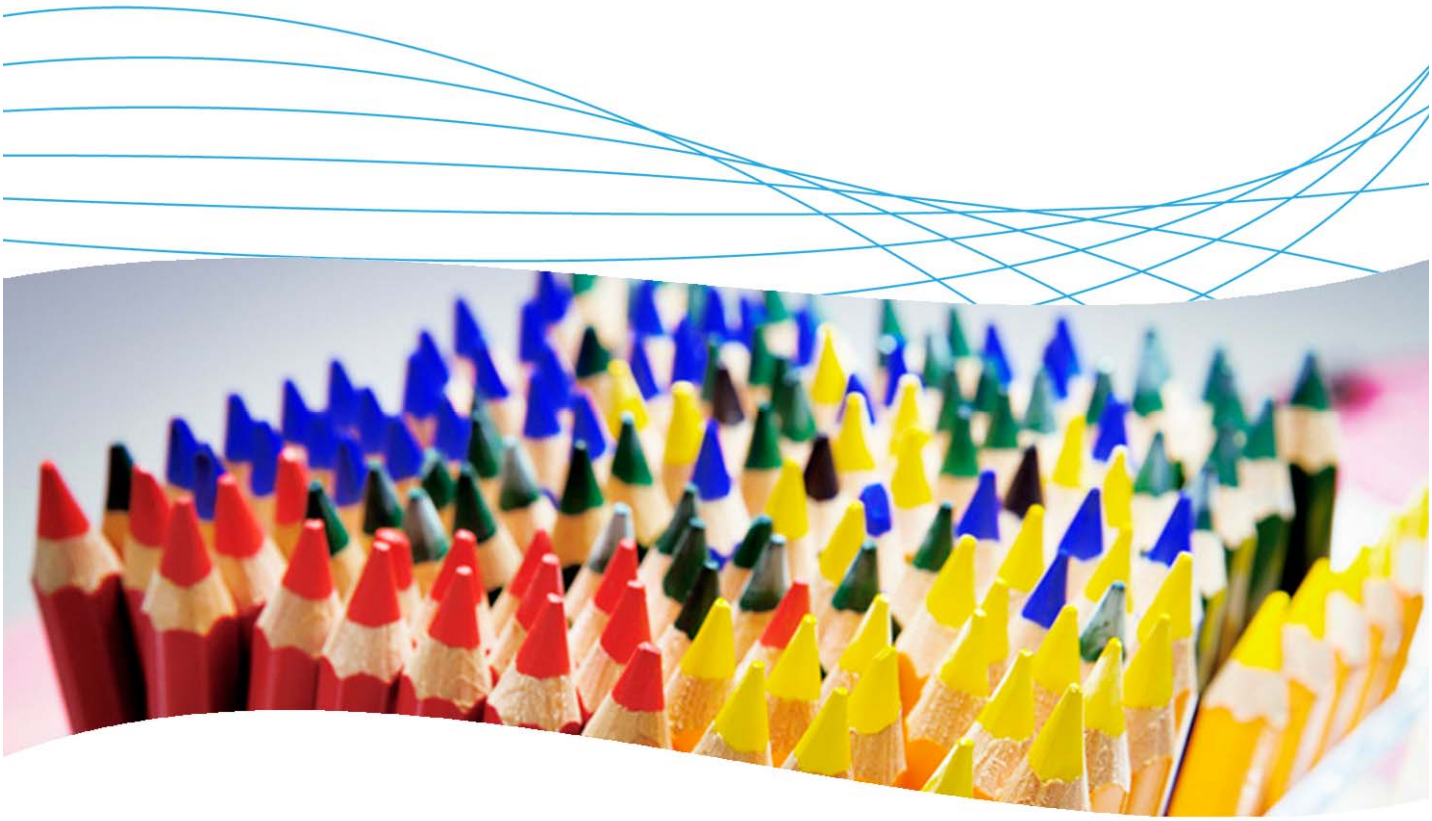
An HP ProCurve Networking Application Note

How to configure ProCurve Identity-Driven Manager (IDM)



Contents

1. Introduction

This document describes how to configure ProCurve Identity-Driven Management software and ProCurve network equipment to implement an identity-driven access control solution on an enterprise network.

2. Network diagram

Figure 1 shows the network referenced in this application note.

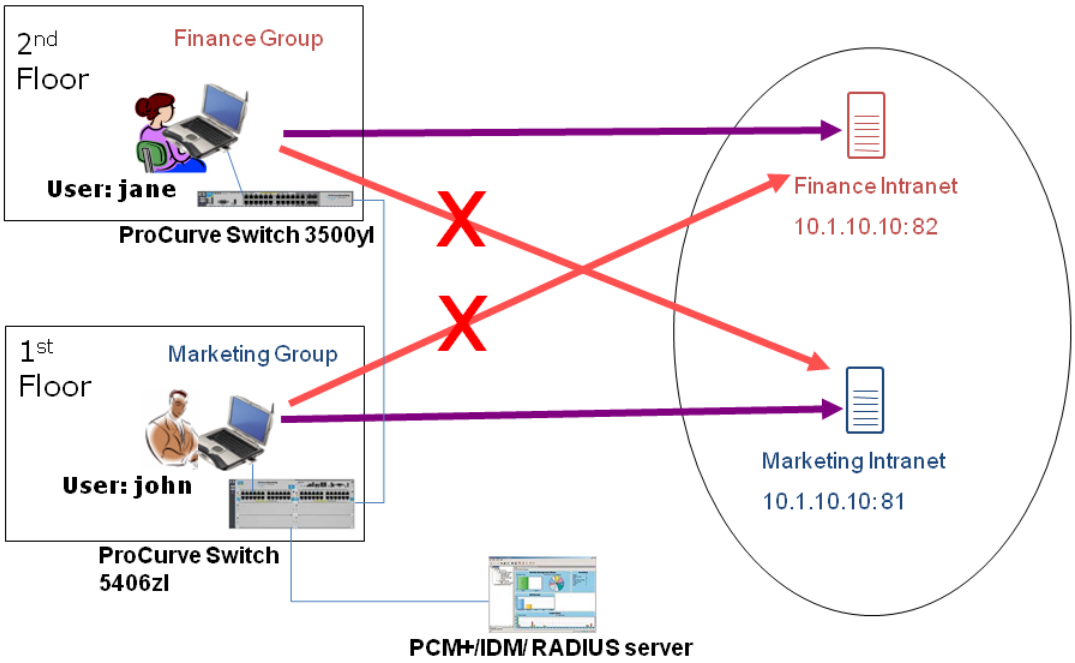


Figure 1. Each group has its own intranet. Users from one group cannot connect to the other group's intranet.

3. Configuring network equipment

To be able to use Identity Driven Manager to control user access on the switches or access points on your network through, there are two prerequisites:

- These devices must have been discovered by ProCurve Manager Plus; otherwise they will not be proposed as possible locations by IDM.
- All VLANs that will be configured in IDM Access Profiles to be applied on a network equipment must be defined on this network equipment, and appropriately tagged on the uplinks. An IP helper address to the corporate DHCP server must be configured on each VLAN.

3.1 Configure the Finance group switch

The ProCurve Switch 3500 will be configured for access control, and only the users in the Finance group will be authorized to connect from that switch. The Finance VLAN (VLAN 30) must be defined on the switch:

```
3500yl(config)# vlan 30
3500yl(config-vlan 30)# ip address 10.1.30.2 255.255.255.0
3500yl(config-vlan 30)# tagged 1
3500yl(config-vlan 30)# ip helper-address 10.1.10.10
3500yl(config-vlan 30)# exit
```

Once the switch has been discovered, VLANs can also be defined directly from ProCurve Manager Plus.

3.2 Configure the RADIUS server and the authentication method

The next steps of the switch and access point configuration are:

- Configure the RADIUS server and shared secret.
- Define the authentication method on each port that will be enabled for user authentication.

You can perform these two steps either from the CLI or from IDM's secure wizard.

