GLOSSARY

A

Access level	A set of access points, each with a corresponding time schedule, that determine where and when a badge holder has permission to pass through an access point. See also: Access point
Access point	An access point is an access-controlled point such as a door, turnstile, or gate. At the hardware level, this consists of a grouping of devices: Door Contact Door Strike Reader REX
ADA	ADA is an abbreviation for the Americans with Disabilities Act.
ADA strike time	ADA strike time refers to the ability of Cisco Physical Access Manager to customize the time before the door strike locks a door after access granted. This can be used for badge holders who need more time entering and exiting access points.
Alarm	An event that has been configured to be presented as an alarm to the operator. Alarms may be in different states indicated by color and/or blinking, and alarms may be acknowledged, cleared, and commented on by the operator. An alarm has an associated priority which indicates its severity or importance. See also: Event
Alarm State	The state of an alarm, based on operator actions. May be one of several states which also have an associated color and/or blinking: *Active:* Blinking red. The alarm is new and has not been acknowledged or resolved in any way. *Acknowledged:* Solid orange. An operator is aware of the alarm, but it has not been resolved. *Cleared:* Solid green. The alarm has been resolved. See also: Alarm See also: Top alarm state
APB	See also: Anti-passback

Anti-passback	A mode of operation that hinders a badge holder from entering an access point, then passing back their badge to another person to enter the same area. The consequences of violating the anti-passback conditions vary depending on the mode of anti-passback the individual access point is configured for.

See also: Area |
| **Anti-passback (APB) delay** | The time a badge holder must wait before they can reuse their badge at the same reader. This is not used for all APB modes.

See also: Anti-passback

See also: Anti-passback mode |
| **Anti-passback (APB) mode** | A mode which determines how anti-passback is enforced. The following is a list of possible modes.

Soft (grant access): Will let the badge use the reader if the badge has an incorrect entry area, but reports the passback violation to the software.

Hard (deny access): Will not let the badge use the reader if the badge has an incorrect entry area.

Reader-based using reader history: Same badge cannot be used twice in a row at this reader within the delay time.

Reader-based using card history: The badge cannot be used two consecutive times at this reader within the delay time, even if others use the reader.

Area-based: Hard APB within delay, soft APB after delay time.

See also: Anti-passback |
| **Area** | When an access point is configured for APB, the access point has an associated entry area and exit area. These areas are used to track the badge holders location.

See also: Anti-passback |
| **Audit record** | A record of an operator modifying an object in the system, including the date, time, and the state of the object before and after the edit. An audit record is a type of event.

See also: Event |

B

Badge	Also known as a card. A type of credential encoded with a card number, generally on a magnetic stripe or internally like a proximity card, and used to enter access points.
Baud rate	A measure of the rate at which a modem or serial connection transmits data. This is measured in bits per second (bps).
Biometric	Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. A biometric in Cisco Physical Access Manager refers to a type of credential used for biometric verification.

C

Calendar A calendar defines a set of holidays. The holidays within the calendars are then used in conjunction with access levels to control access during holiday periods.

Camera Cameras record digital video files to be stored on the DVR.

See also: Closed Circuit Television

CAN (Controller Area Network) bus A 3 wire parallel communication bus that runs between the Gateway and up to a total of 15 additional modules. These additional modules can be any combination of Reader, Input, or Output modules.

The distance limit on the CAN bus is 1320 feet. The last module on the CAN bus must be set to terminate the Can bus.

Card See Badge.

Card format The bit structure of a particular card. The average card format includes the card number, facility code, and parity bits. The two types of card formats supported by Cisco Physical Access Manager are Wiegand and magstripe.

Card format type The type of a card format, which may be Wiegand or magstripe.

See also: Wiegand

See also: Magnetic Stripe

Card number The card number encoded within the badge, often on the magnetic stripe or internally for proximity cards.

See also: Badge

CCTV Closed Circuit Television

CHUID/CUID Card Holder Unique Identity Model.

Cisco PAM client A Java applet that runs on a Windows client PC or workstation that is used to manage the Cisco PAM server and associate Gateways. It can be used to monitor the physical access system of sensors and locks. It can be used to configure the operation of the Cisco PAM server and the access modules.

Cisco PAM server An appliance used to manager and monitor a physical access infrastructure comprised of Cisco Gateway, Reader, Input and Output modules. It can interact with corporate directories like LDAP or MS Active Directory to validate access credentials for user access badges. It also interacts with Cisco VSM to provide video for configured devices and events.

