CHAPTER 10

Multifactor Authentication

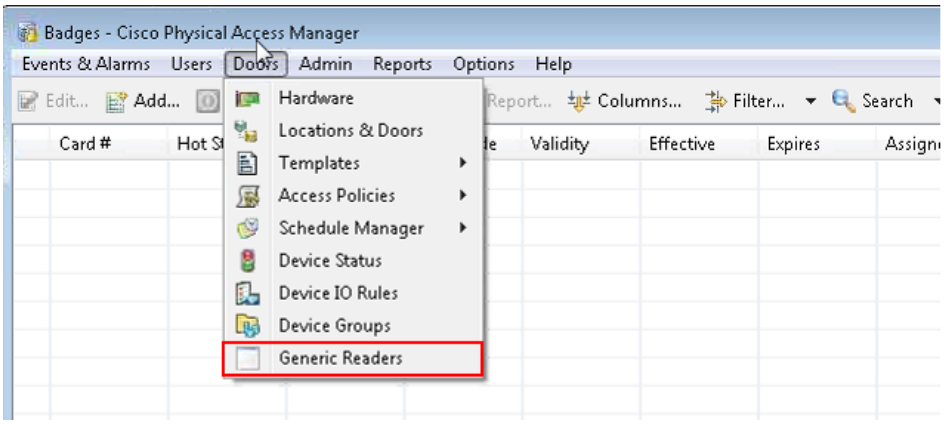
The user can integrate additional access control devices like biometric devices to the Cisco PAM to ensure security. These devices are configured as Generic Readers in the Cisco PAM server. The Generic readers are associated with doors and finally configured to a specific gateway. Once configured, the gateway maps the data from the Generic Reader and matches it with the server, If matched , the events are triggered accordingly.

The Generic Readers are restricted by location hierarchy when the hierarchical location is set in the Data Entry/Validation - Login, page 17-10

Contents

Configuring Generic Readers

	To do this
Step 1	From the Doors menu, click **Generic Readers**.



Step 2 The Generic Reader window opens. Click **Add**.

Enter the following fields:

- Name (alpha-numeric characters)
- ID (numeric)

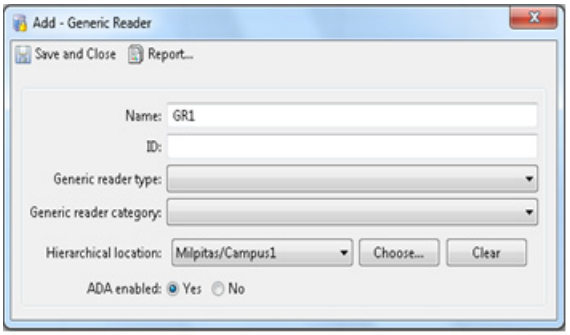
Select values in the following drop down lists:

- Generic reader type

Note This option should be used when using Microsoft Active Directory. Two types of generic readers are configurable. These are Face_detection (Used for facial recognition devices) and Biometric (for all other devices like fingerprint readers).

- Generic reader category
- Hierarchical location

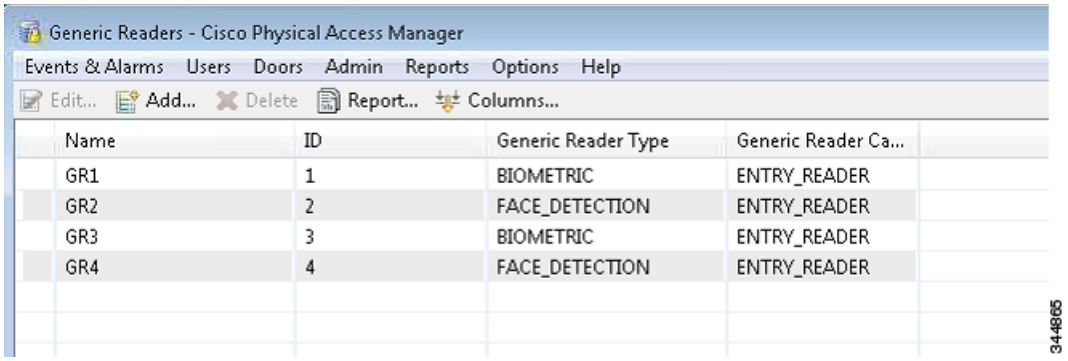
Select the ADA enabled radio button.



Tip Ensure that Name and ID are similar.

To do this

Step 3 Click **Save and Close**. The Reader information is listed in the Generic Reader window.

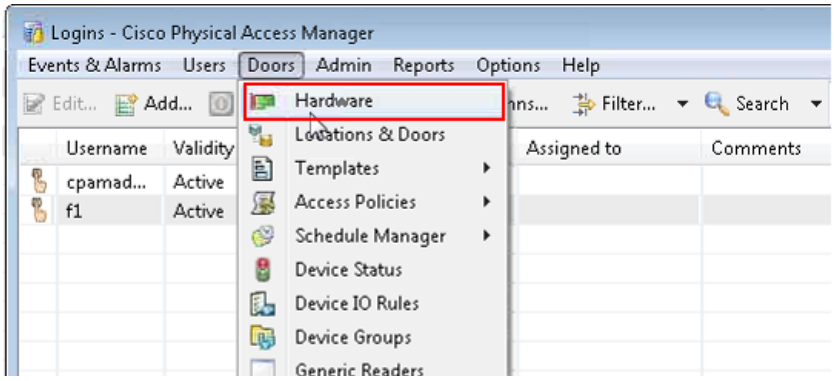


Note Only users with Admin rights are permitted to configure generic readers.