3.2.1 Configuration from the CLI:

```
3500yl (config)# radius-server host 10.1.10.10 key procurve
3500yl(config)# aaa authentication port-access eap-radius
3500yl(config)# Aaa port-access <web | mac | authenticator> Ethernet_port
```

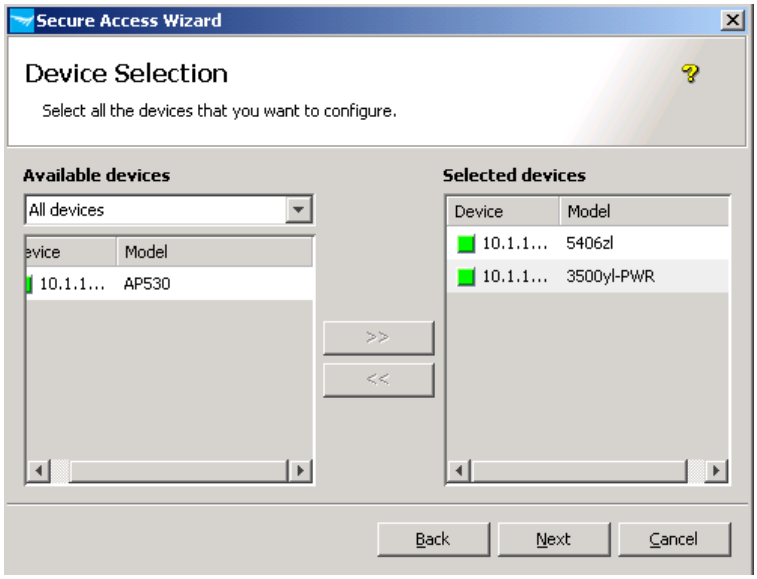
For more details regarding the different authentication methods, please refer to the following application notes:

- AN-S1, *How to configure Web authentication on a ProCurve switch*
- AN-S2, *How to configure MAC authentication on a ProCurve switch*
- AN-S3, *How to configure 802.1X authentication with a Windows XP or Vista supplicant*

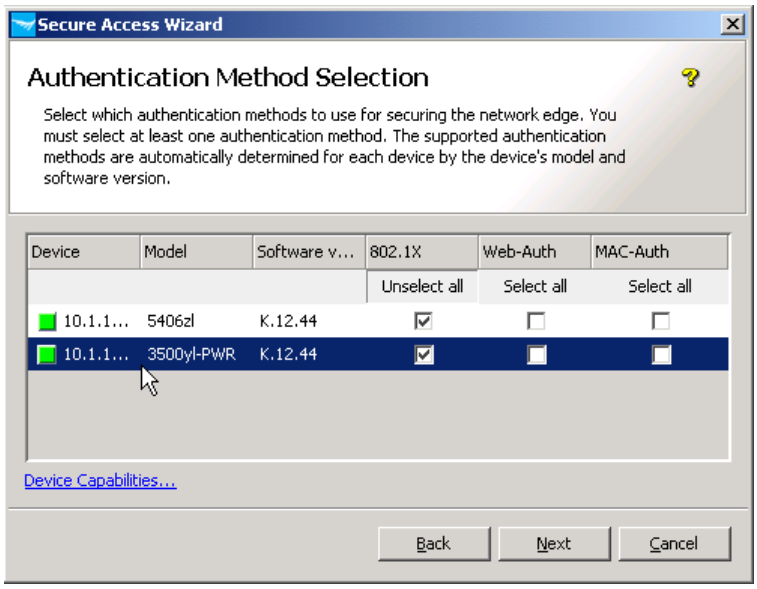
3.2.2 Configuration from the Secure Wizard:

1. From the ProCurve Manager Tools menu, launch the Secure Wizard.
2. At the Device Selection window, select the network equipment on which you want to enable access control.

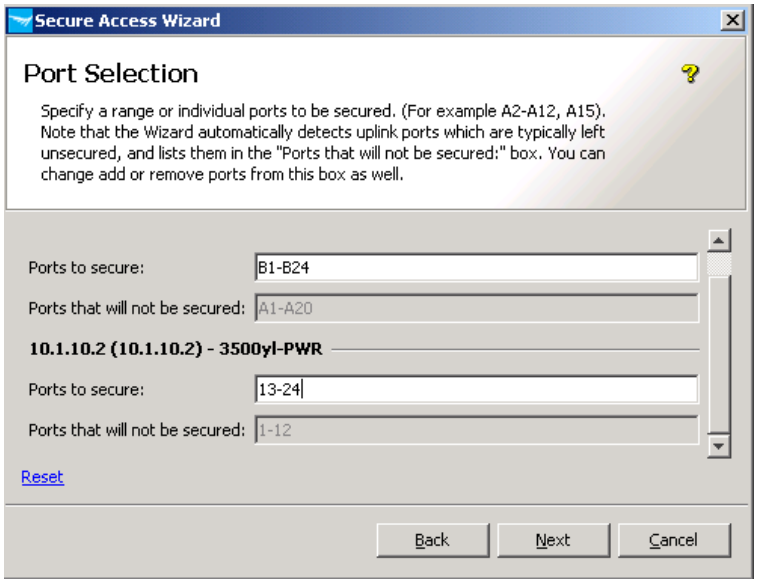
   For example, here the 5406zl and the 3500yl are selected. Note that you can add wireless devices as well.



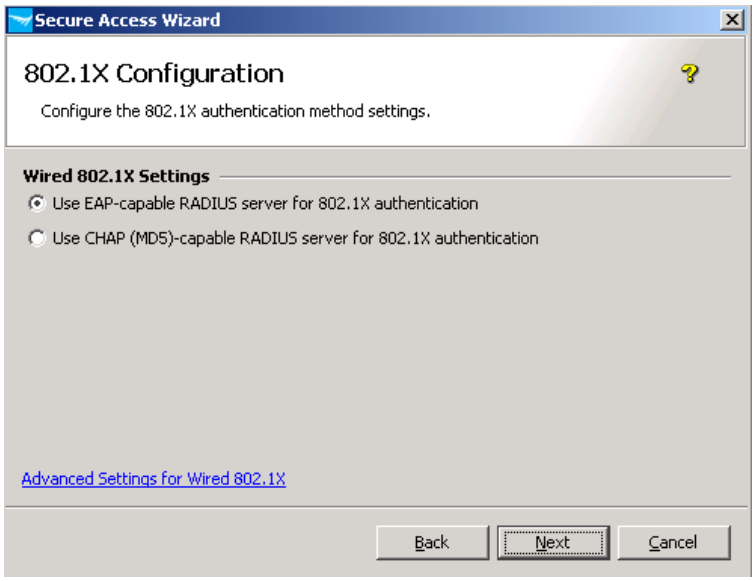
3. At the next screen select the authentication method. For example, here 802.1X is selected for both switches:



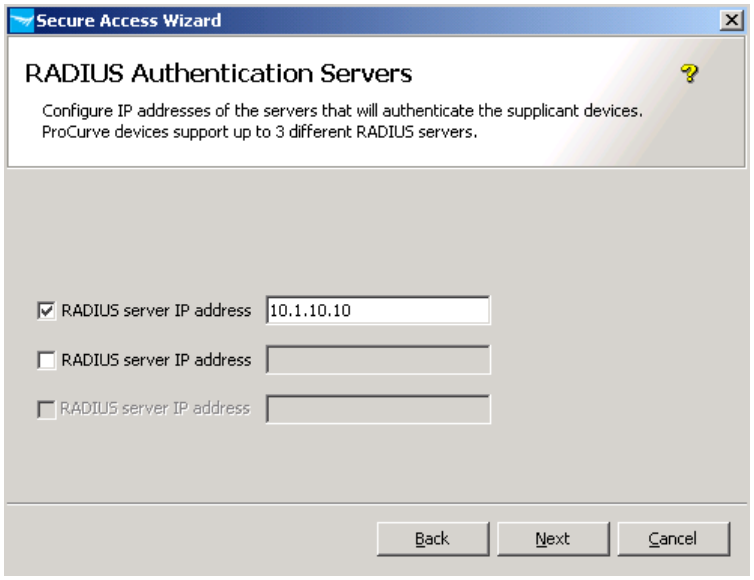
4. Then select the ports to secure: for example, B1-B24 on the 5400 switch and 13-24 on the 3500:



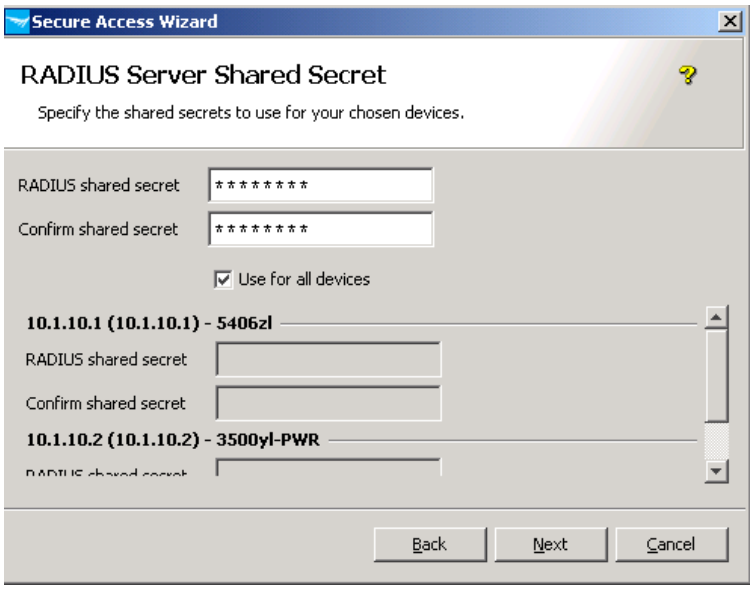
5. At the 802.1X Configuration screen, choose EAP-capable RADIUS:



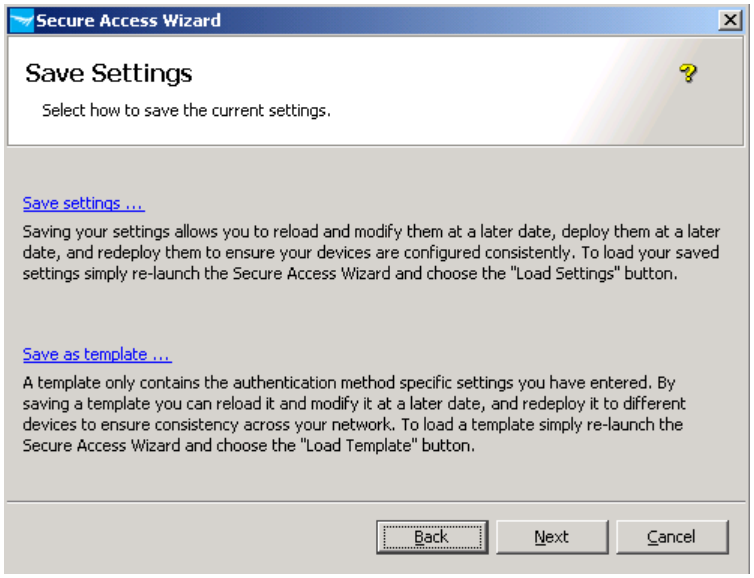
6. At the RADIUS Authentication Servers screen, enter the address of the RADIUS server, here 10.1.10.10:



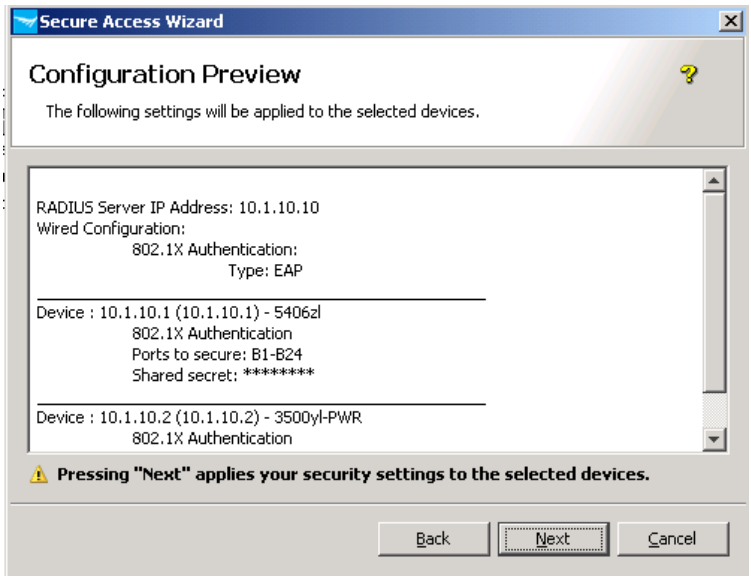
7. Then enter the shared secret for each network equipment. You can use the same secret for all devices. For example:



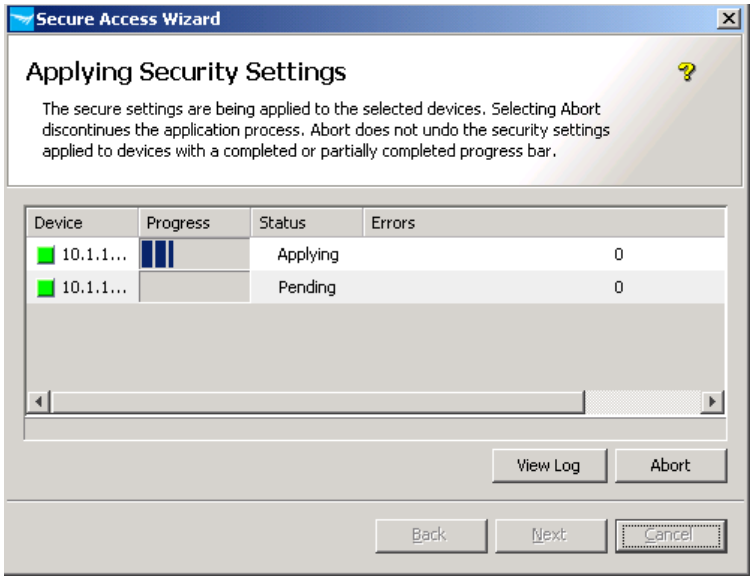
8. Save the settings.



9. Check the configuration, then click Next:



10. Deploy the configuration:



4. Configuring Identity-Driven Manager

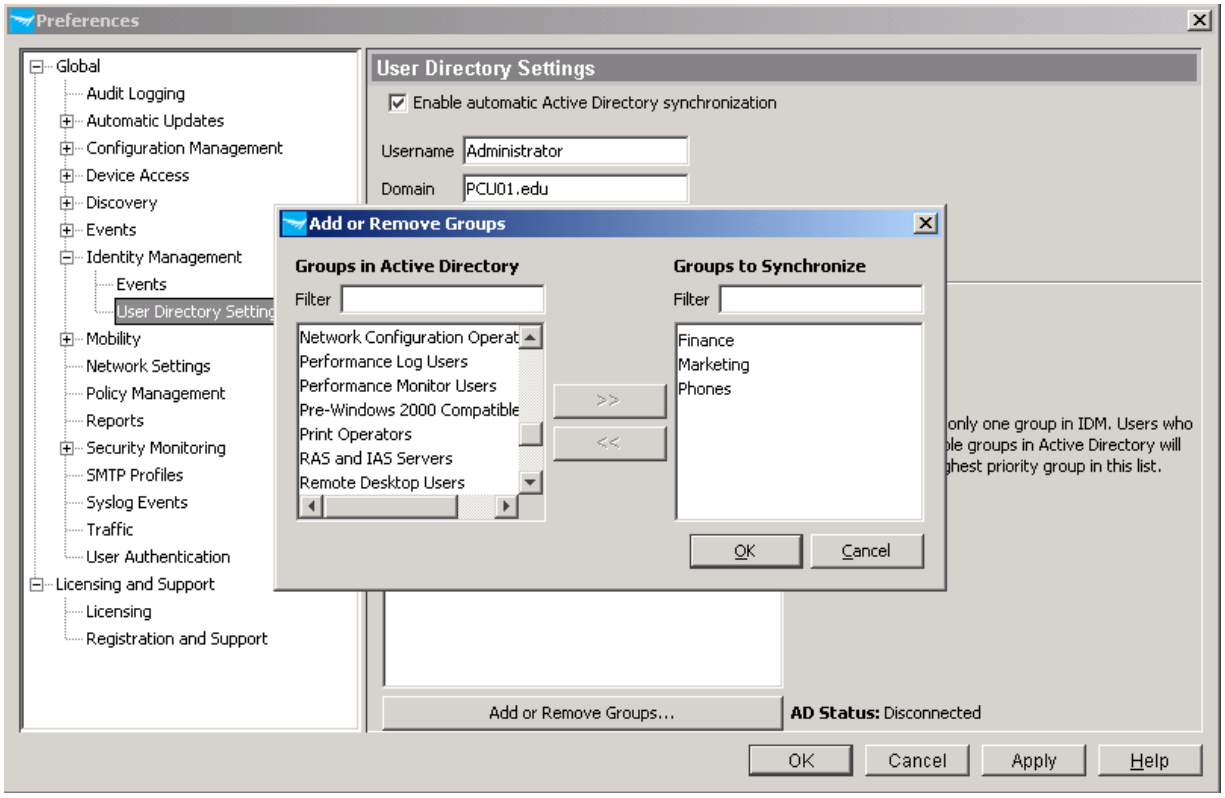
This section explains how to configure IDM.

