CHAPTER 17

System Configuration Settings

This chapter describes the system-wide site settings available in the System Configuration module. The System Configuration module includes additional settings through which an user profile can be associated to a location hierarchy. This feature allow the users to control or execute actions on locations and sub locations mapped to their user profile. See Data Entry/Validation - Login, page 17-10

Note We recommend restricting access to the **System Configuration** module to administrators only.

To modify the system configuration settings, do the following:

Step 1 Select **System Configuration** from the Admin menu.

Step 2 Select a configuration topic from the tabs on the left (Figure 17-1).

Step 3 Enter the settings and configurations as described in the sub-sections listed below.

Step 4 Click **Save** to save changes made in a system configuration window.

Step 5 Log out and log back in to the Cisco PAM application to activate the changes (select Logout from the Options menu).

Note Changes to system configuration settings do not take effect until you stop and start the Cisco PAM application. For some settings in the Cisco Settings window, you must restart the Cisco PAM appliance. See the “Cisco Settings” section on page 17-22 for more information.

Contents

- LDAP Settings, page 17-3
- Event/Alarms Settings, page 17-5
- Data Entry/Validation - Personnel Settings, page 17-6
- Data Entry/Validation - Badge Settings, page 17-8
- Data Entry/Validation - Login, page 17-10
- Password Policy Settings, page 17-11
- Custom Device Fields Settings, page 17-14

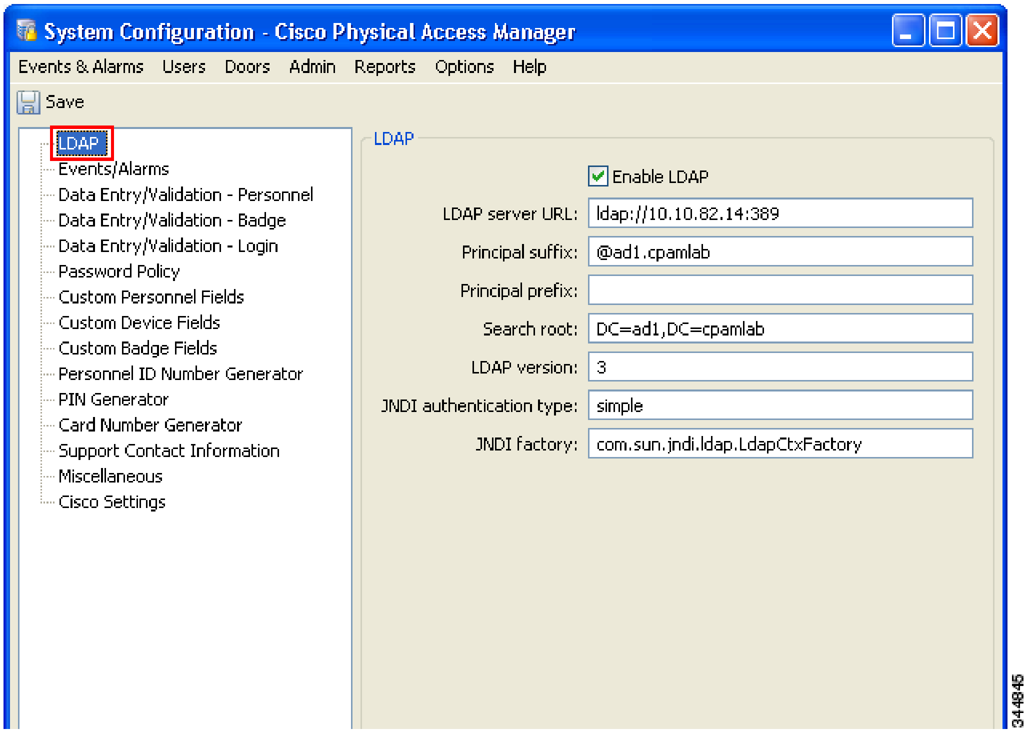
- Custom Badge Fields, page 17-15
- Personnel ID Number Generator, page 17-16
- PIN Generator, page 17-17
- Card Number Generator, page 17-18
- Support Contact Information, page 17-19
- Miscellaneous Settings, page 17-20
- Cisco Settings, page 17-22

LDAP Settings

The LDAP options (Figure 17-1) include login validation settings required to use the Lightweight Directory Access Protocol. See Table 17-1 for field descriptions.

Tip For more information, see Configuring LDAP User Authentication, page 5-12.

Figure 17-1 LDAP Settings



LDAP

☑ Enable LDAP

LDAP server URL:	ldap://10.10.82.14:389
Principal suffix:	@ad1.cpamlab
Principal prefix:	
Search root:	DC=ad1,DC=cpamlab
LDAP version:	3
JNDI authentication type:	simple
JNDI factory:	com.sun.jndi.ldap.LdapCtxFactory

LDAP uses a principle to authenticate. The principle is formed from the username: prefix + username + suffix. The exact format of the principle varies based on the type of LDAP server, and the domain.

- For Active Directory, the prefix should be the (uppercase) domain followed by \\ (example: MY-DOMAIN\\) and the suffix should be blank.
- For OpenLDAP, the prefix should be: uid=
  The suffix should be changed to reflect the actual domain.
  So for my-domain.com, this would be:
  ,dc=my-domain,dc=com

Table 17-1 describes the LDAP settings:

Table 17-1 System Configuration LDAP Settings

Field	Description
Enable LDAP	Click the check box to enable or disable LDAP support.
LDAP server URL	URL of LDAP server, must begin with `ldap://` Example: `ldap://192.168.1.1`

Table 17-1 System Configuration LDAP Settings (continued)

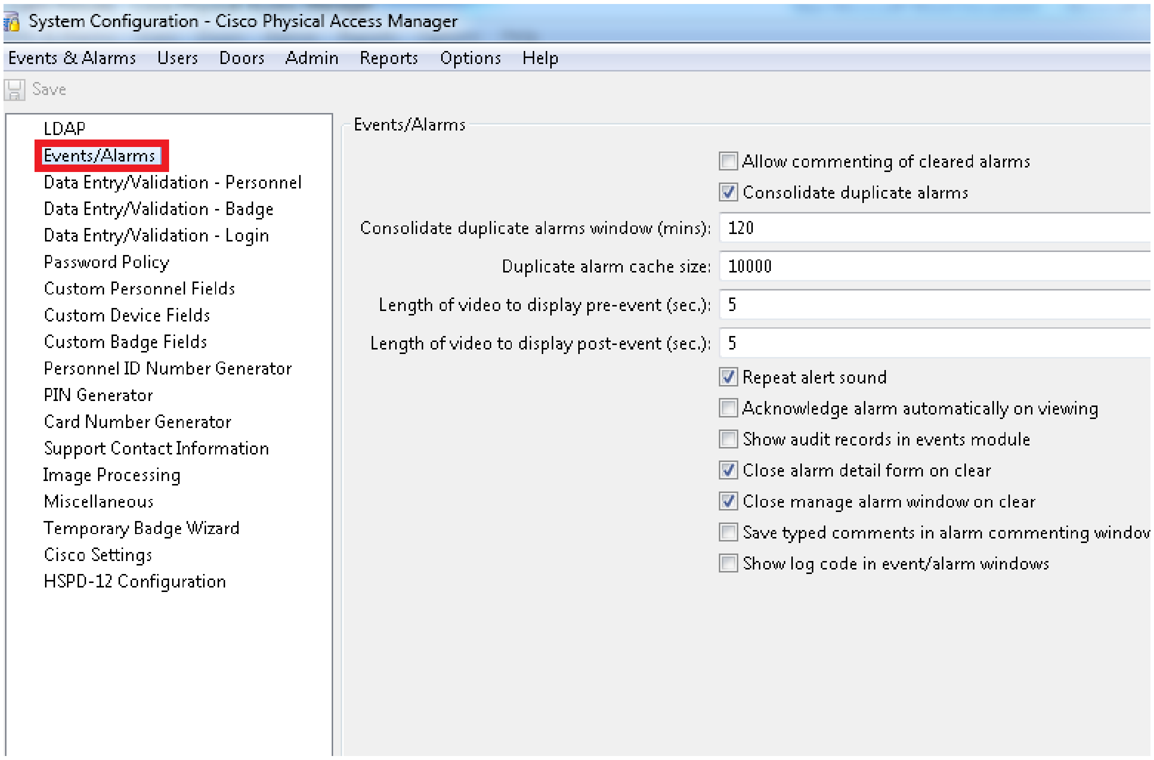
Field	Description
Principle suffix	Appended to the username for authentication. See above.
Principle prefix	Prepended to the username for authentication. See above.
Search root	LDAP search root. The search root is the node in the LDAP tree, the subtree under which the user account should be found. • For Active Directory, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com: `cn=Users,dc=my-domain,dc=com`. • For OpenLDAP, the 2 dc components should be changed to match the full domain name managed by the directory. The following example is for my-domain.com:`dc=my-domain,dc=com.`
LDAP version	Advanced setting that generally should be left unchanged.
JNDI authentication type	Advanced setting that generally should be left unchanged as `simple`.
JNDI factory	Advanced setting that generally should be left unchanged as `com.sun.jndi.ldap.LdapCtxFactory`

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Event/Alarms Settings

Use the Events/Alarms tab (Figure 17-2) to define how alarms are managed by the system, and how much video is recorded for events.