Associating Generic Reader with Doors

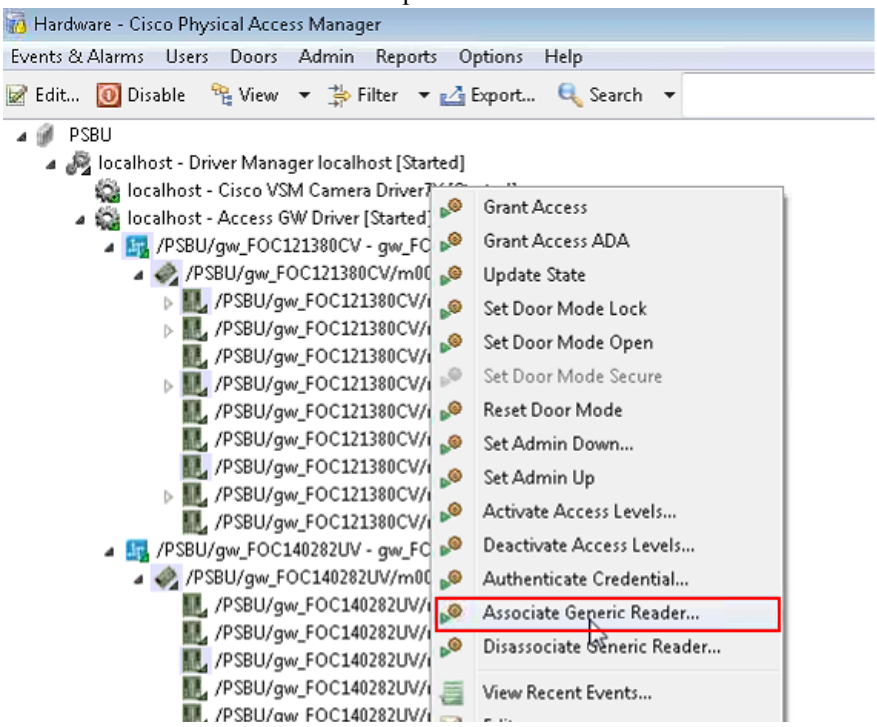
To do this

Step 1 From the Doors menu, select **Hardware**. The gateway drivers, gateways and doors are displayed.

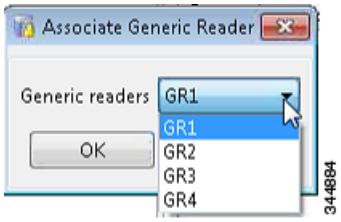


To do this	

Step 2 Select the door and right click to view the drop down menu.Click **Associate Generic Reader**. An Associate Generic reader window opens.



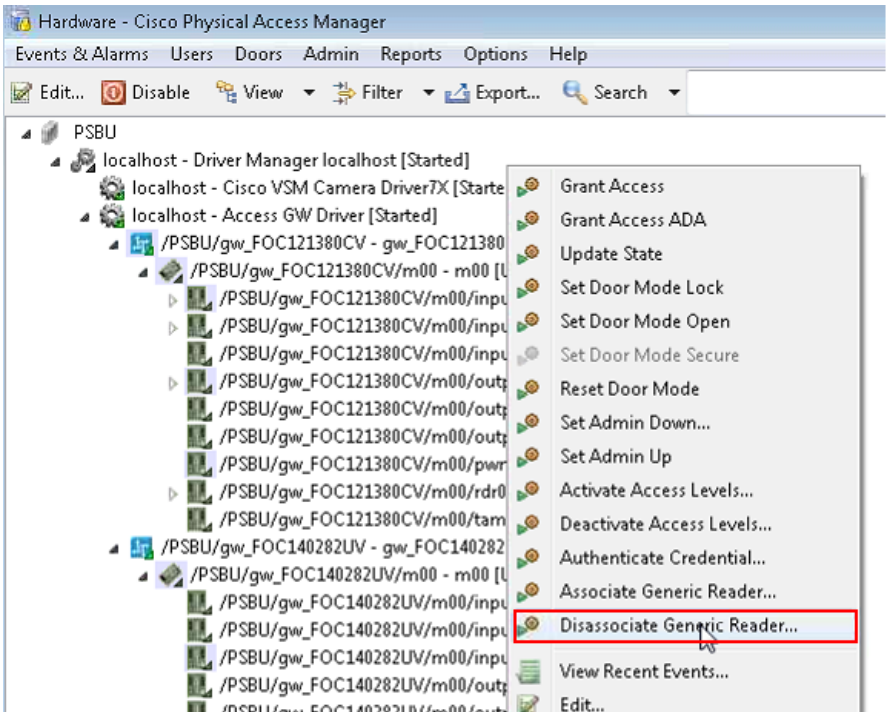
Step 3 Select the Generic Reader from the list and click **OK**.The Generic Reader is configured to the door.



