Release Notes for Cisco Physical Access Control, Release 1.5.2

Last Revised: November 20, 2014,

Contents

Introduction

This document describes important information of the Cisco Physical Access Control 1.5.2 release. In this release, a number of caveats are resolved.

Cisco Systems, Inc.
www.cisco.com

New Features

Cisco Physical Access Control, Release 1.5.2 offers the following additional features:

Delayed Output Activation

- If an input is activated then the system waits for a badge/pin authentication up to the specified time as configured in “Door Sensor Timer” in Door Properties.
- If the badge/pin is not in the database or the countdown comes to zero, then an output is activated and an event is generated.

Toggle

- Toggle is an additional field introduced in “Door properties”.
- This functionality is used to toggle the mode of a door from LOCK to OPEN and vice versa.
- By default, Toggle is configured as “NO” and the configurations are not pushed to the gateway until the user unchecks the check box next to it.

Upgrade Paths

You can use the following upgrade paths to upgrade from older versions of CPAM to CPAM 1.5.2:

- 1.3.2(0.3.5) to 1.5.2
- 1.4.1(0.3.11) to 1.5.2
- 1.4.1(0.3.13) to 1.5.2
- 1.5.0(0.3.17) to 1.5.2
- 1.5.1(0.3.7) to 1.5.2

Note Customers using CPAM 1.3.1(0.3.8) and older version have to upgrade to 1.3.2(0.3.5) first and then to 1.5.2.

Upgrading from 1.4.1 OVA to 1.5.2 OVA

To upgrade 1.4.1 OVA to 1.5.2 OVA, follow the below steps:

Step 1 Upgrade to 1.5.2 using **cpam-msp-1.5.2_0.3.7.upgrade.bin** file.

Step 2 Take a full DB backup.

Step 3 Deploy the 1.5.2 OVA image on UCS and complete the initial setup.

Step 4 Restore the DB backup into the newly deployed 1.5.2 instance.

Upgrading CPAM from 1.5.0/1.5.1 to CPAM 1.5.2

Note The below given procedure should be followed before upgrading from 1.5.0 or 1.5.1 to 1.5.2. This applies to CPS-MSP-1RU-K9, CPAM 1.5.x virtual machines and CPS-UCS-1RU-K9 platforms.

Step 1 Stop **cpamacserver** via webadmin.

Step 2 Copy the **preupgrade-1.5.2.zip** file to the server under **/home/cpamadmin**.

Step 3 Extract the **preupgrade-1.5.2.zip** file using the command **unzip preupgrade-1.5.2.zip**.

Step 4 Change the file to the **preupgrade** folder using the command **cd preupgrade**.

Step 5 Change the permission for all the 3 files namely **preUpgrade.sh**, **immortal.sh** and **upgrade.sh files** using the command **chmod 755 <filename>.**

Step 6 Run the **dos2unix <*filename*>** command for both the scripts.

Step 7 Stop the immortal service using the command **service immortal stop.**

Step 8 Execute the **preUpgrade.sh script** alone.

Note Do not run the **upgrade.sh script.**

Step 9 Start immortal service using the command **service immortal start.**

Step 10 Upgrade to 1.5.2 by uploading the appropriate upgrade bin file from the webadmin.

Post Upgrade Notification

Warning **If the previous installation has partial configuration for location assignment to gateways or doors, the Administrator must log in to the system to validate that the gateways and doors are in the same location, prior to applying/downloading any changes in the existing configuration. This is applicable only if the customer opts to use the Profile Enhancement feature.**

System Requirements

Table 1 describes the minimum requirements for a Cisco PAM appliance, workstation, and gateway module.

Table 1 Cisco PAM Release 1.5.2 Requirements

Requirement	Description
Workstation software requirements	• Windows XP, Windows 7, or Vista and Internet Explorer 6.0 or higher, or Windows 7 (64-bit only) and Internet Explorer 8.0 (32-bit only). • Java 6.0 or higher (JDK 1.6 or higher).
Workstation hardware requirements	• 2.8 GHz Intel Pentium IV processor or higher. • 4GB RAM or more. • 250 MB hard disk space available for the application, and an additional 20 GB or more disk space for data storage.
Cisco PAM appliance software requirements	• Release 1.5.2
Cisco PAM appliance hardware requirements	• For servers shipped with CPAM version 1.4.1 or earlier, please refer to the "Cisco Physical Security Multiservices Platform Series User Guide. • For servers shipped with CPAM version 1.5.2 please refer to the "Cisco Connected Safety and Security UCS Platform Series User Guide.
Cisco physical access gateway firmware requirements	Firmware Release 1.5.2 is required on all gateway modules. • Upgrade older firmware versions to 1.5.2. See the Cisco Physical Access Gateway User Guide for instructions.

Note The gateway can be upgraded through web admin in Internet Explorer 8.0 or above only if TLS 1.1 is enabled in the IE browser's settings. To enable TLS 1.1, choose Tools > Internet Options > Advanced> Security, uncheck the Use TLS 1.0 check box, and check the Use TLS 1.1 check box.

System Recovery

In case of system crash, the Recovery ISO image can be used to bring back the system to normal state.

The ISO prompts for two input options. They are

- **Factory**
- **Recovery**

If the user selects the input as **Factory**, the existing system is uninstalled completely and a new image is installed with zero license. The user can retrieve the original licenses by restoring the DB.