Figure 17-2 Events/Alarm Settings



Events/Alarms

☐ Allow commenting of cleared alarms

☑ Consolidate duplicate alarms

Consolidate duplicate alarms window (mins): 120

Duplicate alarm cache size: 10000

Length of video to display pre-event (sec.): 5

Length of video to display post-event (sec.): 5

☑ Repeat alert sound

☐ Acknowledge alarm automatically on viewing

☐ Show audit records in events module

☑ Close alarm detail form on clear

☑ Close manage alarm window on clear

☐ Save typed comments in alarm commenting windov

☐ Show log code in event/alarm windows

Table 17-2 describes the Event and Alarms settings.

Table 17-2 System Configuration Alarm Fields

Field	Description
Allow commenting of cleared alarms	Allow operators to comment on alarms that have already been cleared.
Consolidate duplicate alarms window (mins)	If duplicate alarms are being consolidated, this is the maximum time difference between the original and the duplicate. If an alarm that would otherwise be considered a duplicate occurs after this time, it becomes a new original alarm and subsequent duplicate alarms will bump up its duplicate count.
Consolidate duplicate alarms	Consolidate duplicate alarms identical other than time, into a single alarm, with an increasing alarm count. This is useful for preventing a flood of individual alarms; for example, if an armed alarm point is on an external gate which is flapping in the wind, repeatedly triggering the alarm. It is not recommended that this be unchecked without careful consideration of the possible performance impact of the increased number of individual alarms.
Duplicate alarm cache size	The size of the cache for duplicate alarms.

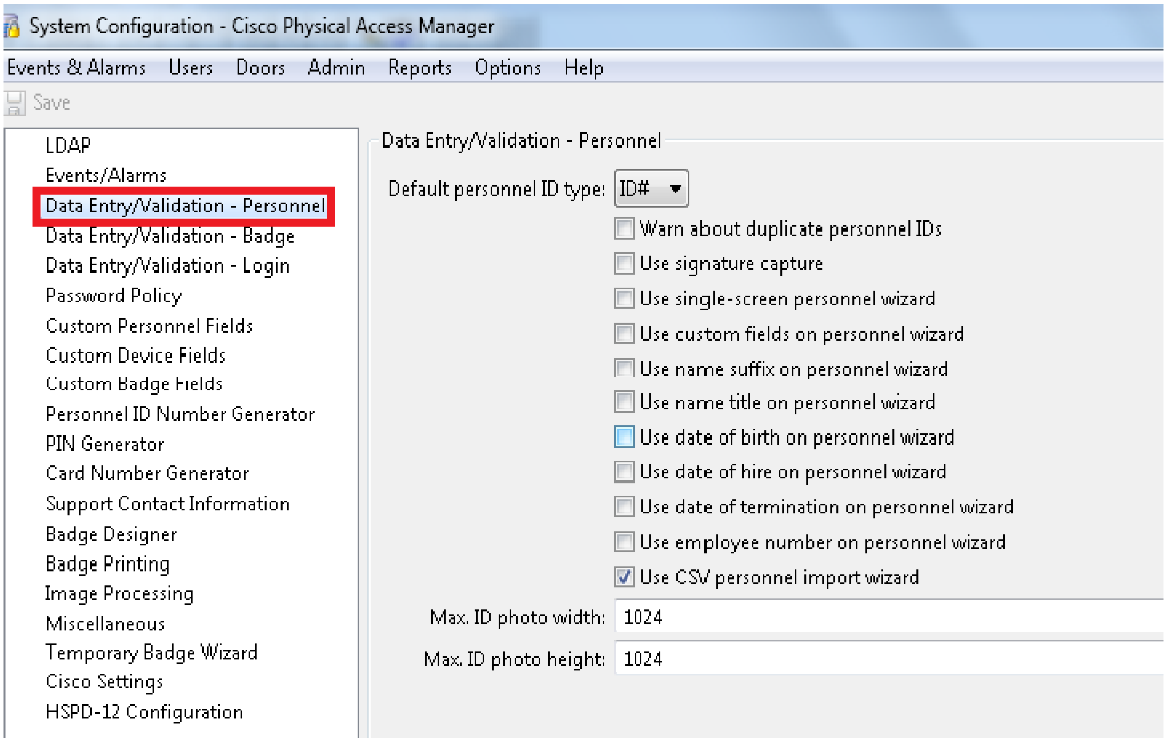
Table 17-2 System Configuration Alarm Fields (continued)

Field	Description
Length of video to display pre-event	The number of seconds of video that are included before the event occurred.
Length of video to display post-event	The number of seconds of video that are included after an event occurs.
Repeat alert sounds	Defines if alarms sounds are played only once, or repeated.
Show audit records in events	Lists the audit records of events.

Note Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

Data Entry/Validation - Personnel Settings

Figure 17-3 Personnel Data Entry Settings



Data Entry/Validation - Personnel

Default personnel ID type: ID#

□ Warn about duplicate personnel IDs
□ Use signature capture
□ Use single-screen personnel wizard
□ Use custom fields on personnel wizard
□ Use name suffix on personnel wizard
□ Use name title on personnel wizard
□ Use date of birth on personnel wizard
□ Use date of hire on personnel wizard
□ Use date of termination on personnel wizard
□ Use employee number on personnel wizard
☑ Use CSV personnel import wizard

Max. ID photo width: 1024

Max. ID photo height: 1024

Table 17-3 describes the Data Entry/Validation - Personnel settings.

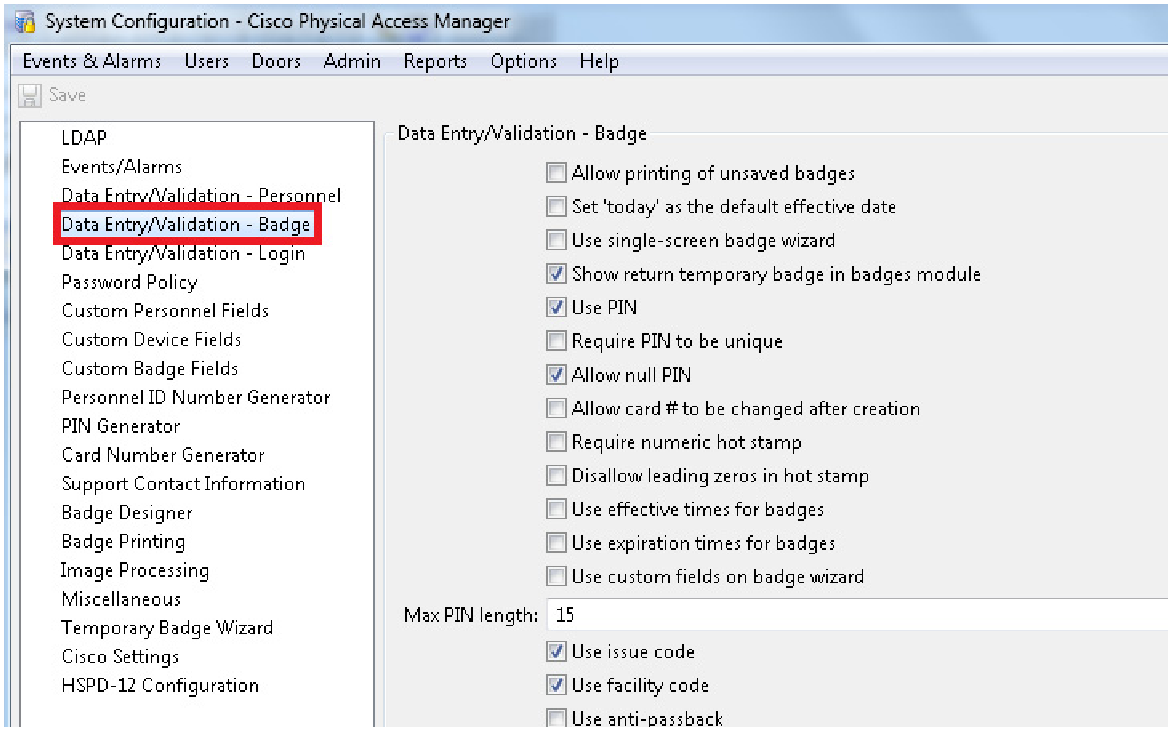
Table 17-3 Data Entry/Validation - Personnel Settings

