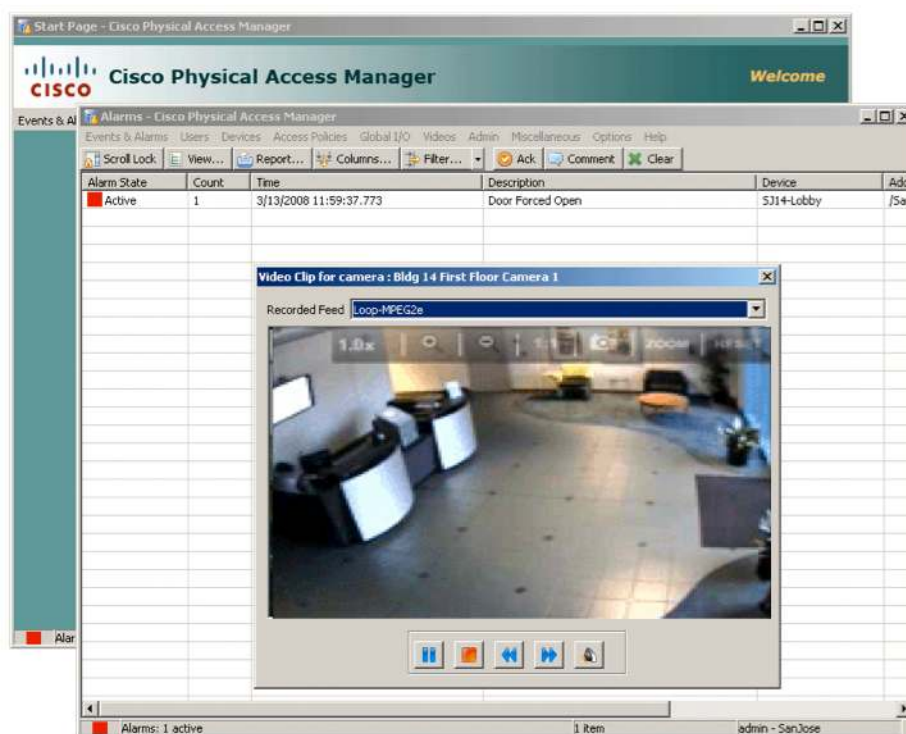


Cisco® Physical Access Manager 1.3

Cisco® Physical Access Manager is the management application for the Cisco Physical Access Control solution. It comes installed on hardware and is sold as an appliance. Cisco Physical Access Manager (Figure 1) is used to configure Cisco Physical Access Gateways and Modules, monitor activity, enroll users, and integrate with IT applications and data stores.

Figure 1. Cisco Physical Access Manager



Features

Table 1 describes the features of Cisco Physical Access Manager.

Table 1. Cisco Physical Access Manager Features

Feature	Description
Thick client and web browser support	Cisco Physical Access Manager supports a thick client model for provisioning and operation. Clients running Windows XP or Windows 7 communicate to the Cisco Physical Access Manager for full-featured operations and administrative purposes. Also supported is a Microsoft Internet Explorer 8 browser connection directly to the Cisco Physical Access Control server and gateways for device administration.
Microsoft Active Directory integration	Administrative users of Cisco Physical Access Manager can be configured to use Microsoft Active Directory for authentication.
Badging and enrollment	An optional licensable module enables the creation of badge templates, badge printing, taking user photographs, and enrolling users into the Cisco Physical Access Manager user database.
Device configuration	Cisco Physical Access Gateway hardware can be configured using Cisco Physical Access Manager. The gateway