If the user selects the input as **Recovery**, the following happens:

- The database and the CPAM software are retained.
- A fresh OS is installed, and the existing password is replaced as **cpamadmin.** This is provided as the password for the webadmin, CPAM client and the SSH. The user is allowed to change the password later.
- The ETH0 IP address is retained but the rest of the NIC configurations (default gateway and subnet mask) is required to be manually configured. After configuring, the network and the immortal services are required to be restarted.
- The DNS server requires reconfiguration in webadmin.
- In case of HA, the server which is recovered will be standby server.
- RPM is not uninstalled in the recovered server. Hence, for a fresh CPAM image to be installed the user should select **Factory** as input by using the Recovery ISO image.

Obtaining Software, Documentation and Related Information

Obtaining Software Images and Other Tools

To access the self-service portal and obtain software, documents, and tools, do the following:

1. Go to the following URL:
   http://www.cisco.com/en/US/partner/products/ps9688/tsd_products_support_series_home.html
2. Click the **Download Software** link.
3. Log in to the Cisco Support Center. You must be a registered user of Cisco.com to access this page. You must have a current Cisco support contract that is linked to your Cisco.com account to download software and obtain help from the Cisco Technical Assistance Center.
4. Click the link for the correct release, or use the search function to locate the software release.
5. Follow the onscreen instructions.

Tip You can also log in to the Cisco Support Center at http://www.cisco.com/support/.

Related Documentation

1. Go to one of the following URLs:

- Cisco Physical Access Manager Documentation
  http://www.cisco.com/en/US/products/ps9688/tsd_products_support_series_home.html
- Cisco Physical Access Gateway
  http://www.cisco.com/en/US/products/ps9687/tsd_products_support_series_home.html

2. Click the link for the appropriate guide.

   For example: **Install and Upgrade Guides** or **End-User Guides**.

3. Use these publications to learn how to install and use the Cisco Physical Access Control.

For example, this page includes links to the following documentation:

- Cisco Physical Access Control API Reference Guide
- Cisco Physical Access Manager User Guide
- Cisco Physical Access Manager Quick Start Guide
- Cisco Physical Access Gateway Quick Start Guide
- Cisco Physical Access Gateway User Guide
- Cisco Physical Security Multiservices Platform Series User Guide
- Cisco Physical Access Manager Migration Guide
- Cisco Physical Access Manager Deployment Guide

Data Sheets and Other Information

To obtain data sheets and other important information about the Cisco Physical Access Gateway, Cisco Physical Access Manager and other optional modules, do the following:

1. Go to the following URL:
   http://www.cisco.com/go/physicalsecurity
2. Click the **Products** link.
3. Click the **Cisco Physical Access Control** link.
4. Select **Cisco Physical Access Control Hardware** or **Cisco Physical Access Control Software**.

Submitting a Service Request and Additional Information

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.

Installation Notes

For installation of UCS C220 server, please refer "Installing the Cisco Connected Safety and Security UCS C220 Server In a Rack" section in Cisco Connected Safety and Security UCS Platform Series User Guide.

Caveats

Unresolved Caveats

Table 2 lists the unresolved caveats in Cisco PAM Release 1.5.2. Click the identifier to view additional descriptions, status or workaround information for each issue.This information is displayed in the Bug Search Tool. You can track the status of the unresolved caveats using the Bug Search Tool.

Table 2 Unresolved Caveats for Cisco Physical Access Control Release 1.5.2

Identifier	Headline and Bug Toolkit
CSCuo83272	CPAM Mysql Bin files occupying the entire space when Stand-by is absent.
CSCul97024	Default columns values are not set for default reports.
CSCul53111	Gateway & Door Status is not populated in CPAM client UI.
CSCuj90739	Peerbad record MAC.
CSCul77903	OutOfMemoryError - Apply cfg for 1000 GW's through Global IO.
CSCuh40768	Audit Trial events not been generated for custom fields.
CSCug64012	WSAPI:SPL Case needs to be supported by various schedule related APIs.

Table 2 Unresolved Caveats for Cisco Physical Access Control (continued)Release 1.5.2

Identifier	Headline and Bug Toolkit
CSCul35210	CPAM Client is not responding.
CSCul62691	CreateTEC API allows to push parallel location objects for a profileUser.
CSCua44458	CPAM server hits out of memory exception.
CSCua707643	CPAM Client throws Fatal error when opening modules.

Resolved Caveats

Table 3 lists the issues that were resolved in Cisco PAM Release 1.5.2. Click the identifier to view additional descriptions, status or workaround information for each issue.This information is displayed in the Bug Search Tool. You can track the status of the resolved caveats using the Bug Search Tool.

Table 3 Resolved Caveats for Cisco Physical Access Control Release 1.5.2

Identifier	Headline and Bug Toolkit
CSCum70671	Events photo module failed to open for MostRestrictedProfile login user.
CSCuo92848	Access Level is not listed at certain condition.
CSCui91226	Client crashed after the report setting is changed.
CSCum95228	Expansion modules are not removed from hardware module.
CSCum09534	Access Policy is deleted when modifying the Access Policy Name.
CSCum17453	Heartbeat fails to start in standby, after Active n/w re-connection.
CSCul80726	Few gateways is reconnecting during credential download to huge gateways.
CSCuq37763	Credential Purging wrong behavior.

Table 3 Resolved Caveats for Cisco Physical Access Control Release 1.5.2

Identifier	Headline and Bug Toolkit
CSCuq11452	Badges created w/o Cred-template id & Role in Single screen badge wizard.
CSCuq75700	Credentials fail to push when there is communication problem btw CPAM/GW.
CSCur05357	Cisco Physical Access Manager / eval for CVE-2014-6271 and CVE-2014-7169
CSCuo96709	CPAM Client Audio Alarms Don't Stop in Restricted Profiles.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.