Field	Description
Default personnel ID specifier	The type of personnel ID specifier the field will default to. The various ID specifiers will be available in the drop-down.
Warn about duplicate personnel IDs	Warn if personnel are added with duplicate personnel IDs.
Use signature capture	Enable the ability to capture personnel signatures with a signature capture device. Signature capture devices must be configured in the application preferences before they may be used. See Enabling Signature Capture Devices, page 9-54.
Use single-screen personnel wizard	Enables a single-screen personnel wizard used for personnel data entry. All personnel information is available on one screen.
Use custom fields on personnel wizard	Enable custom fields in the single-screen personnel wizard. This makes the screen larger, but is useful if important data is being stored in the custom fields. Refer to custom fields in the **Custom Personnel Fields** window.
Use name suffix on personnel wizard	Choose a value from the drop-down menu (such as I, II, III, Jr., and Sr.) or enter the text manually to add suffix at the end the person's name.
Use name title on personnel wizard	Choose a value from the drop-down menu (such as Dr., Mr., or Ms.) or enter the text manually to add a person's formal title.
Use date of birth on personnel wizard	The person's date of birth.
Use date of hire on personnel wizard	The date the employee was hired.
Use date of termination on personnel wizard	The date the employee was terminated.
Use employee number on personnel wizard	The employee number, if applicable. Generally, but not required to be, unique.
Use CSV personnel import wizard	Enables the CSV import wizard in the personnel module. The CSV import wizard allows operators to add personnel to Cisco Physical Access Manager using a CSV file. See Importing Personnel Records Using a Comma Separated Value (CSV) File, page 9-14.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Data Entry/Validation - Badge Settings

Figure 17-4 Badge Data Entry Settings



Data Entry/Validation - Badge

- □ Allow printing of unsaved badges
- □ Set 'today' as the default effective date
- □ Use single-screen badge wizard
- ☑ Show return temporary badge in badges module
- ☑ Use PIN
- □ Require PIN to be unique
- ☑ Allow null PIN
- □ Allow card # to be changed after creation
- □ Require numeric hot stamp
- □ Disallow leading zeros in hot stamp
- □ Use effective times for badges
- □ Use expiration times for badges
- □ Use custom fields on badge wizard

Max PIN length: 15

- ☑ Use issue code
- ☑ Use facility code
- □ Use anti-passback

Table 17-4 describes the Data Entry/Validation - Badge settings.

Table 17-4 Data Entry/Validation - Badge Settings

Field	Description
Allow printing of unsaved badges	Allows printing new badges before the badge is saved. For highest security, leave this unchecked. When allowed (which may be more convenient), it is possible to print a badge without having any record of the badge.
Set 'today' as the default effective date	Uses the current date as a new badge effective date.
Use single-screen badge wizard	Enables a single-screen badge wizard for data entry. Most badge properties are on one screen.
Show return temporary badge in badge module	Displays return badge field in the badge module window if the field is checked.
Use PIN	A PIN associated with the badge. Depending on the configuration of an access point, the pin is entered into the keypad on the access point's reader.
Require PIN to be unique	Requires cardholder PINs to be unique. Useful in systems that use PIN-only access-control.
Allow null PIN	Allows badges to have null PINs. Useful in systems that do not use PIN for access-control.

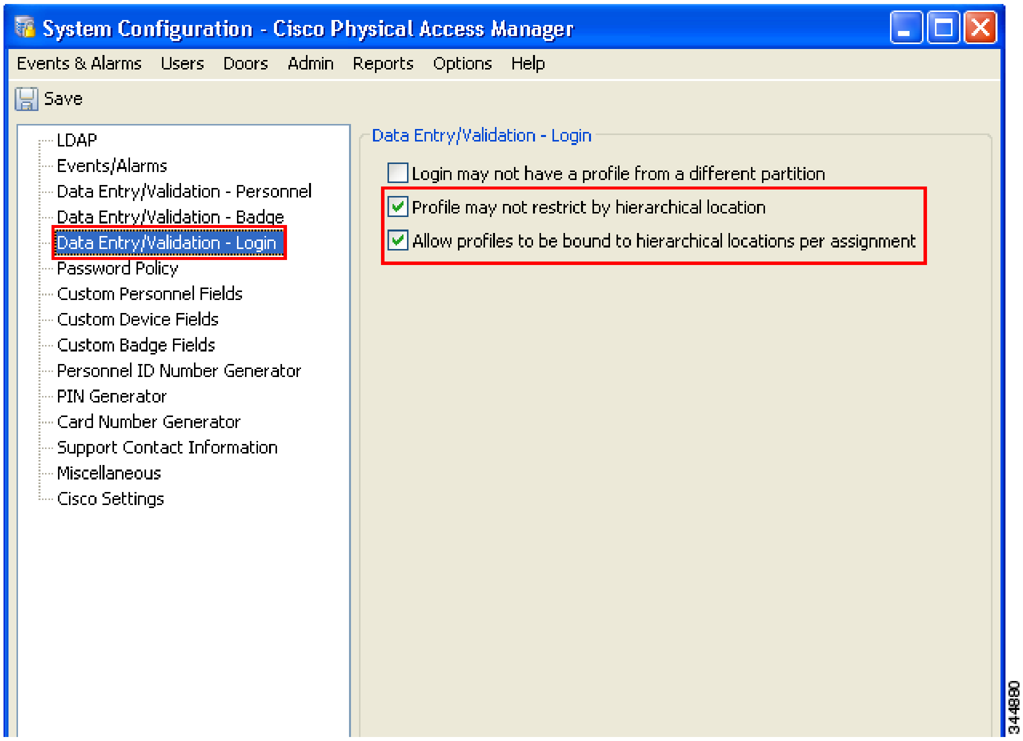
Table 17-4 Data Entry/Validation - Badge Settings (continued)

Field	Description
Allow card # to be changed after creation	Also known as a badge. A type of credential encoded with a card number, generally on a magnetic stripe or a proximity card, and used to enter access points.
Require numeric hot stamp	Requires hot stamp field to be numeric.
Disallow leading zeros in hot stamp	Prohibits users from adding hot stamps with leading zeros.
Use effective times for badges	Select this check box to enable the effective time constraint for badges, in addition to effective date, which is always enabled.
Use expiration times for badges	Select this check box to enable the expiration time constraint for badges, in addition to effective date, which is always enabled.
Use custom fields on badge wizard	Enables custom fields in the badge wizard. This makes the screen larger, but is useful if important data is being stored in the custom fields.
Max PIN Length	The maximum number of characters in a PIN.
Use issue code	Displays the issue code field in the single screen badge wizard if the field is checked.
Use facility code	A segment of bits encoded on a card that represents a number for a facility. Often all cards issued for a single facility have the same facility code.
Use anti-passback	Enables the badge holder to be anti-passback exempt during the next reader use. After enabling this option "Grant one free APB button" is displayed in the badges.
Use anti-passback exemption	Enables the badge to be exempt from anti-passback enforcement if the access point is configured for anti-passback. After enabling this option "exempt from anti-passback" is displayed in the badges.

