hierarchical tree view. The hierarchical maps allow segregation of responsibilities and visibility for different security groups.
- **Support for Bing map services**, allowing operators to view maps on both the Operation and Web Consoles. These maps are geo-referenced to real world coordinates. (An additional license may be required.)
- **Control security sensors, devices, and resources,** through interactive maps that allow operators to click on an IP camera or a door reader and take control directly through the Physical Security Operations Manager interface. Operators can execute a wide range of actions in their domain, such as viewing live and recorded video, taking control of pan/tilt/zoom (PTZ) cameras, executing door commands, taking photo snapshots, and exporting video.
- **Video audio controls,** which allow operators to select from the video window to listen to live and recorded audio feeds from supported video management systems.
- **Web client,** a browser-based interface that provides an efficient, lightweight method to handle incidents. The Physical Security Operations Manager Web Console provides alert lists, alert details, and video from supported platforms, allowing users to remotely view alert information and video as they monitor a specific environment or incident. The Web client only supports operator functions.
- **Video matrix and guard tour**, with video streams presented to the operator in individual windows or in a matrix view (Figure 2). The video windows can also be configured to rotate through camera views, based on predefined camera sequences and times.
- **Centralized alarm management,** with generated alarms automatically shown on the maps at the centralized console. Based on user preferences, alarm details can be automatically displayed, or displayed by an operator with one click of a mouse.

Figure 2. Video Streams



Incident Assessment and Business Logic Builder

The Cisco Physical Security Operations Manager intelligently connects and correlates security events and alarms. It minimizes false alarms, while allowing the security team to respond in real time following predefined business logic. Operators immediately see all the relevant details of an alarm, without searching through multiple windows or systems to find the relevant information. Data available to operators includes:

- **Alarm details,** with specific information about the alarm, the system that generated the alarm, and the location on a map.
- **Live and recorded video,** which can be configured to start recording seconds prior to the alarm.
- **Response workflow tasks**, which provides instructions for the tasks (Standard Operating Procedures) operators must take to respond to and clear a priority alarm. This helps ensure a consistent response to recurring alarms, as well as to critical alarms that rarely occur. The response workflow tasks dynamically change, based on interactive decisions made by the operator. Response workflow can be multilayered and launch additional response workflow business logic, to support more complex and layered response workflows.
- **Response workflow task reassignment,** which can be undertaken by administrators and privileged operators while workflows are in progress. This allows operation centers to better distribute tasks among operators as conditions change.
- **Response workflows assignable by location**, in addition to alert type.
- **Operator notes page,** which let operators capture observations associated with the alarm.
- **Instant Messenger,** which allows operators to send messages to each other and share camera video and alerts directly with other operators, by sharing camera names and alert IDs. Messages between operators are logged as a part of the alert audit trail. Instant Messenger can also run in standalone mode without the Operation Console being launched.

- **Ability to attach documents and URLs to alerts,** as a part of the alert incident resolution process. This gives the Physical Security Operations Manager the ability to centrally manage and interact with information from various sources such as web site URLs, PDF files, and MS Word files. This allows operators to link to these documents and post new documents as a part of their response procedures.
- **Security system control,** which allows operators to take actions on cameras, security doors to temporarily open or lock/unlock a door.
- **Consolidated incident reports,** or incident dossiers, which can be created by the security teams (along with exported video) within seconds. These reports can be used for management reporting or forensic purposes, and they include all alarm details, photos, access attempts, mini-maps, and video files.

Business logic is used to escalate or filter alarms based on predefined conditions. When alarms are escalated, the Physical Security Operations Manager will guide operator response with specific management actions and instructions that should be taken when certain alarms are raised. The business logic templates capture the business processes and requirements for alarm creation and response, based on the alarm's status, schedule, monitoring area, or threat level. Business logic allows security personnel to concentrate on execution of planned responses, instead of reassessing unfolding situations.

Figure 3. Incident Assessment and Business Logic Builder

Advanced Trend Reporting

This Functional Module allows security operators, supervisors, and managers to track and trend alarms by time, sensor, location, and type, to facilitate proactive management of security resources and systems. It includes:

- **A simple-to-use, wizard-driven reporting engine,** which quickly generates reports based on alarms generated in the system across each of the incident reporting subsystems.
- **Predefined reports** for common inquiries, allowing fast access to the information needed to make important business decisions, including:
  - **Incident reports,** which can be viewed by incident type, location, time/date, and severity for a specified period of time (a date range, for example, or daily, weekly, or yearly).
  - **Trend reports,** which can be viewed in minutes and then printed, exported to multiple file formats, or emailed to select people or groups. Reports can also be generated across multiple security systems.