Feature	Description
Access policies	contacts Cisco Physical Access Manager to download pre-provisioned configuration information. Areas (comprised of a group of doors) and users can be assigned entry permission based on schedules.
User rights	Administrative users of the Cisco Physical Access Manager can be assigned permissions. User profiles can be tailored very specifically.
Credential management	Cardholder credentials can be edited, including systemwide card formats.
Alarm and event management	Cisco Physical Access Manager provides a view of events and alarms in the system. Alarm and event views can be filtered based on several criteria.
Global I/O	Events (contact closure inputs or card access denied, for example) can be associated to actions (activate output contact closures, send an e-mail, etc.). Automation rules can be configured with a trigger, action, and notification. The trigger can be manual or periodic based on schedule and event/alarm. The action could be executing device commands or triggering URLs. Notifications could be sent via email with a report.
Reporting	Standard and custom reports can be created with Cisco Physical Access Manager.
Audit trails	Cisco Physical Access Manager provides a log of all administrative use of the system, arranged by user.
Enterprise application integration	An optional licensable component allows Cisco Physical Access Manager to be synchronized with data from either external SQL databases or Microsoft Active Directory. Large numbers of records (including .jpg photographs) can now be imported from external systems into the Cisco Physical Access Manager database using the Cisco Enterprise Data Integration (EDI) tool.
Cisco Video Surveillance Manager integration	Cisco Physical Access Manager dynamically acquires camera inventory from Cisco Video Surveillance Manager and associates cameras to doors. Users can view recorded or live video for every event from the door.
License management	License files (capacity upgrades or feature additions) can be added.
Server administration	Allows a user to administer the Cisco Physical Access Manager appliance by performing tasks such as IP address assignment.
Access gateway image management	Cisco Physical Access Gateway images can be upgraded using the Cisco Physical Access Manager.
Configuration backup	The entire configuration can be backed up to an external server.
System restore	A previously backed up configuration can be restored from an external server.
High availability	Two Cisco Physical Access Manager appliances can be configured as a pair to provide warm standby redundancy. The secondary appliance needs to be installed with a high-availability license.
URL invocation	HTTP/S URLs can be invoked as a result of any event or alarm. Event data can be inserted in the URL to integrate with any external application that accepts URL invocations. URL actions can be sent from the Cisco Physical Access Manager or directly from the Cisco Physical Access Gateway.
Web services API	A licensable option allows for external systems to use a web services API to integrate with Cisco Physical Access Manager. A SOAP binding over HTTP and HTTPS is supported.
Internationalization support	Language packs can be added displaying Cisco Physical Access Manager menu text in a language other than English. For debugging purposes, both English and the local language can be displayed at the same time.
Event management	New events generated by the system can be effectively managed while old events can be archived, automatically reducing the event database size. Events can be excluded from system backups, significantly reducing the backup file size.
Event policies	Event policies could be set up to suppress alarms from device(s) or all devices from a location based on a schedule. For example, an education customer can create different event policies for different schools. Each policy can include the alarm type (such as motion detection) together with the cameras assigned to a specific school's location. A schedule can also be associated with the event policy so events are logged only after normal working hours. If each school has different working hours, the user can create multiple schedules and assign them to the event policy for each school.
NTP configuration	The Network Time Protocol (NTP) server can be configured for all Cisco Physical Access Gateway modules, or for selected modules, over the network using Cisco Physical Access Manager.
Enrollment reader interface	We now support two methods of quickly enrolling new users into the Cisco Physical Access Manager database: Optical scanners or proximity card enrollment readers. The optical scanner allows badge administrators to scan government-issued drivers license ID cards. Data from the cards, like the name and address, is automatically extracted and populated into the new personnel records. Proximity card enrollment readers allow proximity badge data like facility code and ID to automatically populate into the new or existing personnel record, saving valuable time during enrollment.

System Requirements

Table 2 lists the system requirements for server hardware for Cisco Physical Access Manager.

Table 2. Supported Platforms for Cisco Physical Access Manager

Product Name	Part Number
Cisco Physical Security Multiservices Platform; 1 RU	CPS-MSP-1RU-K9

For more information on the supported platforms, please reference the [Cisco Physical Security Multiservices Platform](#).

For information on recommended workstation requirements, please reference the appropriate [technical documentation](#).

Package Contents

Table 3 describes the items that ship with the Cisco Physical Access Manager Appliance.

Table 3. Package Contents

Item
Cisco Multiservices Platform with Hard Drive (CPS-MSP-1RU-K9, CIVS-HDD-1000) , Power Cord (CIVS-CAB-16-xx), and Cisco Physical Access Manager Software (CIAC-PAME-M1X-K9)
Accessory kit
Regulatory compliance and safety information
Quick start guide

Availability

The Cisco Physical Access Manager is available through Cisco Authorized Technology Provider (ATP) Partners.

Ordering Information

Table 4 lists the part numbers for the Cisco Physical Access Manager.

Table 4. Ordering Information

Part Number	Description
CPS-MSP-1RU-K9	Cisco Multiservices Platform Server, 1-RU MSP assembly
CIVS-HDD-1000	1 TB SATA drive for CIVS-MSP
CIVS-CAB-16-CE	CIVS C16 power cable for Europe (CE)
CIVS-CAB-16-CI	CIVS C16 power cable for Italy (CI)
CIVS-CAB-16-CU	CIVS C16 power cable for UK (CU)
CIVS-CAB-16- AC	CIVS C16 power cable for North America (AC)
CIAC-PAME-M1X-K9	Cisco Physical Access Manager Software
CIAC-PAME-BD=	Cisco Physical Access Manager Badge Designer and Enroller
CIAC-PAME-HA=	Cisco Physical Access Manager High-Availability License
CIAC-PAME-M64=	Cisco Physical Access Manager 64-Module Capacity Upgrade License
CIAC-PAME-M128=	Cisco Physical Access Manager 128-Module Capacity Upgrade License
CIAC-PAME-M512=	Cisco Physical Access Manager 512-Module Capacity Upgrade License
CIAC-PAME-M1024=	Cisco Physical Access Manager 1024-Module Capacity Upgrade License

Part Number	Description
CIAC-PAME-EDI=	Cisco Physical Access Manager Enterprise Data Integration License
CIAC-PAME-WSAPI=	Cisco Physical Access Manager Web Services API License

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

For More Information

For more information about the Cisco Physical Access Manager, visit <http://www.cisco.com/go/eac> or contact your local account representative.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)