Note Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

Data Entry/Validation - Login

The profile enhancement feature is set in this page. This configuration setting facilitates the administrator to link a user profile to hierarchial location.Data Entry/Validation - Login Settings


System Configuration - Cisco Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Save
LDAP
Events/Alarms
Data Entry/Validation - Personnel
Data Entry/Validation - Badge
Data Entry/Validation - Login
Password Policy
Custom Personnel Fields
Custom Device Fields
Custom Badge Fields
Personnel ID Number Generator
PIN Generator
Card Number Generator
Support Contact Information
Miscellaneous
Cisco Settings
Data Entry/Validation - Login
344930

☐ Login may not have a profile from a different partition

☑ Profile may not restrict by hierarchical location

☑ Allow profiles to be bound to hierarchical locations per assignment

Table 17-5 describes the Data entry Validation - Login Settings

Table 17-5 Data entry Validation - Login Settings

Field	Description
Login may not have a profile from a different partition	Not supported in this version
Profile may not restrict by hierarchial location	select this check box if you do not want user profiles to be restricted by hierarchial locations
Allow profile to be bound to hierarchial locations per assignment	select this check box if you want user profiles to be restricted by hierarchial locations

On setting these changes , the system configuration settings changes i.e a user is able to associate a location to a login thereby granting privileges to the login user for devices in that location. Also a a user can be associated to several profiles and the one with higher privileges is applied to the login user.

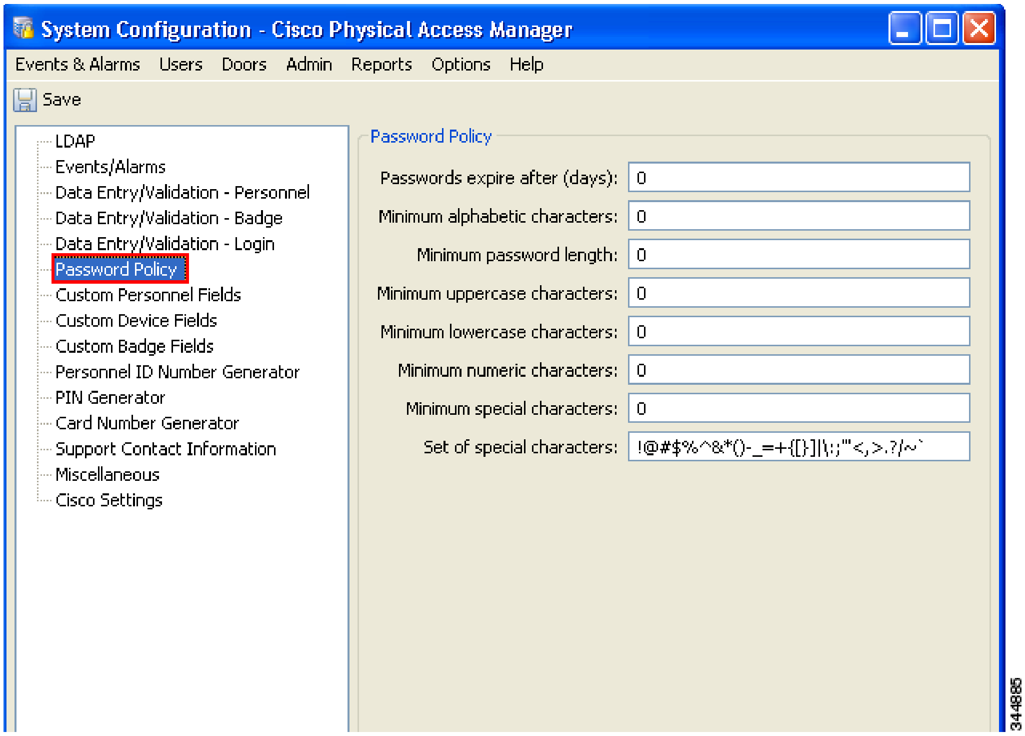
Tip You must select both Profile may not restrict by hierarchial location and Allow profile to be bound to hierarchial locations per assignment to associate profiles to hierarchial location.

Note If the user does not select the fields that associate profiles to locations, the user profile actions are not restricted to the locations or sub locations that they belong to. The configuration settings would then reflect the Cisco Physical Access Manager 1.3 release.

Password Policy Settings

The Password Policy options (Figure 17-5) determine password expiration and strength requirements.

Figure 17-5 Password Policy Settings



Passwords expire after (days): 0
Minimum alphabetic characters: 0
Minimum password length: 0
Minimum uppercase characters: 0
Minimum lowercase characters: 0
Minimum numeric characters: 0
Minimum special characters: 0
Set of special characters: !@#$%^&*()-_=+{[}]|\:;'"<,>.?/~`

Table 17-6 describes the Password Policy settings.

Table 17-6 System Configuration Password Policy Fields

Field	Description
Passwords expire after (days)	Passwords expire after this many days.
Minimum alphabetic characters	Minimum number of a to z characters or A to Z characters in the password.
Minimum password length	Minimum number of characters in the password.
Minimum uppercase characters	Minimum number of uppercase password characters.
Minimum lowercase characters	Minimum number of lowercase password characters.
Minimum numeric characters	Minimum number of numeric password characters.

Table 17-6 System Configuration Password Policy Fields (continued)

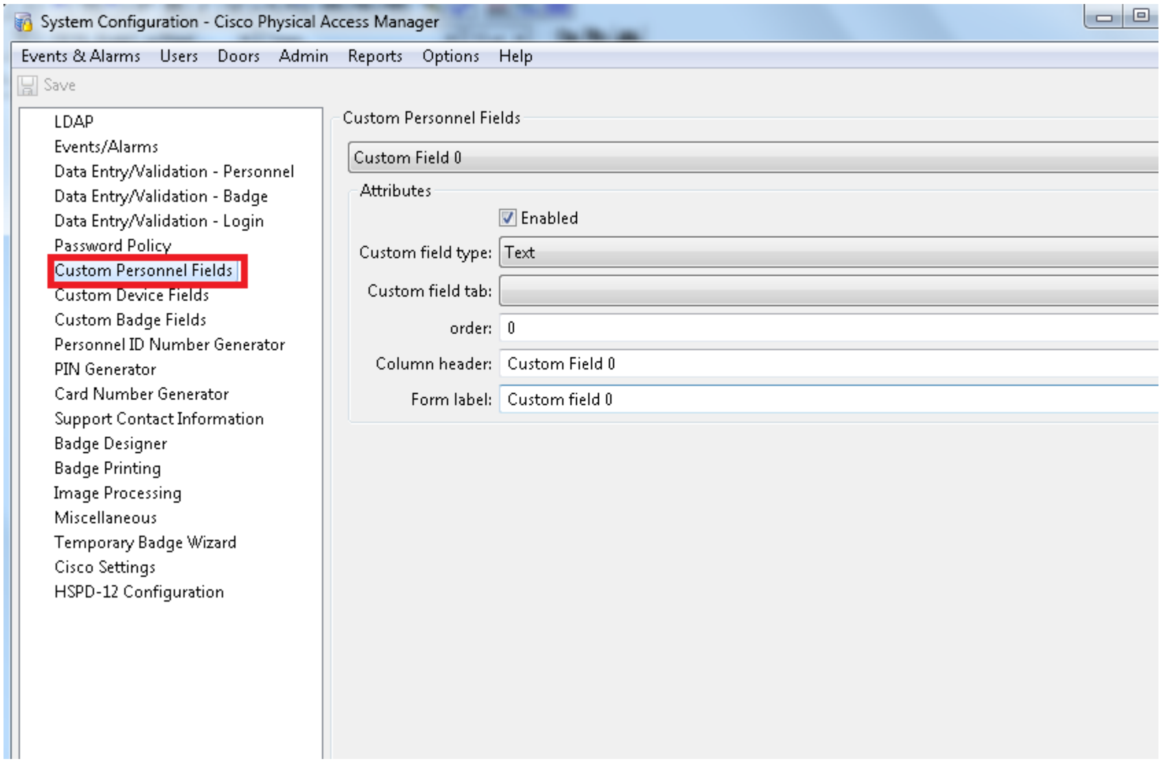
Field	Description
Minimum special characters	Minimum number of special characters in the set specified below.
Set of “special” characters	Which characters qualify as special characters for the above.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Custom Personnel Fields Settings

The Custom Personnel Fields defines the custom fields available in the personnel detail window.