4.1 Synchronize with Active Directory

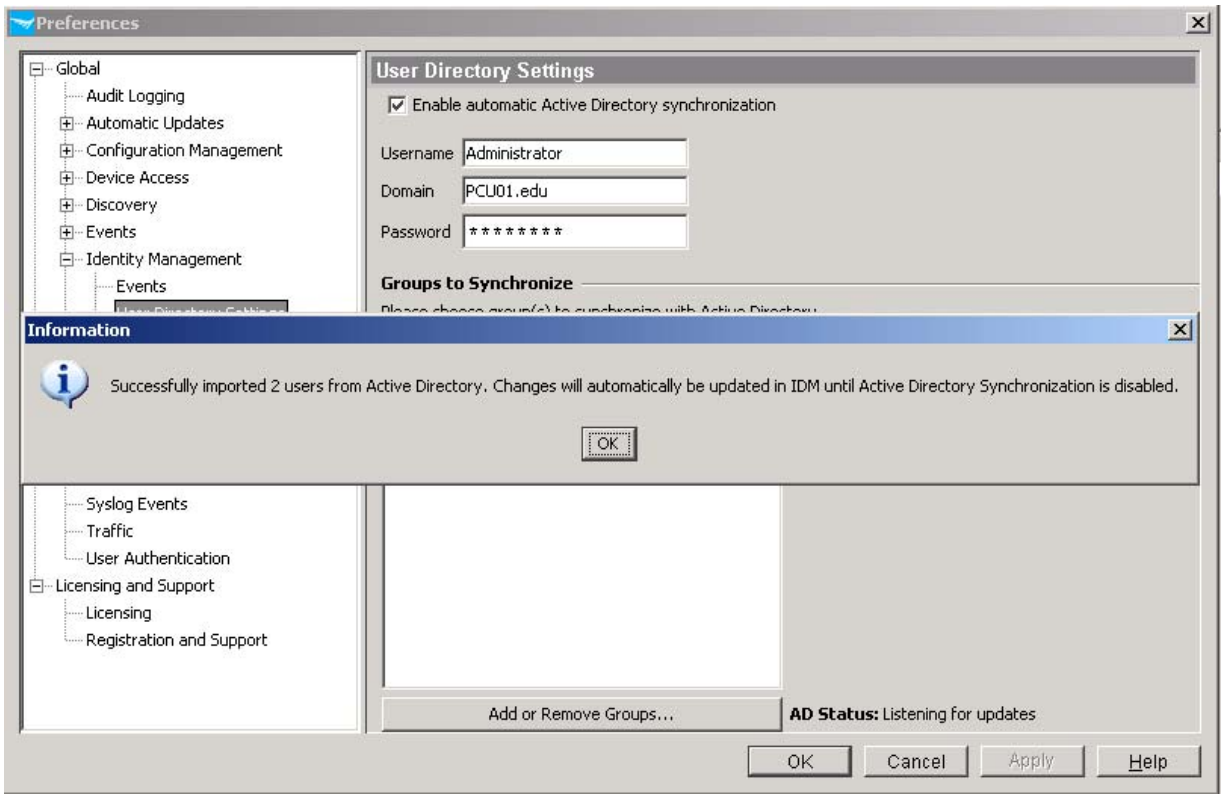
First, you must synchronize IDM with Active Directory groups. To synchronize:

1. In ProCurve Manager, click on the Identity tab in the lower part of the window to go to the IDM home window.
2. In IDM, open the menu Tools > Preferences, expand the line Identity Management, and open User Directory Settings.
3. In the User Directory Settings window, click to put a check mark in the Enable automatic Active Directory synchronization box.

4. Enter the administrative credentials of the domain. For example:
    - Username: Administrator
    - Domain: PCU01.edu
    - Password: password
5. Then in the Groups to Synchronize field, click on Add Groups and choose the groups you want to synchronize with IDM. Then click OK.



6. The AD Status at the bottom right of the window moves from Disconnected to Listening for updates, and an Information message appears, indicating the users have been successfully imported from Active Directory:



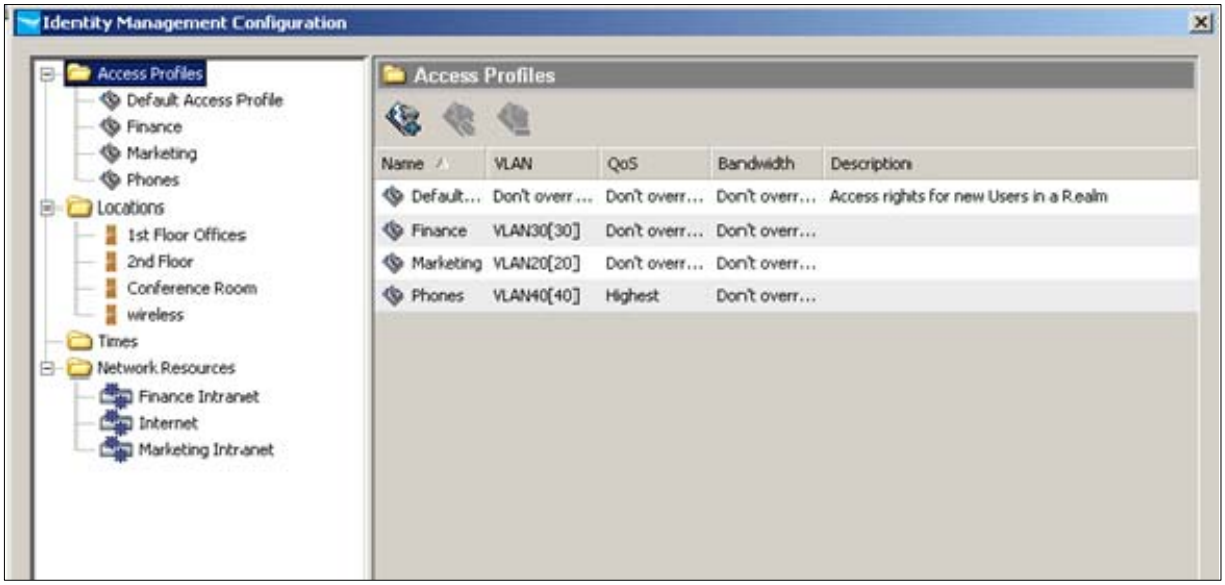
7. Click OK to clear the Information message, and OK again to save the Groups to Synchronize. In the Identity window, in the list of Access Policy Groups in the left-hand pane you see the three new groups synchronized in the list.

   Click on one of the groups. In the Users tab you see the users that belong to this group. If you create new users in these groups in Active Directory, they immediately appear in IDM in the correct Access Policy Group:

4.2 Configure identity management

To configure identity management:

- In IDM, go to the Realm Properties panel and click on the far left icon  to open the Identity Management Configuration window. In the Identity Management Configuration navigation tree on the left you see lists of Access Profiles, Locations, Times, and Network Resources:



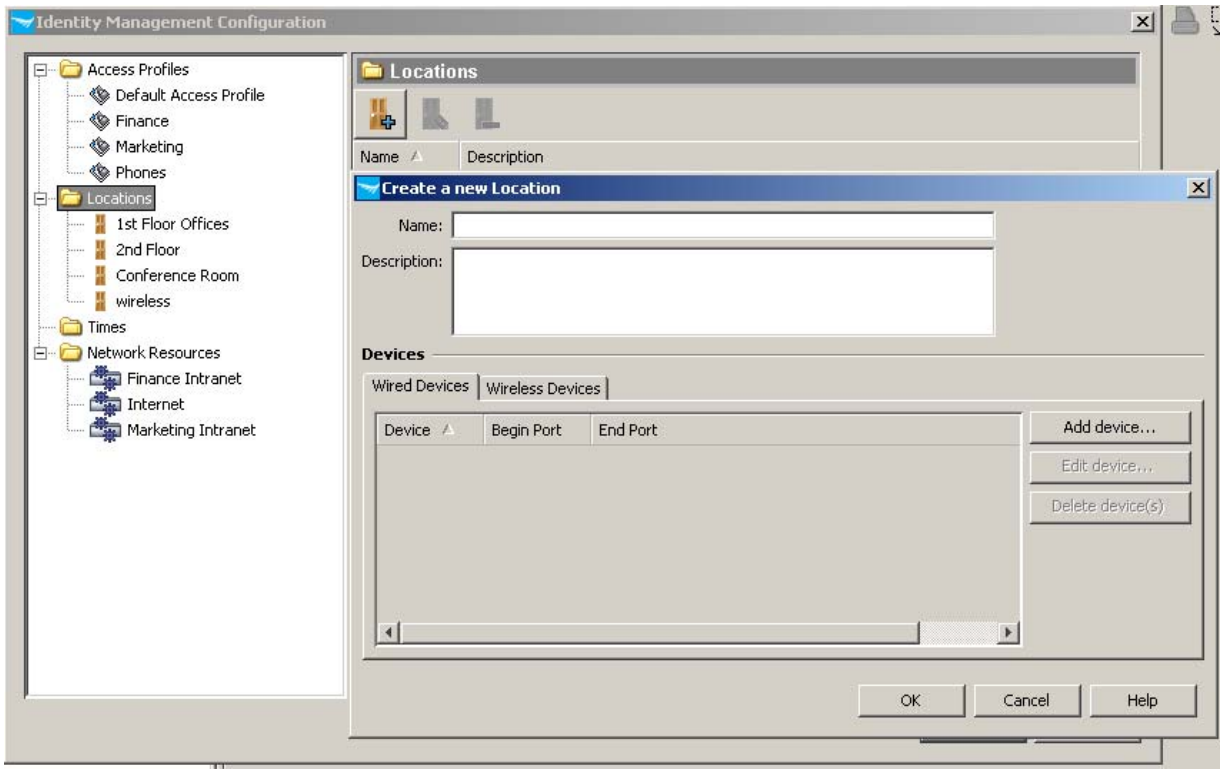
4.2.1 Configure locations:

Locations correspond to the physical places where the access rights will be verified and the access profiles enforced; that is, the locations of:

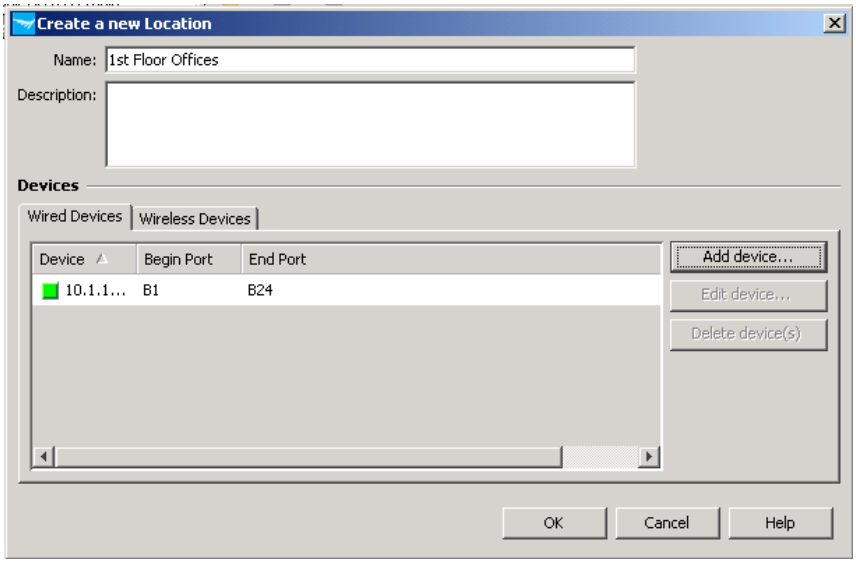
- Switch ports
- Radios on wireless equipment

To configure locations:

1. In the navigation tree on the left, click on Locations, then click the New Location icon  in the Location toolbar to add a new Location:



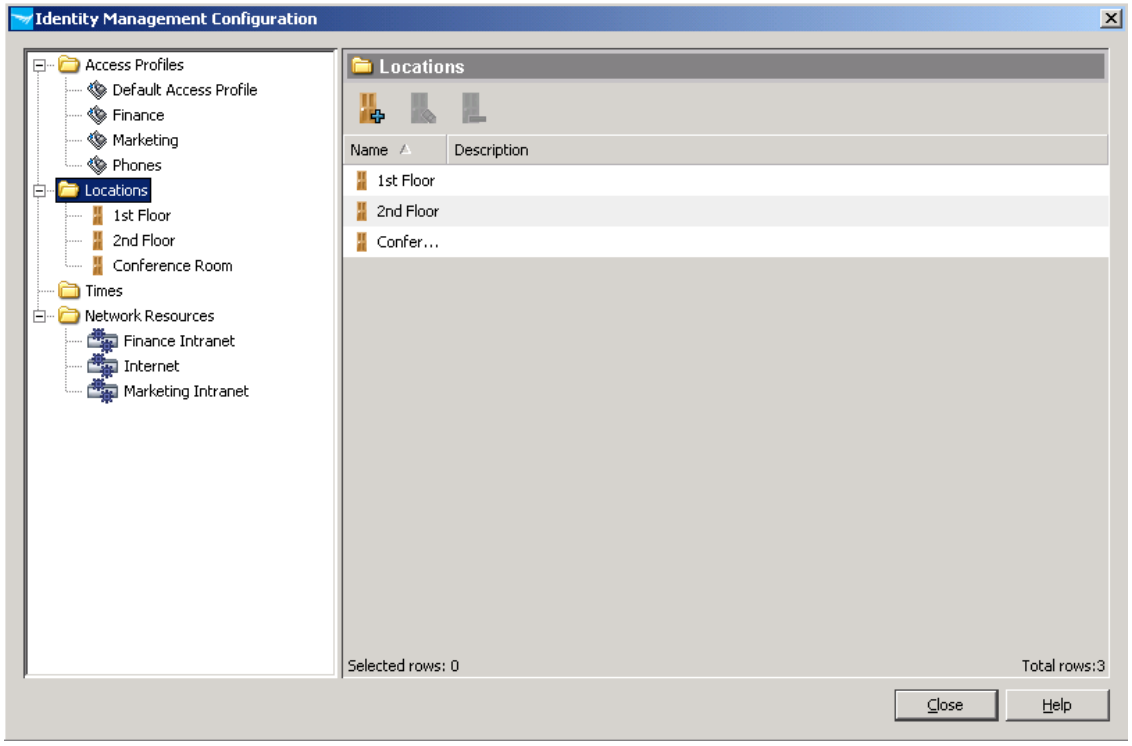
2. To add a new device, fill out the Create a new Location window as follows:
   - Name of the location
   - Description, if desired



3. The Create a new Location window has two tabs for Devices: one for Wired Devices and one for Wireless Devices. Click the appropriate tab and click Add Device. You see windows that let you choose the model of the equipment you want to add (for example 5406zl), and also choose the ports on the equipment. You can add more than one device to a location.

   For this example, you would add three locations: 1st Floor Offices, 2nd Floor Offices, and Conference Room.

4. When you return to the Identity Management Configuration window you can see the list of all Locations. For example:

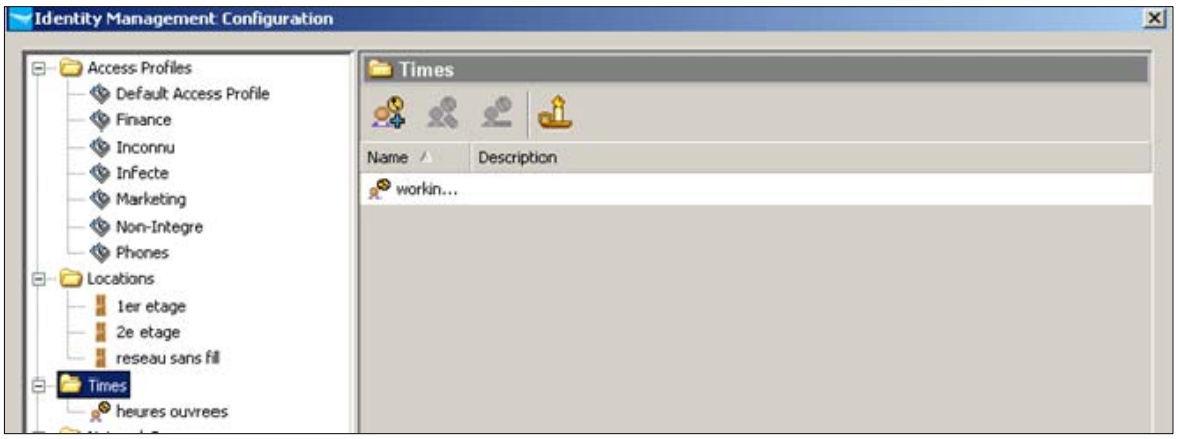


Remember, each location can include multiple devices.