Closed Circuit Television	A collection of surveillance cameras conducting video surveillance. Each camera is viewable on a monitor.
Credential	A general category that includes login, badge, and biometric; something that is used to gain access to a physical or logical resource.
	See also: Login
	See also: Badge
	See also: Biometric

D

Dashboard	A module with real-time graphs, charts, and diagrams that is used for monitoring details and statistics for the system.
Debounce	Debounce is a parameter representing the number of consecutive scans that must be in agreement before changing the state of the input point. Debounce is used to prevent incorrect reads. Each scan period is 16.7 milliseconds. The recommended setting for a REX is 2 and 4-6 for standard inputs.
	See also: Input point
Dedicated Micros Driver	A dedicated micros driver is a software device that manages the sending and receiving of data between the CCTV cameras and the DVR.
	See also: Driver
Default Gateway	In a network using subnets, the router that forwards traffic to a destination outside of the subnet of the transmitting device.
	See also: Subnet
Department	A sub-division of an organization, and used to organize personnel.
	See also: Organization
Device	A hardware (and in some cases software) component in the system. Events are generally associated with a Device. Devices also can have different states with varying color and severity.
Device Status	The real-time status of a device. Examples include: Online, Offline, Unknown, Secure, and Alarm. Each state has an associated color and severity. Not to be confused with top alarm state, which depends on operator actions in the application. For example, if a door is forced open, and then shut again, the status will go from forced open to secure, but the top alarm state will reflect the forced open state until an operator clears it.
	See also: Top Alarm State
Device status module	Allows operators to monitor the real-time status of all devices connected within the access-control. Operators can view the device properties, as well as status and the top alarm at any given device.

DHPC	Dynamic Host Configuration Protocol (DHCP). A network application that automatically assigns IP addresses to devices in the network.
	The Cisco Physical Access Gateway can obtain an IP address via DHCP. DHCP options 150 and 151 can also be passed with the DHCP lease. These options point the Gateway module to the Cisco PAM server and TCP port to use for the Gateway to Cisco PAM server TCP/IP session. The Gateway can also have a static IP address. The Cisco PAM server should have a static IP address. The Reader, Input and Output modules do not require an IP address.
DIP switch	A set of small on-off switches mounted on hardware. The dip switches are used to configure settings on the hardware.
Door contact	A door contact is a device that monitors whether a door is open or closed. A door contact is part of an access point.
	See also: Access point
Door strike	A door strike is a device that physically locks or unlocks the door. A door strike is part of an access point.
	See also: Access point
Driver	A process on a host computer used to communicate between the host computer and hardware devices. Different types of supported hardware generally have different drivers.
Driver manager	A driver manager is a software device that manages all drivers in the system.
	See also: Driver
Duress Request	This is a feature used by a badge holder under duress on a reader/keypad configured to accept PIN and Duress entries. If the badge holder enters their assigned PIN plus the configured duress key or keys, this will send a duress signal to the access-control system.
	For example: Duress code is configured as 1 digit, and that is 5. An individual has a personal identification number of 1111. If that individual enters 11110 or 1111, no duress indication is sent to the access-control system. If the individual enters 11115 a duress indication will be sent to the access-control system.
	In this example, any PIN entry of 1111x, where x is 0 through 4 or 6 though 9 will result in grant access with no duress signal. Only a PIN entry of 11115 will grant access with a duress signal. If the user enters 1111 only, the PIN entry time-out will have to expire and the individual will be granted access with no duress signal.
DVR	DVR is an abbreviation for digital video recorder. A DVR records video from CCTV cameras to disk. Allows for viewing of live or past video.
	See also: CCTV

E

Encryption A method of securing data so it cannot be read by unauthorized users or applications. The configuration file and card database located on the Gateway module are encrypted.

Cisco PAM backup files created by the back up process are encrypted with a password. The password used when creating the backup file must be entered when using the file for a restore operation.

Event An activity within the system, recorded to the database, and available for monitoring or reporting.

Event Policy Manager A module used to configure the way events are processed and displayed. This following attributes can be configured:

- **Is alarm:** This determines whether the event is an event or alarm.
- **Is recorded:** This determines whether the event is recorded. If the event is not recorded, it can not be an alarm.
- **Priority:** This determines the priority of the event or alarm.
- **Alert sound:** The sound to be played when the event occurs.