Figure 17-6 Custom Personnel Fields



Custom Personnel Fields

Custom Field 0

Attributes

☑ Enabled

Custom field type: Text

Custom field tab:

order: 0

Column header: Custom Field 0

Form label: Custom field 0

Table 17-7 describes the Custom Personnel Fields settings.

Table 17-7 Custom Personnel Fields

Field	Description
Custom Personnel Field	Selects which of the available custom fields is to be viewed or edited.
Enabled	Select the check box to enable the selected custom field.

Table 17-7 Custom Personnel Fields (continued)

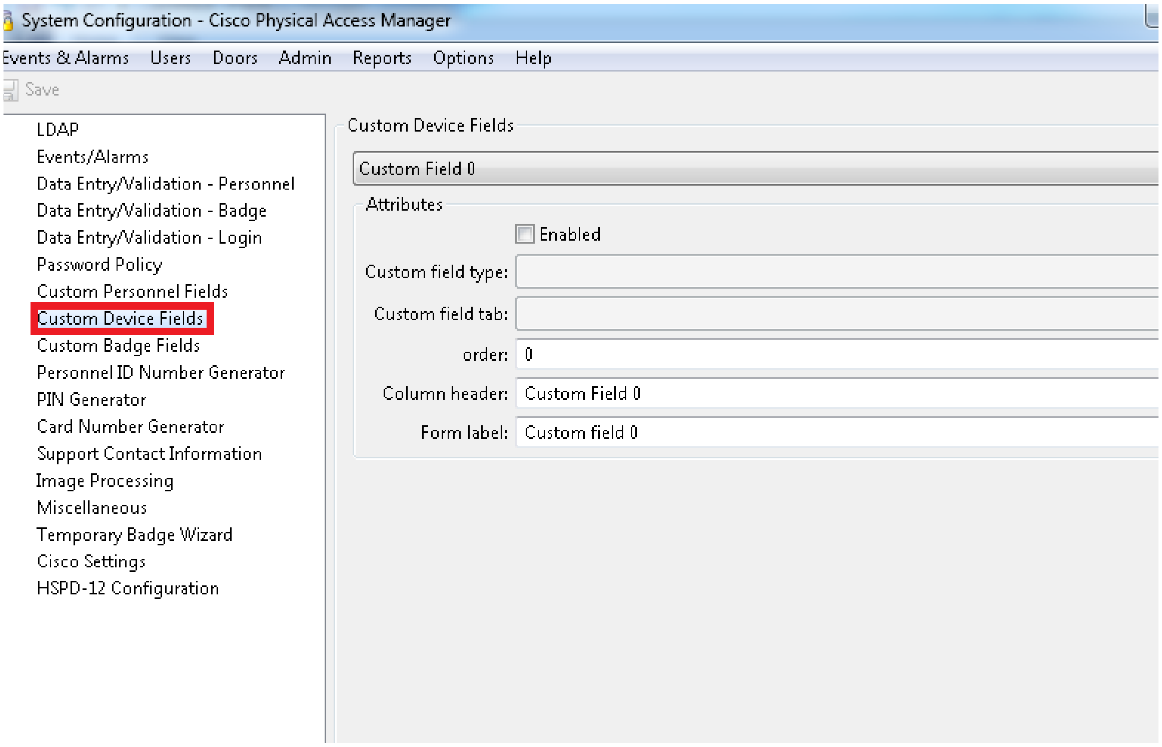
Field	Description
Custom field type	Displays the type of the custom field value (Example: Text, URL) to be associated with a custom field tab, and displays the selected type in the personnel and badges modules.
Custom field tab	Displays the custom field tab names in a drop-down list.
Order	Displays custom personal fields in numerical order in the personnel module custom field.
Column header	Changes the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized such as the title of a book, for example: Driver's License Number.
Form label	Changes the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like the a sentence, for example: Driver's license number.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Custom Device Fields Settings

Configures which the custom fields which are available in the device detail window.

Figure 17-7 Custom Device Fields



Custom Device Fields

Custom Field 0

Attributes

□ Enabled

Custom field type:

Custom field tab:

order: 0

Column header: Custom Field 0

Form label: Custom field 0

Table 17-8 describes the Custom Device Fields settings.

Table 17-8 Custom Device Fields Settings

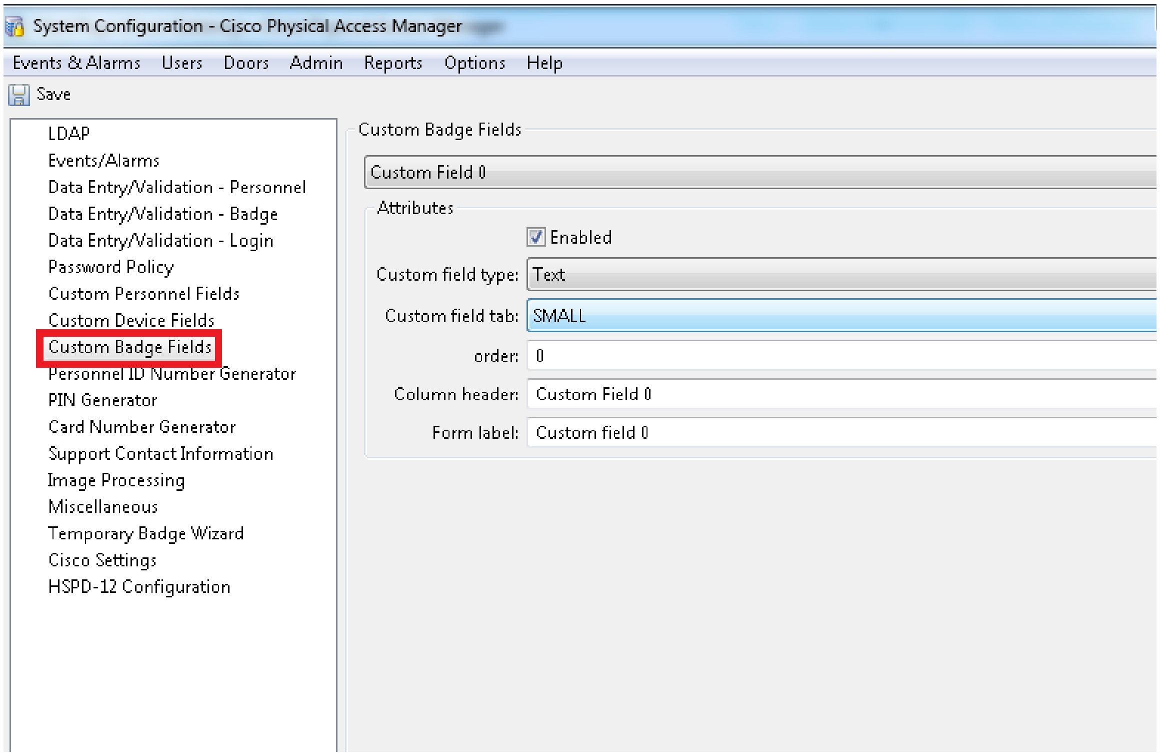
Field	Description
Custom Device Fields	Selects which of the available custom fields is to be viewed or edited.
Enabled	Select the check box to enable the selected custom field.
Drop down	Select the check box to use a drop-down for entry the selected custom field.
Column header	Change the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like the title of a book, for example, Serial Number.
Form label	Change the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like the a sentence, for example, Serial number.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Custom Badge Fields

Configures which the custom fields which are available in the badge detail window.

