



# Release Notes for Cisco Physical Access Control Release 1.1.0

---

Last Revised: January 22, 2010, OL-19462-02

## Contents

- [Introduction, page 1](#)
- [System Requirements, page 1](#)
- [Installation Notes, page 2](#)
- [Upgrade Notes, page 3](#)
- [Caveats, page 6](#)
- [Related Documentation, page 8](#)

## Introduction

These release notes describe important information for Release 1.1.0 of Cisco Physical Access Control, including the Cisco PAM appliance, the Cisco Physical Access Gateway, and optional expansion modules.

## System Requirements

- [Cisco PAM Appliance Requirements](#)
- [PC Client Software](#)
- [Cisco Physical Access Gateway Firmware Requirements](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2009 Cisco Systems, Inc. All rights reserved.

## Cisco PAM Appliance Requirements

- Release 1.1.0 of the Cisco Physical Access Manager software.
- A PC and web browser Internet Explorer 6.0 or higher.

## PC Client Software

A PC is required to access the Cisco PAM client desktop software. The minimum requirements are:

- Microsoft Windows XP or Vista
- Java 6.0 or higher (JDK 1.6 or higher)
- 2.8 GHz Intel Pentium IV processor or higher.
- 1GB RAM or more.
- 100 MB hard disk space available for the application, and an additional 20 GB or more disk space for data storage.

## Cisco Physical Access Gateway Firmware Requirements

Cisco Physical Access Gateway Firmware Release 1.1.0 is required on all Gateway modules. Upgrade the Gateway firmware after upgrading the Cisco PAM software to Release 1.1.0.

See [Cisco Physical Access Gateway Firmware Installation, page 3](#).

## Installation Notes

- [Cisco PAM Installation, page 2](#)
- [Cisco Physical Access Gateway Firmware Installation, page 3](#)
- [Hardware Installation, page 3](#)
- [Part Numbers for the Optional Feature Licenses, page 3](#)

## Cisco PAM Installation

For instructions to install and upgrade the Cisco PAM software and firmware, see the *Cisco Physical Access Manager User Guide*. This guide includes instructions to install the following software components:

- Cisco PAM appliance hardware
- Cisco PAM appliance server software
- Cisco PAM desktop client software
- Cisco VSM Video Player
- EDI Desktop Studio application

## Cisco Physical Access Gateway Firmware Installation

Upgrade the Gateway firmware after upgrading the Cisco PAM software.

If a Cisco Physical Access Gateway is running a firmware version earlier than Release 1.1.0, an alarm indicates the version mismatch. Upgrade the Gateway to firmware Release 1.1.0.

For instructions to upgrade the Cisco Physical Access Gateway firmware, see the *Cisco Physical Access Manager User Guide* and the *Cisco Physical Access Gateway User Guide*.

## Hardware Installation

For instructions to install the Cisco Physical Access Control hardware modules, see the *Cisco Physical Access Gateway User Guide*. This guide includes instructions to install the following hardware modules:

- Cisco Physical Access Gateway
- Cisco Input Module
- Cisco Output Module
- Cisco Reader Module

## Part Numbers for the Optional Feature Licenses

To enable optional features, or additional capacity, purchase and install the Cisco licenses listed in [Table 1-1](#).

**Table 1-1**      *Optional Feature Licenses and Part Numbers*

Part	Optional Feature Licence
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
CIAC-PAME-BD=	Cisco Physical Access Manager Badge Designer and Enroller
CIAC-PAME-HA=	Cisco Physical Access Manager High Availability License
CIAC-PAME-EDI=	Cisco Physical Access Manager Enterprise Data License

## Upgrade Notes

Review the following notes and instructions before upgrading the Cisco PAM server software, desktop client software, or Gateway firmware.

- [Generic Output Devices Installed Prior to Release 1.1 Must Be Rewired](#), page 4
- [Generic Output Device Command and Event Name Changes](#), page 4
- [Select All Options When Upgrading Gateway Firmware](#), page 4
- [Browser Time-out](#), page 5

- [Upgrade the Cisco PAM Desktop Client Software, page 5](#)
- [Java Requirements, page 5](#)
- [Stop EDI Projects Before Upgrading Cisco PAM, page 5](#)
- [Database Password Change Message, page 6](#)

## Generic Output Devices Installed Prior to Release 1.1 Must Be Rewired

All Generic Output devices installed in Cisco PAM systems prior to release 1.1.0, were connected to the Gateway, Reader, or Output modules with the wiring reversed. In Cisco PAM release 1.1.0, the wires for these Output devices must be reinstalled to match the device manufactures recommended connections.