See also: Event

F

Facility code A segment of bits encoded on a card which represent a number in association with a facility. Often all cards issued for a single facility will have the same facility code.

Fail-Safe lock A lock that requires voltage to remain in the locked state. If voltage is removed, the lock will move to the unlocked state.

Fail Secure lock A lock that does not require voltage to remain in the locked state. If voltage is removed, the lock remains in the locked state.

FASC-N Federal Agency Smart Card Number.

Filter A tool allowing operators to select which objects should be displayed.

FIN Foreign Identification Number. Used as an alternative to Social Security Number (SSN).

G

Gateway module
A device that can accept one 10 wire Wiegand reader, or two 5 wire Wiegand readers, three inputs, three outputs, power fail, and tamper sensor inputs. The gateway communicates with the CPAM server over TCP/IP over Ethernet. It also communicates up to 15 additional Reader, Input, or Output modules over a 3 wire CAN bus. The gateway can be powered via POE or 12V or 24V DC.

The Gateway can download badge access credentials and store them locally permitting access control even without network connectivity to the Cisco PAM server. Events that occur while the connection to the server is down are stored locally and uploaded to the Cisco PAM server once the network connection resumes.

GND pins
Ground for the DC voltage input.

Graphic maps editor
A module which allows graphic maps to be imported and configured. A graphic map can have links to other maps and or links to other devices. The map links can be used to navigate between maps in the graphic maps viewer. The device links show the real-time status of the device in the graphics maps viewer.

Graphic maps viewer
A module allowing facility maps to be viewed. The Graphic maps viewer displays the location and status of devices within the facility. The maps can also contain links used to navigate to other maps

H

Hardware
See Device

Hardware module
A module allowing operators to add, edit, and disable the hardware.

See also: Device

Hardware tree
The hardware tree is a hierarchical display of all devices in the system, seen in the Hardware module and the graphic maps editor. Each device in the hardware tree can be expanded or collapsed to show or hide its sub-devices by clicking the **+** or **-** to its left.

See also: Device

See also: Hardware tree

See also: Hardware module

Hexadecimal
A numbering system usually written using the symbols 0–9 and A–F or a–f.

HID
A company manufacturing the industry standard proximity access-control cards.

See also: Proximity

Hold time
The amount of time in seconds that the system will ignore an active state of a monitor point. The system will hold a higher priority status before a lower priority status is reported. As an example, motion detectors can sometimes trigger multiple times per second causing the Event logs to fill unnecessarily fast with useless data.

Hot stamp	The number physically printed or embossed on a badge. This number is generally independent of the Card Number. Not all badges have a hot stamp number.
	See also: Badge
HSPD-12	The Homeland Security Presidential Directive 12. A a policy for a common identification standard for federal employees and contractors.
HTTPS	Hypertext Transfer Protocol Secure. A combination of the Hypertext Transfer Protocol and a network security protocol. Gateway and Cisco PAM HTTP access is via HTTPS.
	See also SSL.

I

input	A sensor that has 2 states, open or closed. The steady state can either be normally open (NO) or normally closed (NC). When moved to the non-steady state, the input is used to make a decision. Typical input is a door sensor. It is used to determine if the door is in the opened or closed position. An input has 2 pins marked + and -. Gateway, Reader, and Input module inputs can be supervised or un-supervised. See also Supervised input.
	Inputs do not require power. Power is supplied from the module.
Input module	A device that can accept 10 inputs. It communicates with the CPAM server via the CAN bus and the Gateway module. The module requires an external 12V to 24V DC source and can not be powered via POE.
IP address	The Internet Protocol address. The Cisco Physical Access Gateway can obtain an IP address via DHCP. DHCP options 150 and 151 can also be passed with the DHCP lease. These options point the Gateway module to the Cisco PAM server and TCP port to use for the Gateway to Cisco PAM server TCP/IP session. The Gateway can also have a static IP address. The Cisco PAM server should have a static IP address. The Reader, Input and Output modules do not require an IP address.