Figure 17-8 Custom Badge Settings



Custom Badge Fields

Custom Field 0

Attributes

☑ Enabled

Custom field type: Text

Custom field tab: SMALL

order: 0

Column header: Custom Field 0

Form label: Custom field 0

Table 17-9 Custom Badge Fields

Field	Description
Custom Badge Fields	Selects which of the available custom fields is to be viewed or edited.
Enabled	Select the check box to enable the selected custom field.
Custom field type	Added custom field tab value is displayed in “custom field tab” drop down list of personal module and badge module.
Custom field tab	Add Custom field tabs value in custom field tabs window (Example: Admin>>Custom Field Tabs>>Add) to display custom field tab value in personal module and badge module
Order	Displays custom personal fields in order in the personnel module custom field.

Table 17-9 Custom Badge Fields (continued)

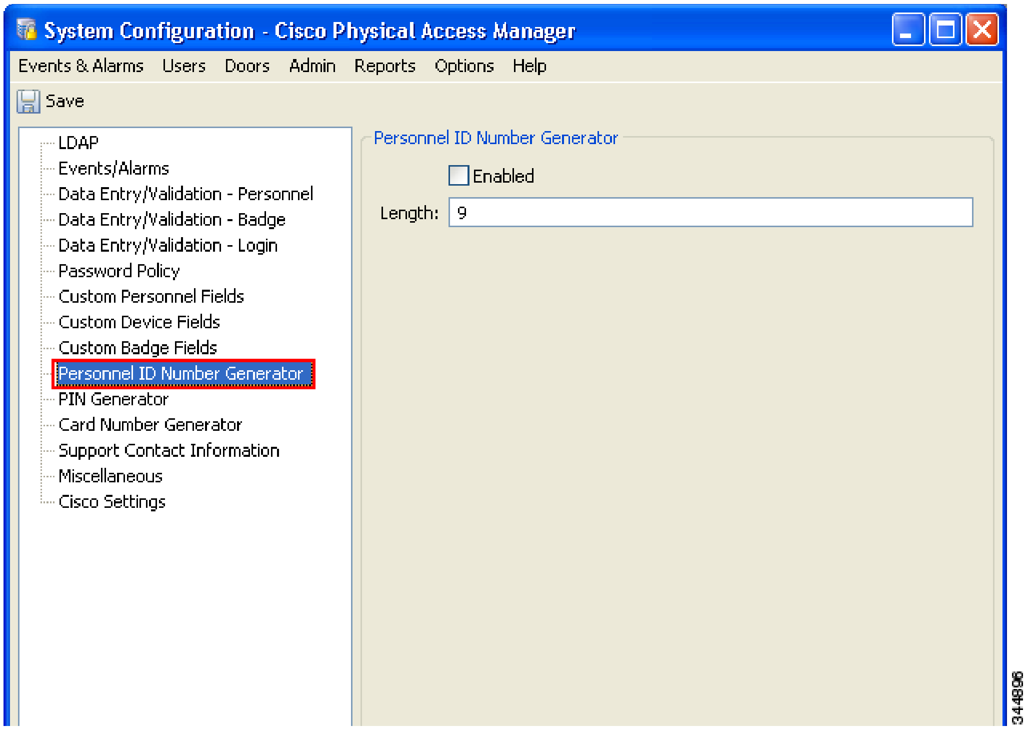
Field	Description
Column header	Changes the name of the column header of the selected custom field. The column header is displayed in list view columns. To be consistent with the rest of the application, this would be capitalized like the title of a book, for example: Serial Number.
Form label	Changes the name of the form label of the selected custom field. The form label is displayed in detail window fields. To be consistent with the rest of the application, this would be capitalized like the a sentence, for example: Serial number.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Personnel ID Number Generator

The personnel ID number generator is used for generating random personnel ID numbers, and is useful when personnel IDs do not correspond to any pre-existing ID numbers, such as employee ID, Social Security Number.

Figure 17-9 Personnel ID Number Generator Settings


System Configuration - Cisco Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Save
LDAP
Events/Alarms
Data Entry/Validation - Personnel
Data Entry/Validation - Badge
Data Entry/Validation - Login
Password Policy
Custom Personnel Fields
Custom Device Fields
Custom Badge Fields
Personnel ID Number Generator
PIN Generator
Card Number Generator
Support Contact Information
Miscellaneous
Cisco Settings
Personnel ID Number Generator
344896

☐ Enabled

Length: 9

Table 17-10 Personnel ID Number Generator Settings

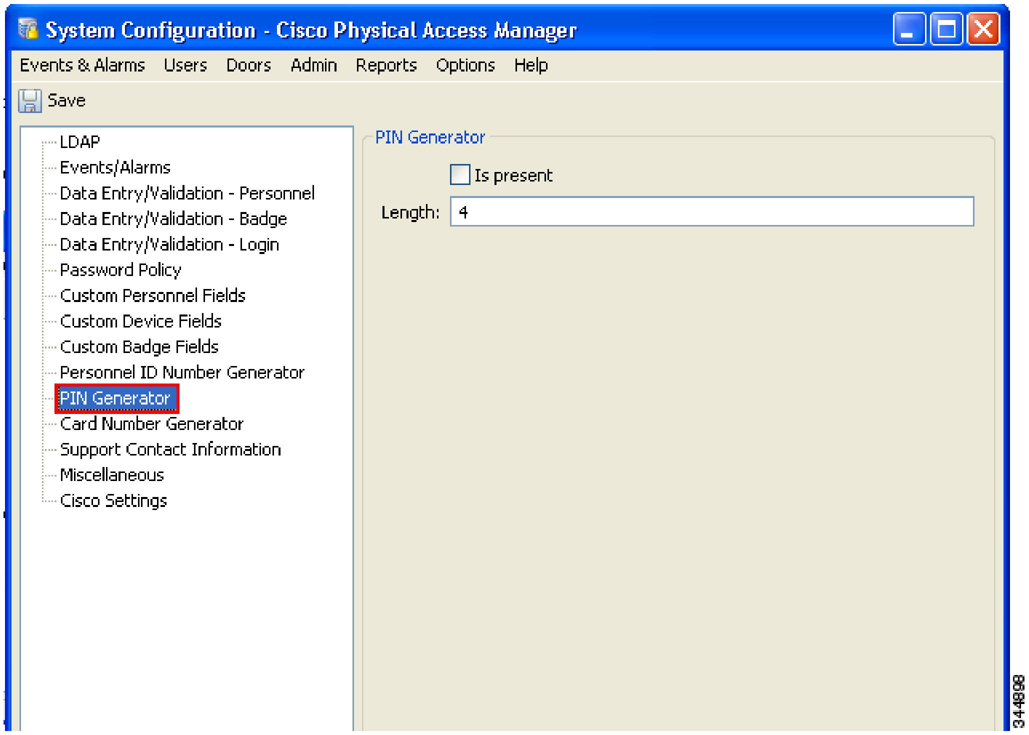
Field	Description
Enabled	Enables the personnel ID number generator. New personnel entries will have randomly generated ID numbers entered in the field.
Length	The digit length of generated IDs.

Note Changes to system configuration settings do not take effect until the Cisco PAM desktop application is restarted (exit and re-launch the application).

PIN Generator

Use the PIN generator to generate random PIN numbers for badges.