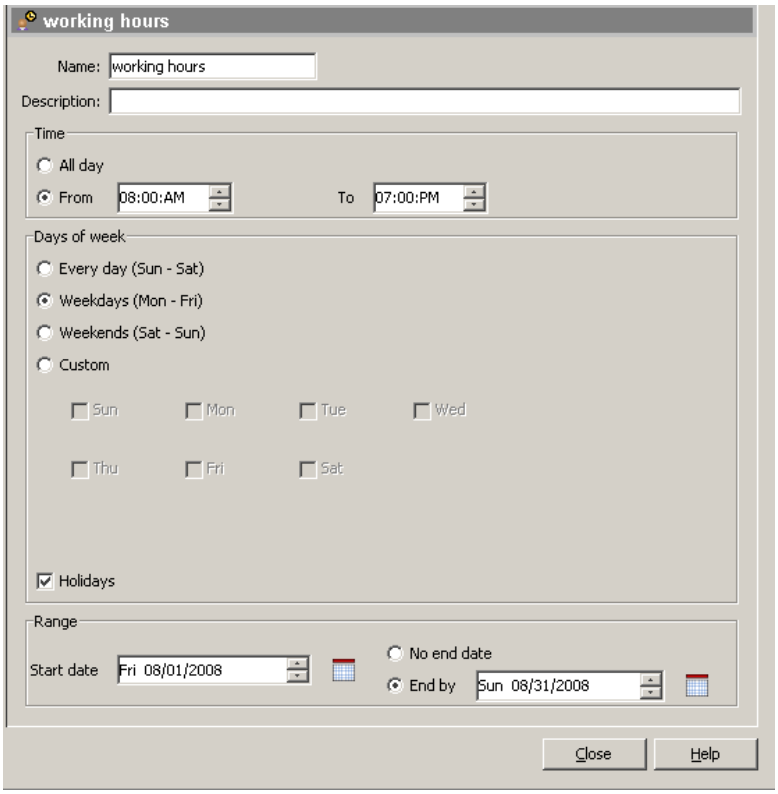
4.2.2 Configure access times:

You can define different time periods, to restrict access to different categories of users outside non-working hours or days. To create a new time period:

1. In the Identity Management Configuration navigation tree on the left, click the Times node. You see a list of Times:



2. In the Times panel toolbar, click the left-most icon to add a new Time. You see window for adding a new Time:



3. Fill out the new time window as follows:
    - Enter a name and description for the new time period.
    - Then define the time (From-To) and days of the week you want to include.
    - You can also exclude a range of days (defined as Holidays) between two dates.

    In the example above, working hours is defined as weekdays (Monday to Friday) between 8:00 am and 7:00 pm. A holiday range from August 1st to August 31st is also defined.

4.2.3 Configure network resources:

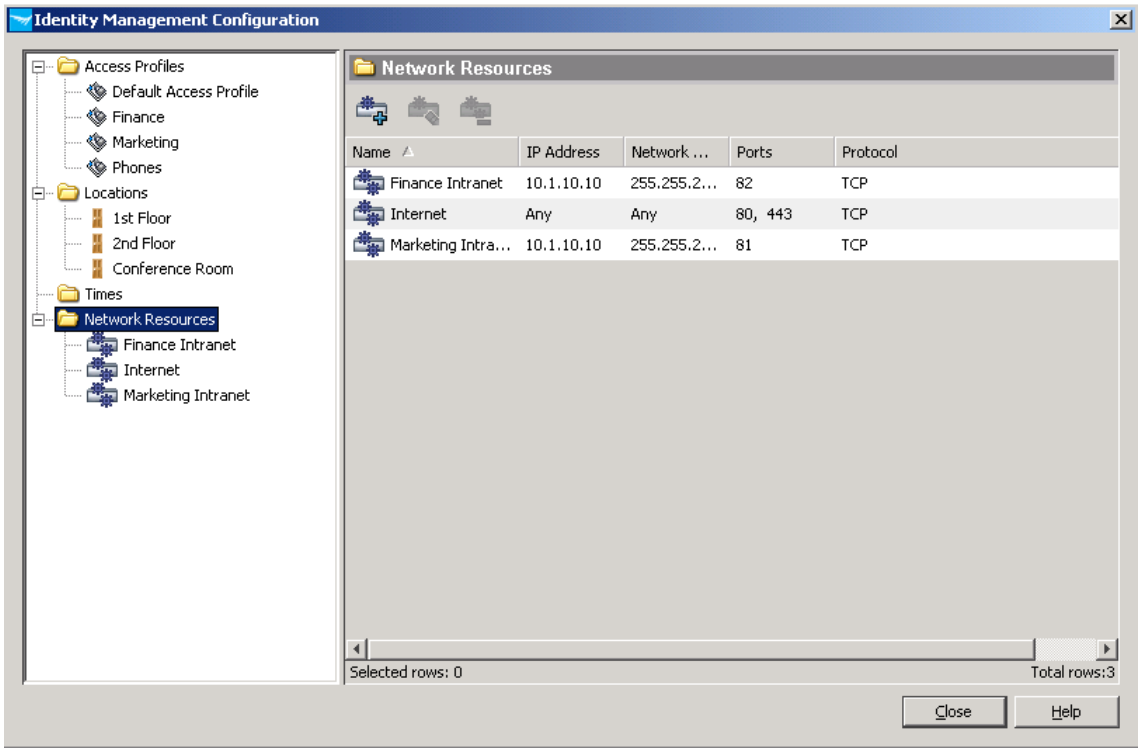
The definition of per-user access-lists is done in two steps:

- First you create the different Network Resources
- Then you allocate the rights to these different resources for each Access profile.

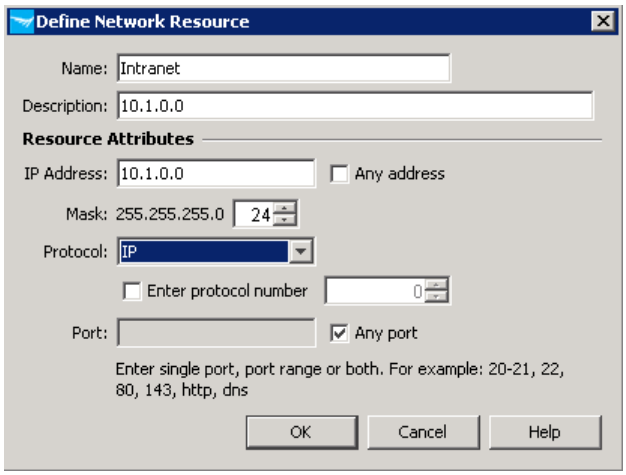
A Network Resource can be a subnet, a client machine, a protocol, even a TCP or UDP port on a subnet or machine. The definition is quite flexible.

To create a new Network Resource:

1. In the Identity Management Configuration navigation tree on the left, click on the Network Resources node at the bottom of the Identity Management tab. You see the Network Resources panel.

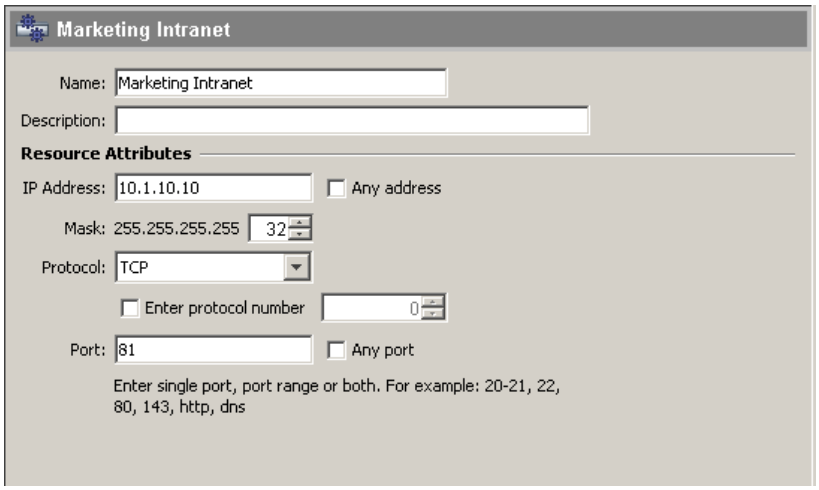


2. On the Network Resources panel toolbar, click on the first icon on the left to define a network resource. You see a Define Network Resource window:



3. Fill out the Define Network Resource window. For example, to define an intranet network:
   - Enter the Name (Intranet) and a Description (10.1.0.0) for the network.
   - Then in the Resource Attributes enter the IP address (for example 10.1.0.0), the network mask (24), the protocol (IP for full access to the network; or else choose among ICMP, IGMP, routing protocols, etc.).
   - Leave the Port set to Any port.