L

LDAP	LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.
LED	Light-emitting diode. A semiconductor diode that converts applied voltage to light. LEDs are used to display status, communication, and other information on various devices.
Localhost	Default hostname describing the local computer address.
Login	A credential used to obtain access to the application as an operator. A login has a username and password, along with a set of profiles which determine what the operator has access to within the application. See also: Profile
Logins module	A module used to manage operator logins in the application. See also: Login

M

MAC Address	MAC address is an abbreviation for Media Access Control address that uniquely identifies each node of a network. Each type of network medium requires a different MAC address.
Magnetic Stripe	A strip of magnetic recording material on which a certain data is stored. See also: Card Format Type and Wiegand
Masked	A hardware state for monitor points and access points where one or more active conditions will be reported to the software as masked.
Module	An independent section of Cisco Physical Access Manager with some distinct function.
Monitor point	A monitor point is an input on a sub-controller that is configured to monitor an external device or signal, typically an alarm input.
Monitor point group	MPG is an abbreviation for monitor point group. A MPG is an operator defined organization of access points and monitor points. Commands issued to the MPG influence all of the contained devices. A total of 128 monitor points or 64 access points can be included in a MPG. One access point counts for two monitor points.
Multiplexer	A type of hardware which can combine multiple communication channels into a single communications channel.

O

output	A device that requires a trigger to change state. The steady state is either normally open (NO) or normally closed (NC). Once a decision is made for the device to change state, the module output interface will open or close a relay to trigger the device. A typical output device is an electric-mechanical door lock. IE: When not triggered, the lock is in the 'locked' position. When triggered by the output module, the lock moves to the 'unlocked' position.
	Outputs generally require power, and the output module will either close or open a relay to trigger the device. The power to drive the device should be inline with the relay on the output module. The output relay on the module has 3 pins marked NC, C and NO. NC is normally closed, C is common or ground and NO is normally open. Exception might be for a POE capable lock, where the power for the lock is obtained from the Reader attachment of a Gateway or reader module.
Output module	A device that can drive 8 outputs. It communicates with the Cisco PAM server via the CAN bus and the Gateway module. The module requires an external 12V to 24V DC source and can not be powered via POE.
Organization	An organization with which a personnel record can be associated.

P

PDF	Portable Document Format. A document format defined by Adobe, which represents a printable/viewable document in a manner that is independent of the original system used to create it. Viewing PDF documents requires the Adobe Reader, freely available at www.adobe.com.

Personnel module	A module used to manage personnel information.
PF input	This input is used to detect a power failure. If activated, an alarm is posted notifying the administrators that a device has lost power. The PF input has 2 pins marked + and -. This input can be re-allocated to act as an unsupervised input.
PIN	Personal Identification Number. A badge has a PIN associated with it, which, depending on the configuration of an access point, is entered into the keypad on the access point's reader.
POE	Cisco Power Over Ethernet. This provides up to 15.4 watts to power devices attached via a CAT5 cable to a POE capable switch.
Power Over Ethernet	See POE.
Privilege	Privileges define what a credential has access to. Examples of privileges include access levels and profiles.
	See also: Credential
	See also: Profile
	See also: Access level
Profile	A profile determines the software modules and the commands that an operator has access to upon logging in.
Profiles module	A module for managing profiles. See also: Profile
Proximity	A technology where the presence of a certain object can be sensed by a device without having direct contact. See also: HID

R

Reader	A reader is a device for receiving a card number and/or PIN from a badge holder.
Reader module	A device that can accept one 10 wire Wiegand reader, or two 5 wire Wiegand readers, three inputs, three outputs, power fail, and tamper sensor inputs. It requires a Gateway module to facilitate communication with a CPAM server. The module requires an external 12V to 24V DC source and can not be powered via POE.
Relay	A device that responds to a small current or voltage change by activating switches or other devices in an electric circuit.
REX device	REX is an abbreviation for "request to exit". A REX is a type of door hardware, typically a button that allows people to exit through an access point without using a badge. When a door state changes from closed to open, it means someone has unlocked the door from the secure side. If the door state moves from closed to open, with no valid reader swipe or REX activation, it can indicate that the door was forced open.
	A REX is part of an access point. See also: Access point.
RTS mode	A method of hardware flow control used in serial communications.

S

Scroll lock
A tool button in some modules that allows the operator to stop the scrolling of items in the window. New items will continue to be added to the window, but the window will not automatically scroll to show the most recently added item.

Serial communications
A method of communicating over a dedicated line.

Site
A site is a single instance of a Cisco PAM database. It generally, but does not necessarily, correspond with a single geographical location, such as a building complex, building, or part of a building. Most installations of Cisco Physical Access Manager only have a single database, and hence a single site. Multiple sites are used in larger configurations, for example a company with offices around the world, with a Cisco PAM database at each office.

