CHAPTER 2

New and Changed Information

The Cisco Physical Access Control Release 1.4.1 is backward compatible with the Cisco Physical Access Control 1.3.x and 1.2.x releases. The services that worked with Cisco Physical Access Control 1.3.x continue to work with Access Control 1.4.1.

This chapter summarizes the new and changed features in the Cisco Physical Access Control 1.4.1 release, and provides information on where the feature is documented. For more information on the Cisco Physical Access Control 1.4.1 release, see http://www.cisco.com/en/US/products/ps9688/prod_release_notes_list.html.

Contents

Profile Enhancements

The profile enhancements is a new feature that enriches user profile by enabling location constraints that restricts the access of the logged in user to their locations alone. This feature can be set across several modules.The default hierarchy of a location is:

Base > Campus > Building > Floor > Area > Subarea

The enriched user profile feature is activated under the following conditions:

- Profile may not restrict by hierarchical location
- Allow profiles to be bound to hierarchical locations per assignment

On setting these conditions the system property changes, For more information, see Data Entry/Validation - Login, page 17-9. It displays fields and values that are applicable to the assigned area/location to the profile that is associated to the user. Thus, a user can be associated to several profiles and the one with higher privileges is applied to the login user.

The profile enhancement feature impacts the following modules:

Table 1 Modules impacted by Profile enhancements

No	Module	Reference
1	Login	Creating User Login Accounts and Assigning Profiles, page 5-8
2	Profiles	Defining User Profiles for Desktop Application Access, page 5-2
3	Locations and Doors	Locations and Doors in Cisco PAM 1.4.1, page 6-9
4	Access Policy, Schedule, Holiday, Work Weeks and Time entry collections	Access Policies in Cisco PAM 1.4.1, page 11-4 Schedule Manager in Cisco PAM 1.4.1, page 11-11
5	Device Groups	Device Groups in Cisco PAM 1.4.1, page 7-34
6	Two-Door Policy/APB	Two-Door Policies in Cisco PAM 1.4.1, page 11-27 Anti-Passback areas in Cisco PAM 1.4.1, page 11-19
7	Events and Alarms	Events and Alarms in Cisco PAM 1.4.1, page 12-3
8	Event Policy Manager	Event Policy Manager in Cisco PAM 1.4.1, page 12-30
9	Hardware Manager	Hardware Manager in Cisco PAM 1.4.1, page 6-5
10	Report Manager	Report Manager in Cisco PAM 1.4.1, page 13-39
11	Global/IO	Automation Rules in Cisco PAM 1.4.1, page 13-35
12	Graphic Maps	Graphic Maps in Cisco PAM 1.4.1, page 12-40
13	Camera Manager	Camera Manager in Cisco PAM 1.4.1, page 15-1

VTG Integration

The Cisco PAM Server supports use of IP Phone services to grant access to doors. External system can be integrated with Cisco PAM using HTTP. IP Phones can be integrated with Cisco PAM using HTTP service. The integration of VoIP phone to Cisco PAM enables users to grant access to doors through the VoIP phone. This new feature of Cisco PAM allows the entry of personnel without badges.

For more information see, VoIP Integration.

VSM 7.0 Integration

The Cisco PAM integrates with new VSM 7.0. while retaining its support to VSM 6x camera driver. However, at any given point of time, only one driver can be configured and associated with the camera device.

There following GUI level differences between the 6x and 7x camera drivers are:

- Configuring to the VSM server
- Grid Arrangement Options
- Default classification of the camera devices to System folder in 7x
- Viewing the event options

For more information see, Camera Manager in Cisco PAM 1.4.1, page 15-1.

Debounce Timer

The input devices like a door sensor can generate multiple spurious events due to technical defect, or due to vibrations. To prevent spurious events getting logged, a debounce timer can be used to mask events for a specified time interval. The debounce timer ensures that any event that is repeated till a given time is ignored. If the condition persist beyond the time, then the alarm is logged.

For more information, see Debounce Timer, page 8-36.

Badge Authentication

Badge authentication is to validate whether the badge being issued be authenticated for the selected door in the given futuristic timestamp.

For more information, see Badge Authentication, page 9-36.

Multifactor Authentication

The user can integrate additional access control devices like biometric devices with the Cisco PAM to ensure security. These devices are configured as Generic Readers in Cisco PAM server.

For more information, see Multifactor Authentication.

Virtual Machine Ware

Virtual Machine (VM) support is only on UCS Express and UCS C-series. The manufacturing SKU for VM image is done by downloading the software and documentation from CCO, the order and license details are delivered through email.

Currently VM ware supports 20 simultaneous connections for this release.

For more information, see Configuring Cisco PAM on Virtual Machine (VM), page 3-16.