4. Define other network resources. For example, the following shows the Web server Marketing intranet, defined as TCP port 81 on server 10.1.10.10:



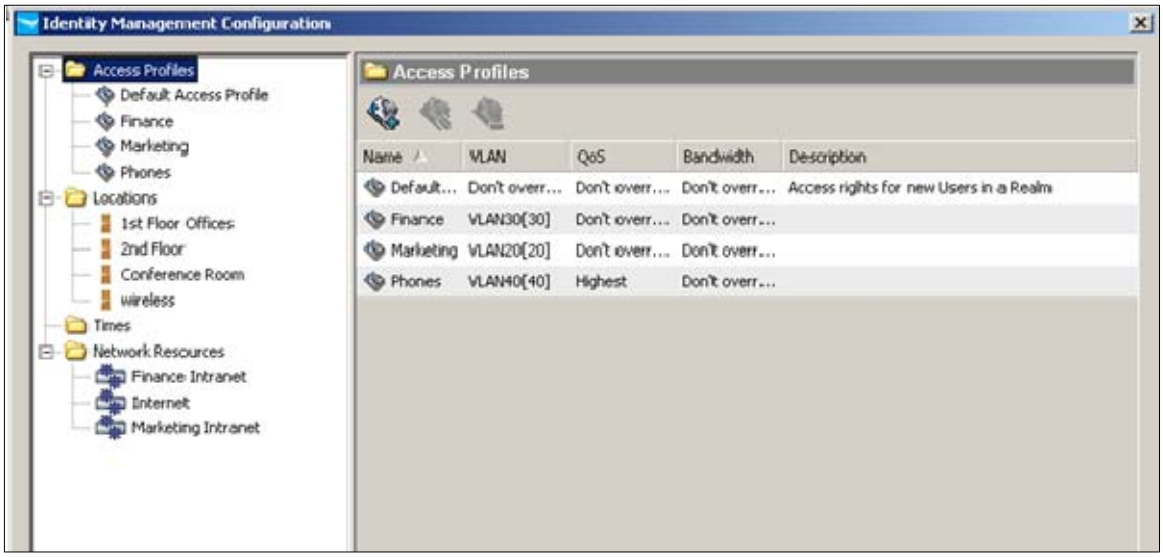
4.2.4 Configure access profiles:

Each Access Profile defines the settings that will be assigned to a group of users after successful authentication. An Access Profile is a combination of:

- A VLAN
- A QoS parameter, whose values can be between lowest and highest priority
- A bandwidth, which can vary between 1 Mbps and the physical bandwidth of the port to which the user will connect (e.g., 100 Mbps, 1000 Mbps)
- Network access rules

To configure an Access Profile:

1. Click the Access Profiles node in the Identity Management Configuration navigation tree to display the Access Profiles window. You see a list of defined Access Profiles. For example:



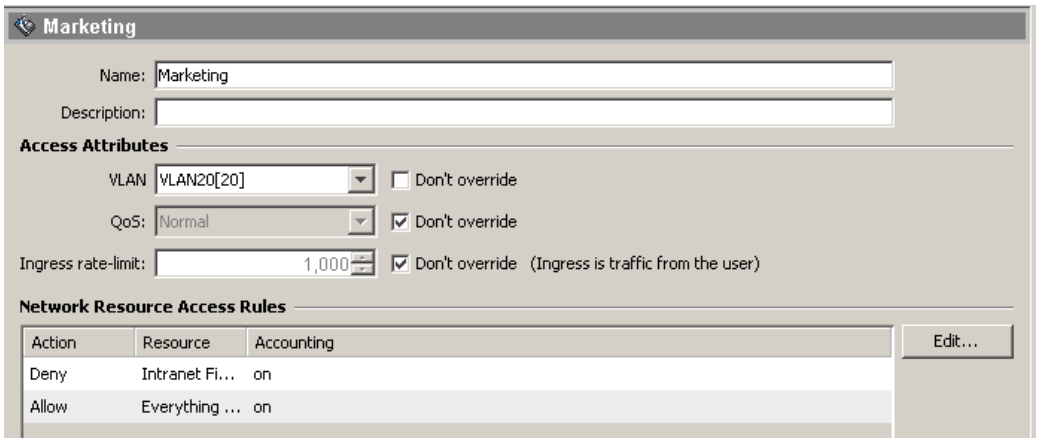
   In the Access Profiles shown in this example, Finance is configured to use VLAN 30, and Marketing is configured with VLAN 20.

2. Click the Add Access Profile icon in the toolbar to display the Create a new Access Profile window.
3. Define the attributes for the Access Profile: VLAN, QoS, bandwidth, etc.
4. To assign the Network Resources, click Edit to launch the Network Resource Assignment Wizard.

5. Follow the instructions in the wizard to choose among different Network Resources, including which resources will be allowed or denied, and in which priority order.

For example, the Access Profile for Marketing is defined as follows:

- Access Attributes:
  - VLAN 20
  - QoS not specified
  - Bandwidth not specified
- Network Resources Access rules:
  - Deny access to Finance intranet
  - Allow access to everything else



4.3 Access policy groups

Access policy groups correspond to the groups imported from the Active Directory. Rules are applied to these groups as a combination of the previously defined settings:

- Location
- Time,
- System (optional)
- WLAN (optional)
- Endpoint integrity state (optional)
- Access profile

When a user assigned to the access policy group is authenticated on the RADIUS Server, the IDM Agent applies the appropriate rule, which can cause the switch or access point to accept or reject the user. The IDM Agent modifies the RADIUS reply to provide the appropriate network access to the user.

For example, users from the Marketing access policy group are allowed to connect either from the first floor offices or the conference room, at any time, and from any PC. The WLAN is not taken into account:

When the user is authenticated, IDM checks the access policies in the order listed.

Similarly, users from the Finance access policy group connecting from the same physical ports will be authenticated using the access policy profile Finance, with the appropriate VLAN and network resources.

5. User experience

When connecting to the network on a particular port, the user is challenged for authentication according to the authentication method configured on that port: MAC, Web or 802.1X authentication.

After entering credentials, the user is allocated the profile corresponding to the Access Policy Group and the Access Policy Rule matched by the user's parameters for location, time and system. The user obtains an address in a particular VLAN, and access rights to different resources on the network.

Example: User John from the Marketing department connects to one of the ports on the 5406zl switch defined as the Conference Room location. He is allocated the Marketing access profile, and receives an IP address in VLAN 20, the Marketing VLAN: for example, 10.1.20.100. When trying to connect to the network, he has access to the Marketing intranet with URL http://10.1.10.10:81, but not to the Finance intranet with URL http://10.1.10.10:82.

User John disconnects and user Jane from the Finance department connects to the same switch port. She is allocated the Finance access profile and receives an IP address in VLAN 30: for example, 10.1.30.100. She is authorized to access the Finance intranet but not the Marketing intranet.

6. Troubleshooting

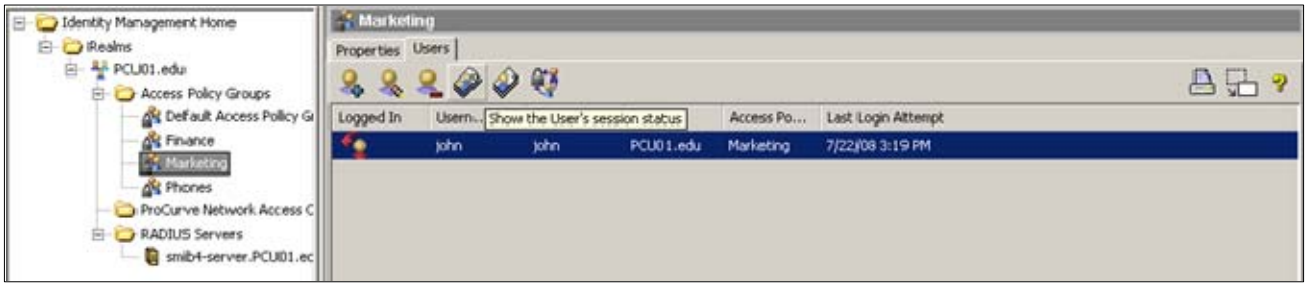
This section provides some tips and tools for troubleshooting IDM configuration.

6.1 Verify user status

The Users tab of each Access Policy Group lists all users of this group. Authenticated users appear in green and inactive users in red.

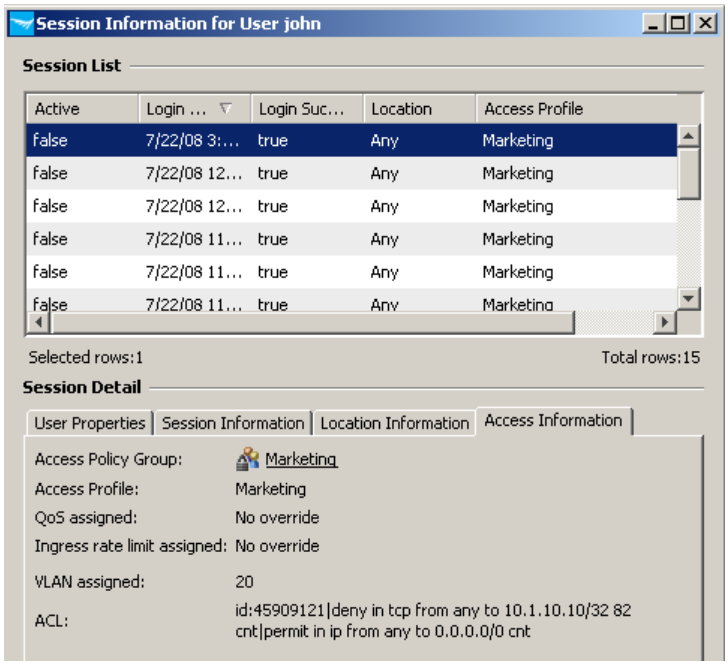
To verify the status of a user session and check that the user received the correct access profile:

1. Highlight the user and in the Users tab toolbar click the 4th icon from the left: Show the User's session status.



You see the Session Information window for the user.