SSN
Social Security Number. A nine-digit number issued to individuals by the U.S. government for tax purposes, and often used as an identification number.

SSL
Secure Sockets Layer. A security protocol for secure connections using over the internet. Gateway to Cisco PAM server can utilize SSL for the connection. All gateways and Cisco PAM server must be configured for SSL, or for no SSL. A mix of SSL and non-SSL is not supported.

Gateway and Cisco PAM HTTP access is via HTTPS. See also HTTPS.

Status
See Device Status

Subnet
A portion of a network, which shares a common network address with other portions of the network and is distinguished by a subnet number. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100 would be part of the same subnet.

Supervised input
A supervised input has 4 states. (1) Short (2) Open (3) Non-Alarm or (4) Alarm.

An unsupervised input has 2 states. (1) Normal or (2) Alarm.

Unsupervised inputs have limited functionality. If a wire is cut or shorted between the input module and a normally open device. The server cannot determine the change and the device would remains in inactive state even when the switch is closed.

To make the input device supervised, use two 1K resistors in the circuit.

- In the *inactive* state, the circuit measures 2000 ohms.
- In the *active* state, the circuit measures 1000 ohms.
- In the *short* state the circuit measures 0 ohms
- In the *open* state the circuit measures infinite ohms.

Once the input device is supervised, CPAM can determine if a wire is cut or shorted.

See also input and Input module. See Device Configuration Properties for more information.

T

TCP/IP communications　　A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

Telnet　　An Internet communications protocol that enables a computer to function as a terminal working from a remote computer.

Time interval　　A period of time defined using a start time and time. Each period has a list of days of the week (Sun. through Sat.) and holidays of when it can be active.

Time received　　The time an event or alarm was actually received by the access-control system and stored in the database.

Time schedule　　A defined set of time intervals used to make access-control, triggering, and other decisions. See also: Time interval

Time zone　　24 longitudinal divisions of the globe, nominally 15 degrees wide, in which clocks show the same time.

TM input　　This input is used to detect if a component box is being tampered with. It acts like a normal input and would be in the normally closed position indicating that the component box access door is closed. Once opened, this input would alert and administrator that the component access door is, or was, opened. The TM input has 2 pins marked + and -. This input can be re-allocated to act as an unsupervised input.

Top alarm　　The most important alarm present at a given device. Based on alarm state, time, and priority. See also: Alarm and Alarm state

Top alarm state　　The state of the top alarm at a given device. Possible states include active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity. Not to be confused with device status, which is independent of operator actions in the application. For example, if a door is forced open, and then shut again, the status will go from forced open to secure, butthe top alarm state will reflect the forced open state until an operator clears it. See also: Device Status and Alarm state

Trigger　　A trigger waits for an operator-defined combination of events, addresses, properties, and time schedules to occur, then executes a procedure. See also: Procedure

TTR　　Triple Technology Reader. A reader which combines three devices in one: a magnetic card reader, HID proximity card reader, and piezoelectric keypad.

U

Use limit　　An option which can restrict a badge to a certain number of uses. The default is 0 (off). See also: Badge

Username　　A sequence of characters used as identification when logging onto the application.

V

View query	An option within the filter tools, giving operators the capability to view the actual filter definition as an SQL-like expression string. See also: Filter
VIN pins	Voltage input. This is where you can use +12 to +24 volts DC to power the module.

W

Wiegand card format	Wiegand card format stores card data using binary values. The information includes parity error detection, facility code and the card ID. Each card has a particular format that must be configured in the access-control panel to permit the panel to correctly interpret the card data. A very common Wiegand card format is a 26 bit format, with the first and last bit for parity, 8 bits for the facility code and 16 bits for the card number.
	When configuring the Credential Template on the Cisco PAM server you must configure it to match the card format for the reader. The format might be more or less than 26-34 bits.
Wiegand Interface	This is a 10 pin interface on the Gateway or Reader module used to attach a card reader. The 10 pin interface can be logically configured to operate as two 5 wire Wiegand interfaces to support two readers. When run in 5 pin mode, the LED function on the reader is not used.
	The minimum leads needed for the Wiegand reader to work are:
	PWR = Power
	GND = Ground
	D0 = Data bit 0
	D1/clock = Data bit 1 and the clock
	GRN = LED power
	DRTN = Data return (1 end only)
Wizard	An interactive utility that guides an operator through potentially complex tasks, including adding and configuring a new sub-controller.

Cisco Physical Access Manager User Guide