Figure 17-10 PIN Generator Settings



PIN Generator

☐ Is present

Length: 4

Table 17-11 PIN Generator Settings

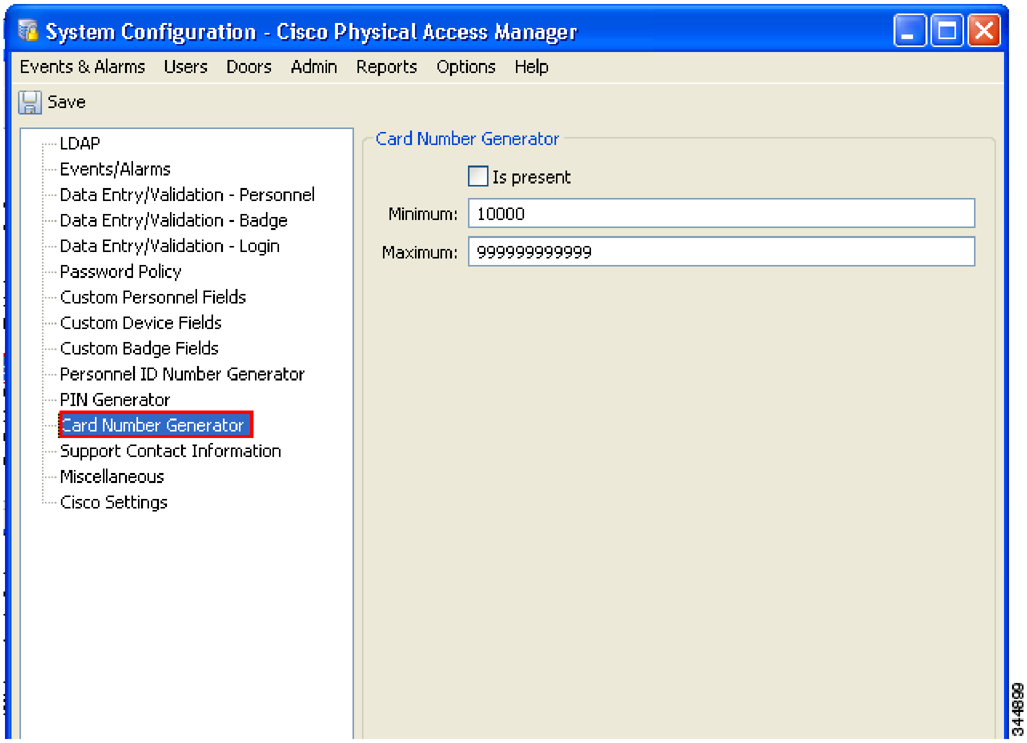
Field	Description
Is Present	Enable the personnel ID number generator. Adding new personnel will have randomly generated ID numbers entered in the field.
Length	The amount of digits in the generated PIN.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Card Number Generator

With the card encoder enabled the card number generator will create a card number with the minimum and maximum digits specified below.

Figure 17-11 Card Number Generator Settings



□ Is present

Minimum: 10000

Maximum: 999999999999

Table 17-12 Card Number Generator Settings

Field	Description
Is Present	Enables the card number generator. Adding new badges will have randomly generated card numbers entered in the **Card #** field.
Maximum	Maximum amount of card digits.
Minimum	Minimum amount of card digits.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Support Contact Information

Customer contact information is displayed in the **About** window available from the **Help** menu. It is intended to be customized with the dealer/installer/integrator's contact information, as this is often the first contact for support purposes.

Figure 17-12 Support Contact Information Settings

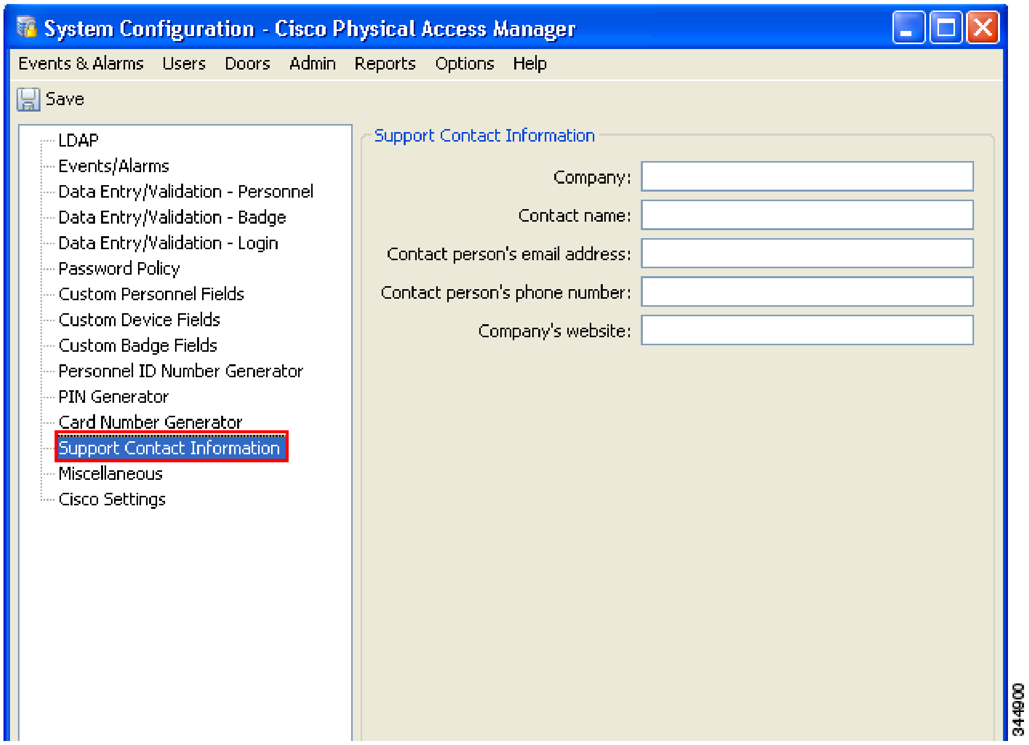

System Configuration - Cisco Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Save
LDAP
Events/Alarms
Data Entry/Validation - Personnel
Data Entry/Validation - Badge
Data Entry/Validation - Login
Password Policy
Custom Personnel Fields
Custom Device Fields
Custom Badge Fields
Personnel ID Number Generator
PIN Generator
Card Number Generator
Support Contact Information
Miscellaneous
Cisco Settings
Support Contact Information
Company:
Contact name:
Contact person's email address:
Contact person's phone number:
Company's website:
344900

Table 17-13 Support Contact Information Settings

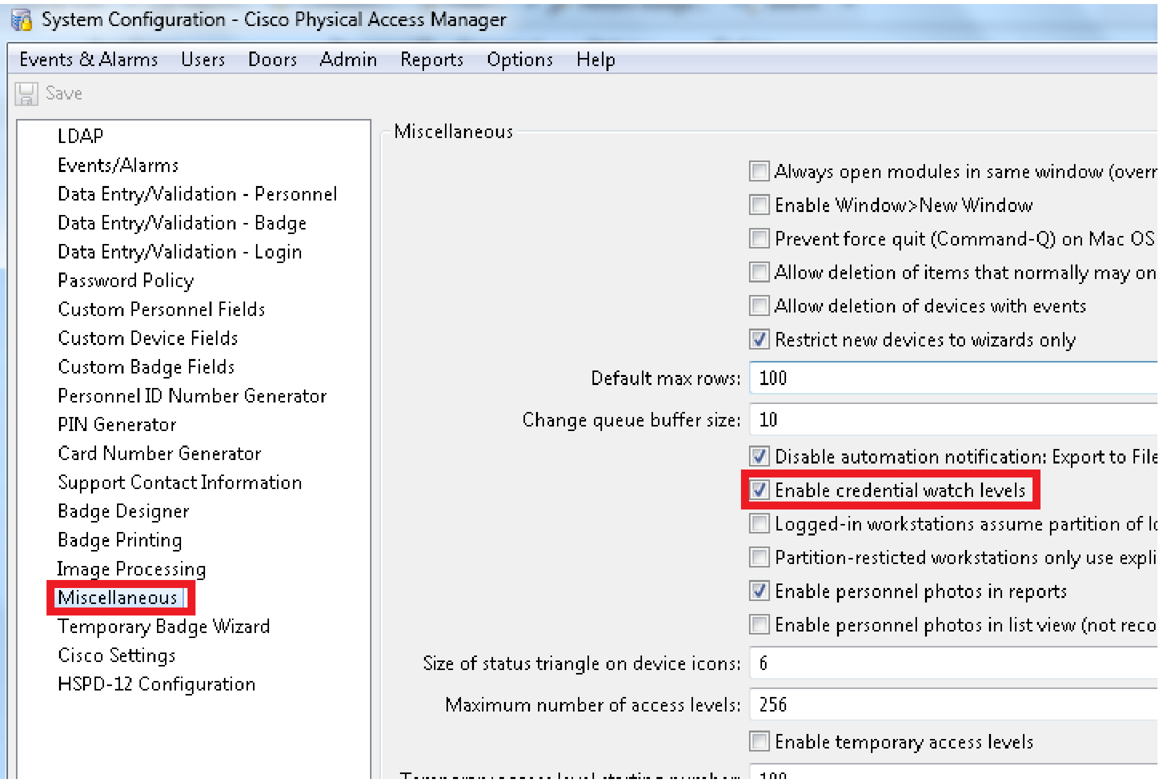
Field	Description
Company	Support company's name.
Contact name	The name of the contact person.
Contact person's email address	The contact person's email address.
Contact person's phone number	The contact person's phone number.
Company's website	Support company's company website address.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Miscellaneous Settings

Figure 17-13 includes a variety of settings, as described in Table 17-14.