### Required Generic Output Device Connections in Cisco PAM release 1.1.0

Disconnect all Generic Output devices installed with Cisco PAM release 1.0.0, 1.0.1, or 1.0.3, and do the following:

- Connect *Normally Open* devices to the **N.O.** and **C** connectors on the Gateway, Reader, or Output module.
- Connect *Normally Closed* devices to the **N.C.** and **C** connectors on the Gateway, Reader, or Output module.

Failure to re-wire these devices will cause the devices to act in the opposite way intended.

See *Cisco Physical Access Gateway User Guide* for more information on module and device wiring.

## Generic Output Device Command and Event Name Changes

The following generic output device command names were changed for Release 1.1.0. The functionality is the same:

Release 1.0 Command Name	Release 1.1 Command Name
Turn output off	Activate Relay
Turn output on	Deactivate Relay

The following generic output device event names were changed for Release 1.1.0. The functionality is the same:

Release 1.0 Event Name	Release 1.1 Event Name
Output Off	Output Deactivated
Output On	Output Activated

## Select All Options When Upgrading Gateway Firmware

When upgrading Gateway firmware images to Cisco PAM Release 1.1.0 from any earlier release, select all available options, including the following:

- **Set as active image:** (checked by default) make the firmware file new active image.
- **Delete credentials:** delete the module credentials.

- **Delete configuration:** delete the module configuration. The configuration is automatically reloaded when the module established communication with the Cisco PAM appliance.
- **Delete events:** delete all events stored on the module.
- **Reset Gateway:** (checked by default) perform a soft reset to powercycle the module. Changes to the active image are applied only after the Gateway is reset.

**Note**


---

When all options are selected, wait approximately 10-15 minutes for the firmware upgrade to complete.

---

See the instructions in the *Cisco Physical Access Gateway User Guide* or the *Cisco Physical Access Manager User Guide* for more information.

## Browser Time-out

When upgrading to Cisco PAM Release 1.1.0 and higher, the web browser may display an error such as “Page Not Found” while the upgrade is in process. Wait approximately five minutes for the upgrade to complete, then refresh the browser to display the login page.

## Upgrade the Cisco PAM Desktop Client Software

Always upgrade the Cisco PAM desktop client when the server software is upgraded. If the versions are not the same, an error will occur when launching the desktop client. See the *Cisco Physical Access Manager User Guide* for instructions.

**Note**


---

If the download fails, check your Java Web Start network settings. The Cisco PAM client launches using Java Web Start.

---

## Java Requirements

Before upgrading the Cisco PAM server, upgrade your PC to Java 6.0 or higher (JDK 1.6 or higher), if necessary.

- To install Java 1.6, log on to the Cisco PAM appliance, select **Downloads**, and then select **JRE 1.6 (Windows)**.
- To download the latest Java, go to <http://www.java.com/en/download/manual.jsp>

## Stop EDI Projects Before Upgrading Cisco PAM

Stop any running EDI projects before upgrading the Cisco PAM appliance software. After the upgrade, re-import the project to EDI Administration and start it again. See *Cisco Physical Access Manager User Guide* for instructions to stop, start and import EDI projects.

If EDI projects are not stopped before a Cisco PAM upgrade, the project execution (or run) will not be successful. If this occurs, contact your Cisco support representative for assistance.

## Database Password Change Message

When the server restarts, a message appears asking if you want to change the database password. Click **Cancel** or **OK**. This password is a security measure used for troubleshooting and technical support. It does not impact user operation.

## Caveats

- [Using the Bug Toolkit, page 6](#)
- [Open Caveats, page 7](#)

## Using the Bug Toolkit

You can search for problems by using the Cisco Software Bug Toolkit. To access the Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Software Bug Toolkit, follow these steps:

### Procedure

- 
- Step 1** To access the Bug Toolkit, go to <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>.
- Step 2** Log on with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the “Search for bug ID” field, then click **Go**.
- Step 4** To look for information if you do not know the bug ID number:
- Select Product Category:** Select **Security**.
  - Select Product:** Select **Cisco Physical Access Control**.
  - Software Version menu: (Optional) Select the version number.
  - Advanced Options:** Select **Use default settings** or **Use custom settings**. The default settings search for severity 1, 2 and 3 bugs, open and fixed bugs, and bugs containing bug details. Use the custom settings to change the severity and status parameters, or to search for keywords within the bug headline and description.



### Tip

For information about how to search for bugs, create saved searches, create bug groups, etc., click **Help** in the Bug Toolkit page.