Tables 1 through 3 list valuable integration features of Cisco Physical Security Operations Manager.

Table 1. Important Integration Features with Cisco Physical Access Manager

Features
Automatic or on-demand import of all sensors (doors, gateway inputs that do not belong to any doors, power fail inputs, and tamper inputs)
Ability to define custom policies regarding which Physical Access Manager alarms should appear in the Physical Security Operations Manager, as well as what to correlate and what actions should be taken (by default, all door and reader alarms show up in the Physical Security Operations Manager)
One-click execution of access door commands (lock, unlock, etc.) from the operator's window
Automatic trigger of access door commands, based on predefined policies
Association of door alarms with relevant video
Bidirectional update of incident status in both Cisco Physical Security Operations Manager and Cisco Physical Access Manager
List of access attempts through a particular door
Retrieval of user information based on badge identification

Table 2. Critical Integration Features with Cisco Video Surveillance Manager

Features
Easy import of all camera sensors from multiple media servers or Video Surveillance Operations Managers
Ability to define custom policies regarding which Video Surveillance Manager alarms appear in the Physical Security Operations Manager, as well as what to correlate and what actions should be taken
Simultaneous access to live and recorded video in individual windows or in a matrix view (2x2, 3x3, or 4x4)
Rotation of camera views at predefined sequences and times, using the Video Guard feature
One-click access to live and archived video from the operator's window
Control of PTZ cameras
One-click video snapshot
DVR-type controls (rewind, fast forward)
Ability to track the path of suspects across multiple camera views, using the EZ-Track feature

Table 3. Useful Integration Features with Cisco IPICS

Features
Automatic or one-click dispatch of incidents, complete with details and relevant video, to the IPICS server
Automatic or one-click execution of policies defined on the IPICS server

Ordering Information

To place an order, visit the Cisco Ordering Home Page and refer to Table 4.

Table 4 lists Cisco Physical Security Operations Manager part numbers.

Table 4. Part Numbers

Product Name	Part Number
Enterprise Edition	
License for Cisco Physical Security Operations Manager Enterprise Edition	L-PSOM6-ENT-SW=
Cisco Physical Security Operations Manager 10-Sensor License Bundle	L-PSOM-10EP=
Cisco Physical Security Operations Manager 100-Sensor License Bundle	L-PSOM-100EP-
Cisco Physical Security Operations Manager 500-Sensor License Bundle	L-PSOM-500EP=
Cisco Physical Security Operations Manager 1000-Sensor License Bundle	L-PSOM-1000EP=

Product Name	Part Number
Cisco Physical Security Operations Manager 2500-Sensor License Bundle	L-PSOM-2500EP=
Cisco Physical Security Operations Manager 5000-Sensor License Bundle	L-PSOM-5000EP=
License for Cisco Physical Security Operations Manager - Standard Client	L-PSOM-USTD=
License for Cisco Physical Security Operations Manager - Premium Client (with IPICS Support)	L-PSOM-UPREM=
License for Cisco Physical Security Operations Manager - Web Client (requires Web Module)	L-PSOM-WEB-CLT=
License for Cisco Physical Security Operations Manager - Web Module	L-PSOM-WEBMOD=
License for Cisco Physical Security Operations Manager – Map Module (only needed if using Microsoft BING maps)	L-PSOM-MAPMOD=
License for High Availability	L-PSOM-HA=

Service and Support

Cisco and our certified partners can help you accelerate success and improve your return on investment (ROI) in a Cisco Physical Security Solution. The Cisco lifecycle approach to services defines the requisite activities at each phase of the solution lifecycle:

- Reduce deployment costs by identifying the features that will best meet your business requirements
- Accelerate migration by assessing the readiness of your network to support the system and by developing a sound design
- Support smooth implementation through effective planning and expert installation, configuration, and integration
- Increase operational efficiency and extend the value of your investment with award-winning technical support

For more information about Cisco services, visit http://www.cisco.com/go/services.

Find Out More

For more information about the Cisco Physical Security Operations Manager, visit http://www.cisco.com/go/physicalsecurity or contact your local account representative.

For more information about the Cisco End-of-Life Policy, go to http://www.cisco.com/en/US/products/products_end-of-life_policy.html.

To subscribe to receive end-of-life/end-of-sale information, go to http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-714743-01 02/13