Figure 17-13 Miscellaneous Settings



Miscellaneous

□ Always open modules in same window (overr

□ Enable Window>New Window

□ Prevent force quit (Command-Q) on Mac OS

□ Allow deletion of items that normally may on

□ Allow deletion of devices with events

☑ Restrict new devices to wizards only

Default max rows: 100

Change queue buffer size: 10

☑ Disable automation notification: Export to File

☑ Enable credential watch levels

□ Logged-in workstations assume partition of lo

□ Partition-resticted workstations only use expli

☑ Enable personnel photos in reports

□ Enable personnel photos in list view (not reco

Size of status triangle on device icons: 6

Maximum number of access levels: 256

□ Enable temporary access levels

Temporary access level starting number: 100

Table 17-14 Miscellaneous Setting fields

Field	Description
Always open new modules in same window	If checked, opening a new module simply replaces the module in the same window, rather than opening a new window.
Enable Window>New Window	Allows modules to be opened in multiple windows. Adds an additional **New Window** button to the toolbar.
Prevent force quit (Command-Q) on Mac OS X	Blocks the force quit command.
Allow deletion of items that normally may only be disabled	Enables a true delete option in some modules. Normally, important items should be disabled, not deleted. Even with this option enabled, only items that are not referenced by other items may be deleted. For example, if a device has an event occur for it, it may no longer be deleted, as the event references the device. This is because true deletion in this case would result in the inability to correctly report on any such events.

Table 17-14 Miscellaneous Setting fields

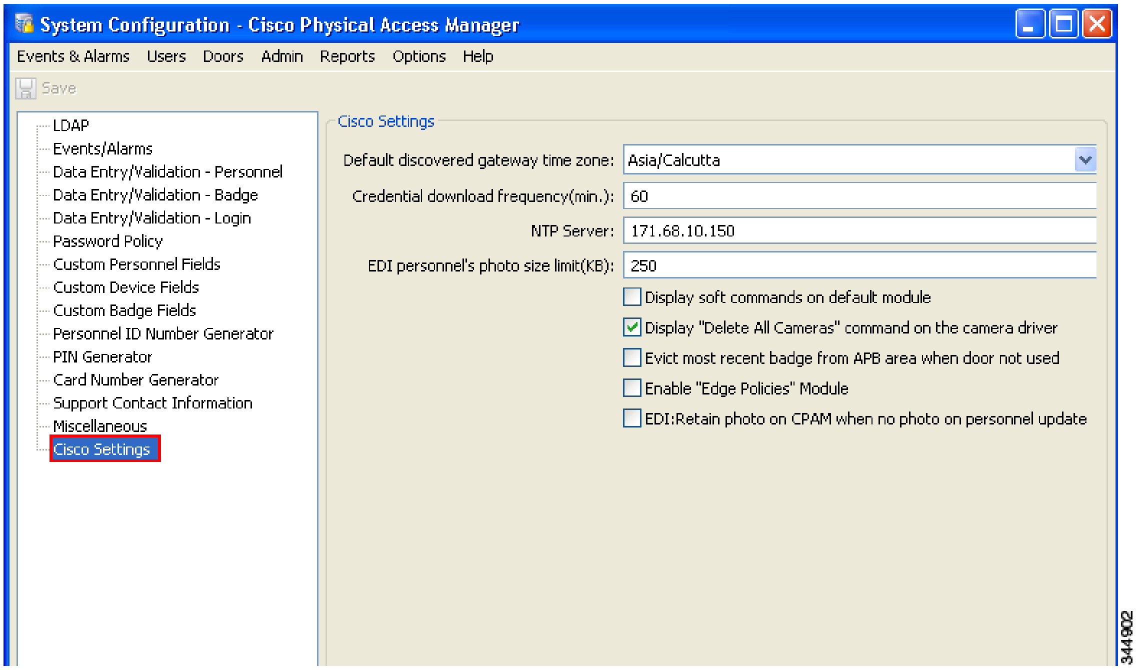
Field	Description
Allow deletion of devices with events	Deletes events associated with a device when a device is deleted. **Note** Cisco recommends that you do not delete devices. Events that are associated with the device will be deleted if the device is deleted.
Restrict new devices to wizards only	All new devices added to the **Hardware** module will use an add wizard.
Default max rows	Limits the number of visible rows in list-based modules such as Events and Badges. For example, if the default max rows is set to 100, the badges module displays a maximum of 100 rows. Enter a number between 1 and 5000.
Change queue buffer size	Enter a new buffer size.
Logged in workstations assume partition of login's profile	not supported in both 1.4.1, 1.5.0 and 1.5.1 versions.
Partition-restricted workstations only use explicitly assigned license items	not supported in both 1.4.1, 1.5.0 and 1.5.1 versions.

Note Changes to system configuration settings do not take effect until you log out and log back in to the Cisco PAM application (select **Logout** from the Options menu).

Cisco Settings

Figure 17-14 includes the settings described in Table 17-14.

Figure 17-14 Cisco Settings



Cisco Settings

Default discovered gateway time zone: Asia/Calcutta

Credential download frequency(min.): 60

NTP Server: 171.68.10.150

EDI personnel's photo size limit(KB): 250

☐ Display soft commands on default module

☑ Display "Delete All Cameras" command on the camera driver

☐ Evict most recent badge from APB area when door not used

☐ Enable "Edge Policies" Module

☐ EDI:Retain photo on CPAM when no photo on personnel update

Note To activate changes made to *Cisco settings*, you must either log out and log back in, or restart the Cisco PAM appliance, as described in the following table. To restart the appliance, see Using the Web Admin Menus, Commands and Options, page 3-17, or ask your system administrator for assistance.

Table 17-15 Cisco Settings

Field	Description	To Activate Changes
Default discovered gateway time zone	Defines the time zone for all discovered Gateways. This time zone is configured on all discovered Gateways.	Restart the Cisco PAM appliance.
Credential download frequency (mins)	Defines how often (in minutes) credential information is downloaded to the Gateways. **Note** You can also download credential changes immediately. Select **Hardware** from the **Doors** menu, right-click on the **Access GW Driver**, and select **Apply Credential Changes**. See Configuring Personnel, page 9-1 for more information.	Restart the Cisco PAM appliance.
NTP Server	Defines a default NTP server when updating multiple Gateways. See the "Changing the NTP Setting for Multiple Gateway Modules" section on page C-7.	Log out and log in.

Table 17-15 Cisco Settings

Field	Description	To Activate Changes
EDI personnel's photo size limit	Defines the maximum file size for imported photo files using the System Configuration module. For example, if you enter a maximum file size of 500 kb, then any files larger than 500 kb will be automatically compressed when the personnel record is imported. • Enter a value, in kb, between 50 and 750. • The default value is 250 kb. See the "Understanding Photo File Compression When Importing Personnel Records" section on page 14-17.	Log out and log in.
Display soft commands on default module	Displays the soft commands for the default m01 (Gateway) module.	Log out and log in.
Display "Delete All Cameras" command on the camera driver	Displays the **Delete All Cameras** command for the Cisco VSM Video Driver in the Hardware module. See Deleting the Cisco VSM Cameras, page 15-31.	Log out and log in.
Evict most recent badge from APB area when door not used	If a user presents their badge and is granted access to an Anti-Passback Area, but decides not to enter the door, then a *Door Not Used* event is generated by the door's Gateway module. To prevent the badge from being added to the Anti-Passback monitoring list, enable the System Configuration setting for **Evict most recent badge from APB area when door not used**. See the "Evicting a Badge from APB if the User Does Not Enter the APB Area" section on page 11-24	Restart the Cisco PAM appliance.
Enable "Edge Policies" Module	Enables the Edge Policies module. See the "Configuring Edge Policies" section on page 13-9.	Log out and log in.