Note You can associate a maximum of six Generic Readers to a door.

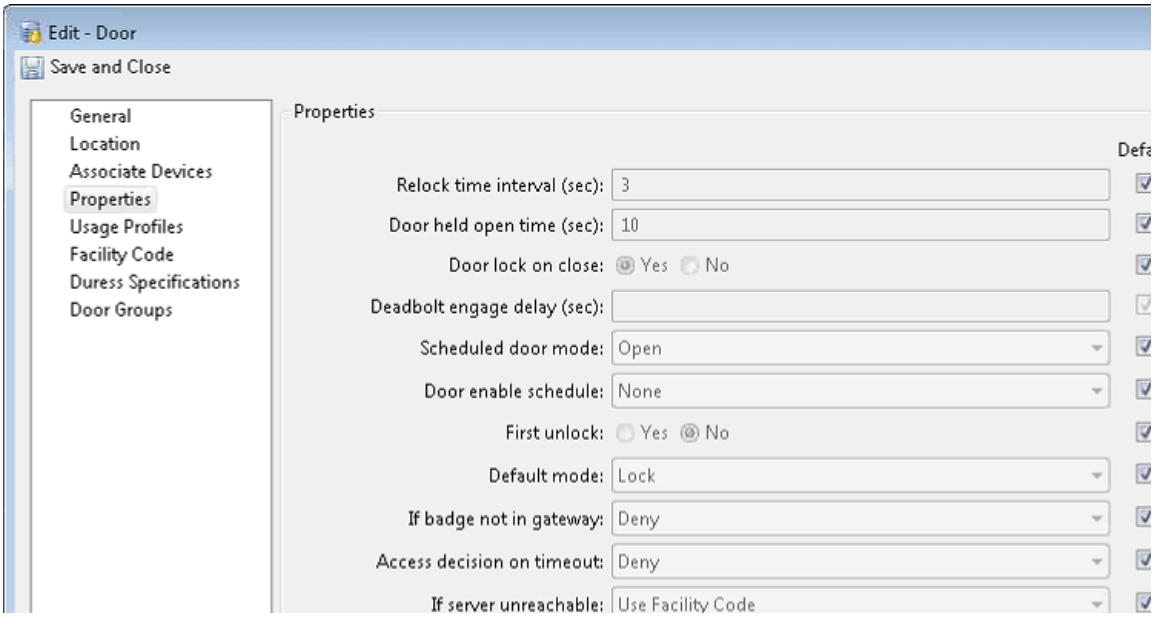
To do this

Step 4 Click **Dissociate Generic Reade**r to remove a reader from the door configuration.



Note The drop down menu displays the list of generic readers assigned to the door.

Step 5 Right click the door and select Edit. The Edit Door window opens. Select Properties to view the Generic Readers added to the door and the Multifactor Authentication timer (sec). You can edit the timer and set the time.



Note The default value of Multifactor Authentication timer (sec) is 10 seconds.

Note

- The generic readers configured by the cpamadmin is not restricted to any hierarchical location.
- When a location-restricted user creates a generic reader, the hierarchical location field is auto-populated.
- The location-restricted users can access only devices (generic readers) of their location and the events for these devices alone is populated for them.

Note These points are applicable only when the Profile enhancement feature is set in the System Configuration of the Cisco PAM. Otherwise the Cisco PAM appliance retains its behavior as in the previous version (1.3).

Additional Information

Multifactor authentication depends on the external system to authenticate biometric or facial data that the Cisco PAM receives from the generic reader. The Cisco PAM does not claim support to authenticate the received data. The gateway authenticates the data based on the badge swipe by the user and HTTPS MFA requests it receives from external devices configured as generic readers in Cisco PAM.

The External system must send the following HTTPS request for establishing a session with GW

For example:

```
POST /fcgi/user.login?login HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-application,
application/vnd.ms-xpsdocument, application/xaml+xml, application/x-ms-xbap,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR
2.0.50727)
Host: 10.78.179.95
Content-Length: 48
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-au
Cache-Control: no-cache

username=gwadmin&password=Cisco123&TRACKID=12345
```

The External system after authenticating the biometric data must send the following HTTPS request to GW

For example:

```
POST /fcgi/webmgr.ac?post_generic_rdr_event HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-ms-application,
application/vnd.ms-xpsdocument, application/xaml+xml, application/x-ms-xbap,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR
2.0.50727)
Host: 10.78.179.95
Content-Length: 59
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-au
Cache-Control: no-cache

hibadge=0&lobadge=34959&Generic_Reader_id=GR1&TRACKID=12345
```

where,

TRACKID — user defined cookie

hibadgeq—higher 32 bits of a badge (badge supports max of 64 bits)

lobadge—lower 32 bits of a badge

Generic_Reader_id—ID of the generic reader as configured under the Generic Reader Module.