---

## Open Caveats

The following caveats describe the known issues and limitations with Cisco PAM Release 1.1.0. Click the link to view the workaround for each issue.

**Table 2** *Unresolved Caveats for Cisco Physical Access Control Release 1.1.0*

Identifier	Headline and Bug Toolkit
<a href="#">CSCsr78085</a>	Upgrade screen sometimes does not display all fields. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsr78085">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsr78085</a>
<a href="#">CSCsy75985</a>	All Schedule entries within a collection (TimeEntryCollection) need to have the same disposition (Grant or Deny). <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsy75985">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsy75985</a>
<a href="#">CSCtd58794</a>	If the recovery CD is used to replace the Cisco PAM software on the active server, you must also use the recovery CD to install the software on the standby server, if installed. After the software is installed, restore the server data from a backup file. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd58794">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd58794</a>
<a href="#">CSCtd04239</a>	Cisco PAM is not updated when a module is in the Down state. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd04239">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd04239</a>
<a href="#">CSCtd82174</a>	Events generated by a Cisco PAM client are logged using the client time zone. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd82174">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd82174</a>
<a href="#">CSCtd82297</a>	Access granted into an anti-passback area (APB) area but not entered requires Admin override. Log into Cisco PAM as an administrator, open the Doors:Access Policies:Anti-Passback Monitoring module, select the area in question and select the <b>Reset</b> command to rectify APB state for that area. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd82297">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtd82297</a>
<a href="#">CSCtc74271</a>	The web browser does not always respond to the <b>Image Upgrade</b> button in the Gateway Web Admin tool. To address this issue, close the browser, reopen it, and issue the command again. The progress bar at the bottom of the window indicate successful submission of the request. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtc74271">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtc74271</a>
<a href="#">CSCtc79685</a>	The web browser does not always respond to the <b>Image Activate</b> button in the Gateway Web Admin tool. To address this issue, close the browser, reopen it, and issue the command again. The progress bar at the bottom of the window indicate successful submission of the request. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtc79685">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtc79685</a>
<a href="#">CSCte40705</a>	Changes to the password for the Cisco PAM Web Admin tool are not synchronized to the HA pair. If the password is changed on one server, you must log in to the second server and change the password. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte40705">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte40705</a>

**Table 2** *Unresolved Caveats for Cisco Physical Access Control Release 1.1.0 (continued)*

Identifier	Headline and Bug Toolkit
<a href="#">CSCte35844</a>	Moving a device icon after scale resets icon scale to 100%. Move icon first, then rescale. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte35844">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte35844</a>
<a href="#">CSCte38769</a>	Can not delete Base Location from Doors & Locations in Cisco PAM. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte38769">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte38769</a>
<a href="#">CSCsq04020</a>	Holiday schedules that span two months (for example, December 25 through January 4) should be split into two entries: one that covers the first month and the second that covers the following month. For example, one entry for December 25 through December 31, and a second schedule entry for January 1 through January 4. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsq04020">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsq04020</a>
<a href="#">CSCsy75985</a>	A TimeEntryCollection with opposing actions (such as Permit and Deny) requires two different entries. For example, if you create Schedule S1 with Time Entry Collection TEC1 with action “Permit”. If the you create another Schedule S2 with the same Time Entry Collection TEC1, but with the action “Deny”, then the previous schedule S1 action changed to Deny. To resolve this, create separate Time Entry Collection instances for use in more than one schedule, even if the instances are the same definition. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsy75985">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsy75985</a>
<a href="#">CSCsu93207</a>	EAI projects fail after a Cisco PAM upgrade from Release 1.0.0 to post 1.0.0 which was previously running fine. EDI projects must be stopped and restarted after a Cisco PAM upgrade is complete. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsu93207">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsu93207</a>
<a href="#">CSCte52017</a>	Unique Department names are required across Organizations for data import. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte52017">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCte52017</a>
<a href="#">CSCta94141</a>	Badge IDs greater than 31 bits are not handled correctly. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCta94141">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCta94141</a>
<a href="#">CSCtb79778</a>	Gateway resets on badge swipe without keypad pin. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtb79778">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtb79778</a>
<a href="#">CSCtb98101</a>	Badge changes using “Group-Edit” are not always synchronized to the Gateways. <a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtb98101">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCtb98101</a>

## Related Documentation

- Cisco Physical Access Manager User Guide
- Cisco Physical Access Gateway User Guide

- Cisco Physical Access Manager Quick Start Guide
- Cisco Physical Access Gateway Quick Start Guide

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008-2010 Cisco Systems, Inc. All rights reserved.