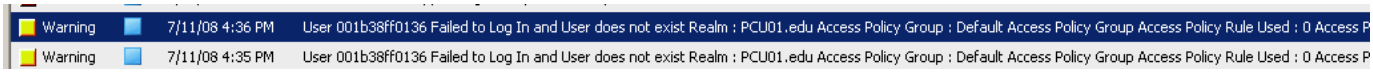
2. In the Session Information window examine the session details in the different tabs. The Access Information tab shows the details of the assigned access profile:



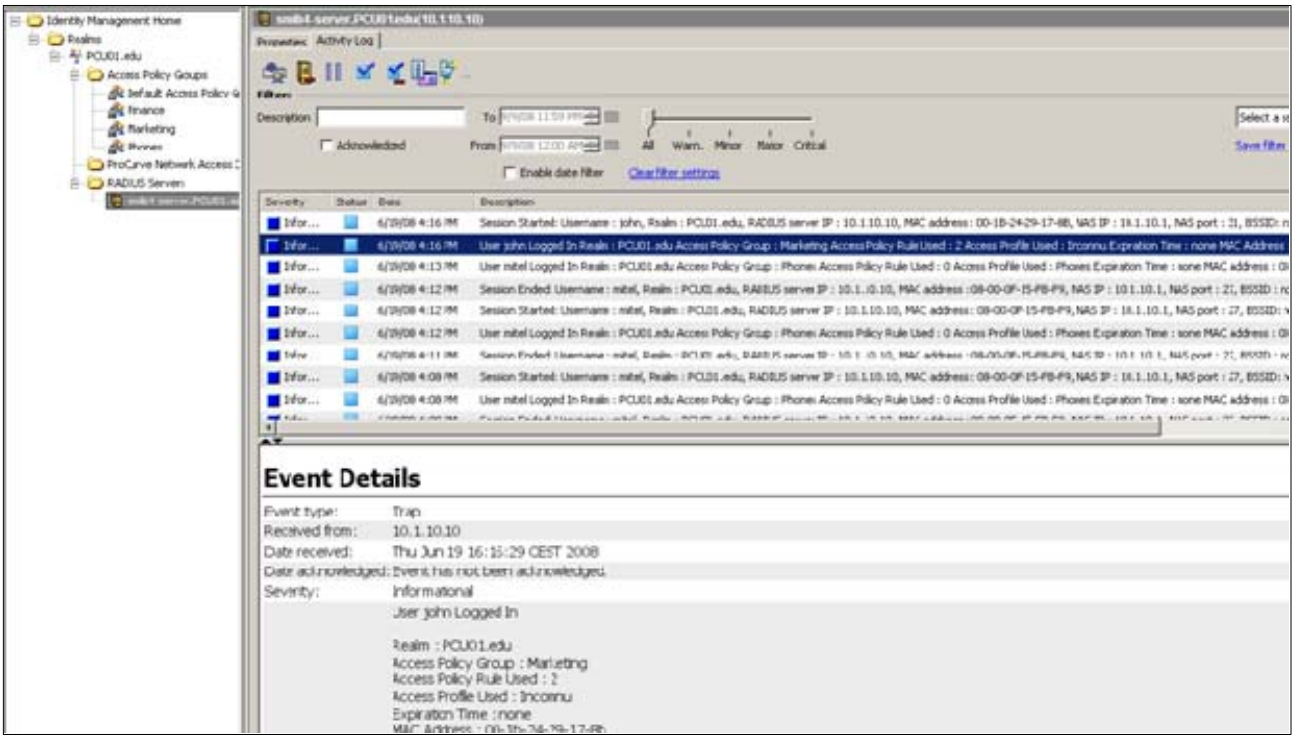
6.2 Check the IDM RADIUS log

The RADIUS log in IDM displays all authentication attempts accepted or rejected by IAS or IDM, and the details of the user session. For example:

Failed MAC authentication: The message User 001b38ff0136 failed to Log in and User does not exist means this event corresponds to an authentication attempt on a MAC authenticator port by a user with a MAC address that has not been registered in the Active Directory:



Successful authentication: The message User john logged in... indicates a successful authentication:

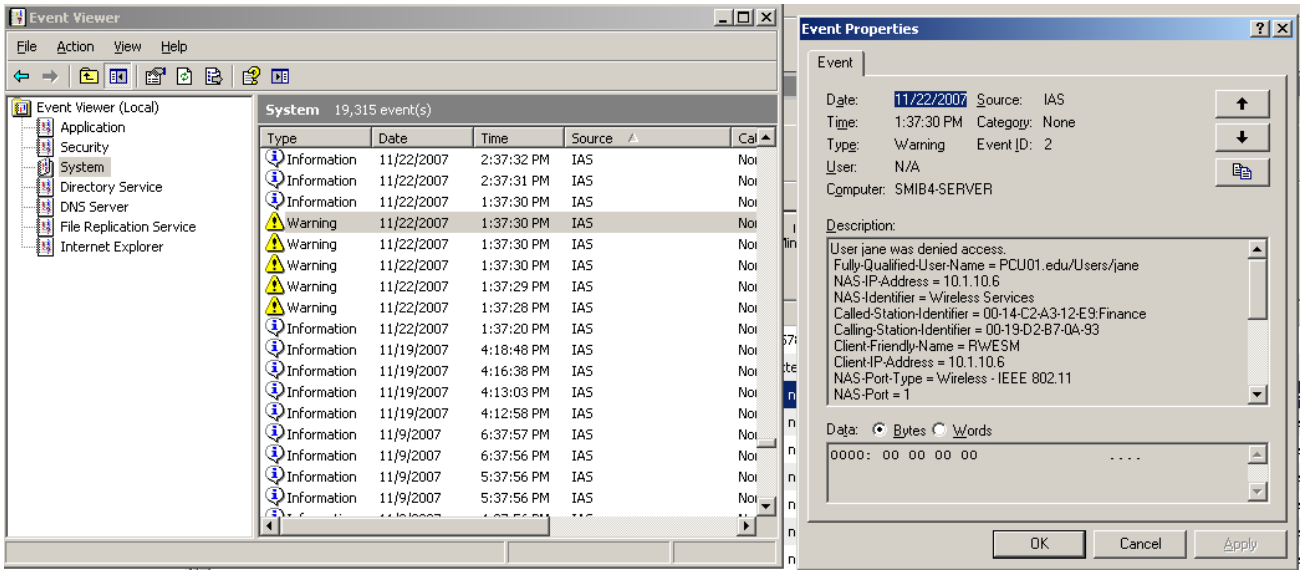


6.3 Use the IAS Event Viewer

When a user tries to authenticate and receives no response, and when no event for this user appears in IDM, another useful tool is the RADIUS log—the Microsoft IAS Event Viewer in the example used in this application note.

To use the Event Viewer:

1. In the Windows server, go to the Start menu, select Run, and enter eventvwr. You see the Event Viewer window:



2. In Event Viewer, check the IAS log entries in the System tab. A Warning indicates a failed authentication attempt.

3. Open the Warning message to view the details. Some hints:
    - Failed RADIUS authentication attempts are usually due to wrong passwords or authentication attempts by an unknown user.
    - The message This request was rejected by a third-party extension dll file indicates that the user was authenticated by IAS but rejected by IDM, usually because the user attempted to connect from an unauthorized location or at an unauthorized time.

7. Firmware versions

Switch firmware versions used for this application note are as follows:

- K.13.09 for ProCurve switches (5400zl, 3500yl). Free updates are available from the ProCurve web site: http://www.hp.com/rnd/software/switches.htm

- PCM+/IDM version 2.3 or later, also available from the ProCurve web site: http://www.hp.com/rnd/software/network_management.htm

8. Reference documents

This concludes the procedure for configuring IDM on ProCurve switches.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches: http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm

- For PCM+ and IDM manuals: http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm

  http://www.hp.com/rnd/support/manuals/IDM.htm

For further information, please visit www.procurve.eu

4AA2-2180EEE, July 2008