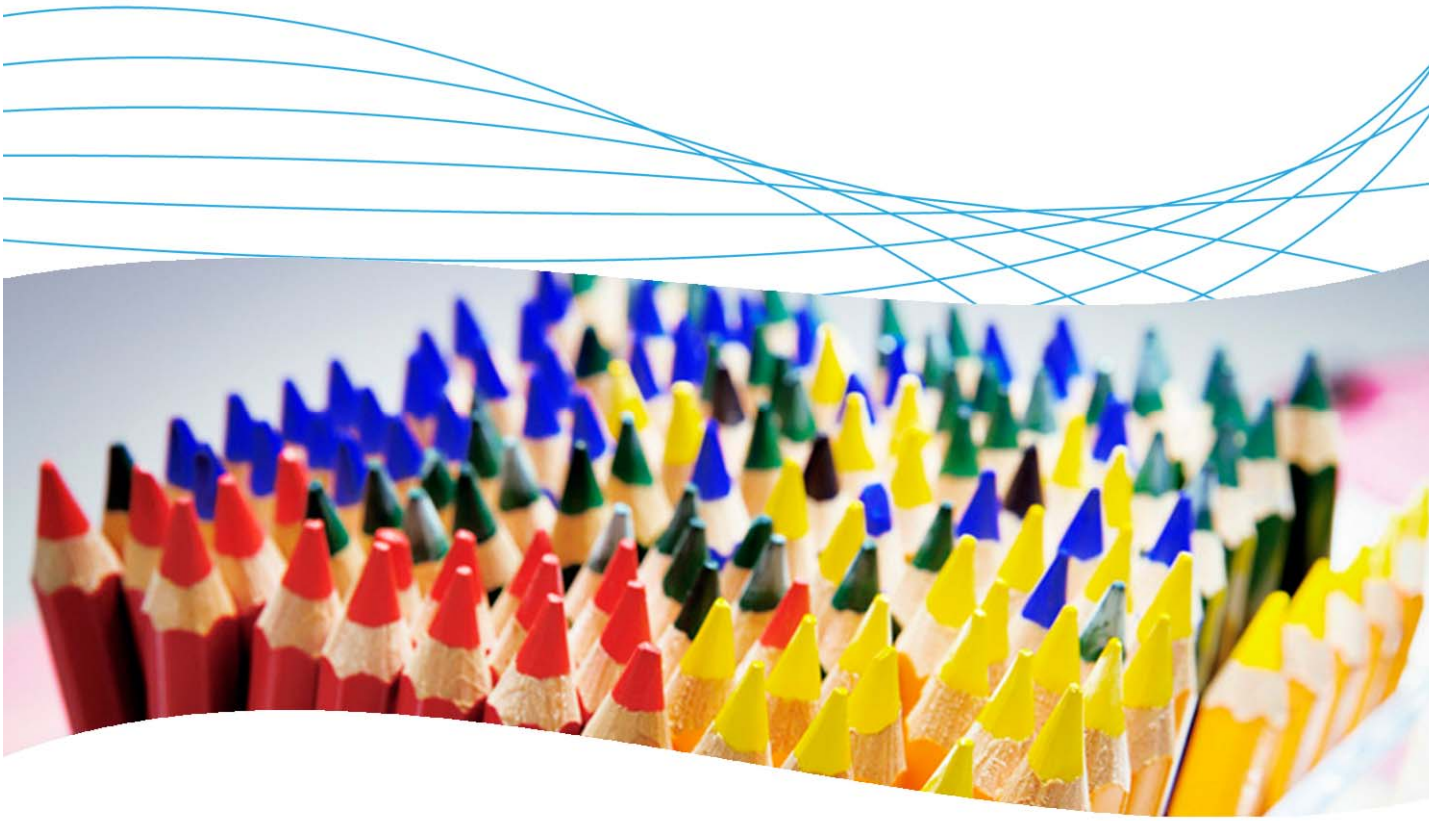
An HP ProCurve Networking Application Note

Synchronizing ProCurve IDM and Windows Active Directory



Contents

1. Introduction

This document describes how to integrate and synchronize ProCurve Identity Driven Manager (IDM) with Windows Server 2003 Active Directory. The switch used in this example is a ProCurve Switch 5400zl but most ProCurve switches can be configured in the same manner.

2. Prerequisites

This procedure assumes you have an already configured PCM/IDM server connected to a ProCurve Switch 5400zl, and an already configured RADIUS server (Microsoft IAS, on Windows Server 2003), along with the necessary users and groups created.

3. Network and Active Directory tree diagrams

Figure 1 details the hardware configuration referenced in this section.

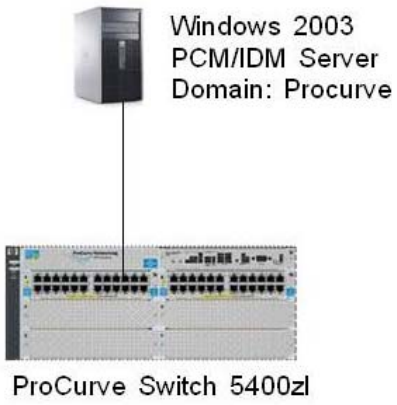


Figure 1. Setup for integrating PCM/IDM and Windows Active Directory

Figure 2 shows the Windows Active Directory tree referenced in this application note.

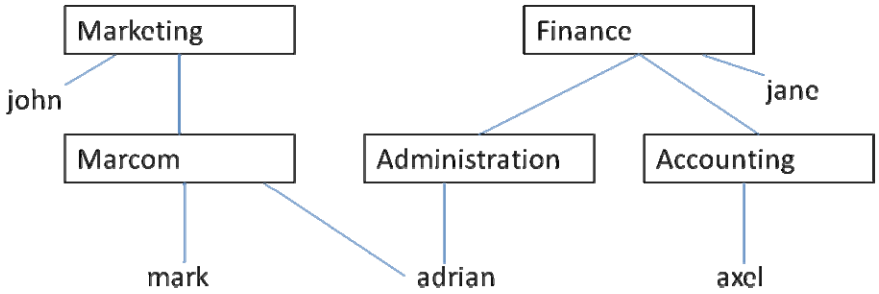


Figure 2. Windows Active Directory tree

4. Synchronization and nested group capabilities in IDM 2.3

Release 2.3 of ProCurve Identity Driven Manager now offers support for nested groups in Active Directory synchronization. This new feature is explained on page 2-40 of the *ProCurve Identity Driven Manager User's Guide* for Software Release 2.3, available from ProCurve at:

http://cdn.procurve.com/training/Manuals/IDM_UG-59908851-0508.pdf

When synchronizing Active Directory and IDM, the key factors to keep in mind are:

- Synchronization includes all users who are indirect members of a group via intervening nested group relationships.
- Users belonging to more than one AD group are added to the IDM group with the highest priority.
- If an AD group is deleted while synchronized, the corresponding Access Policy Group disappears from IDM.

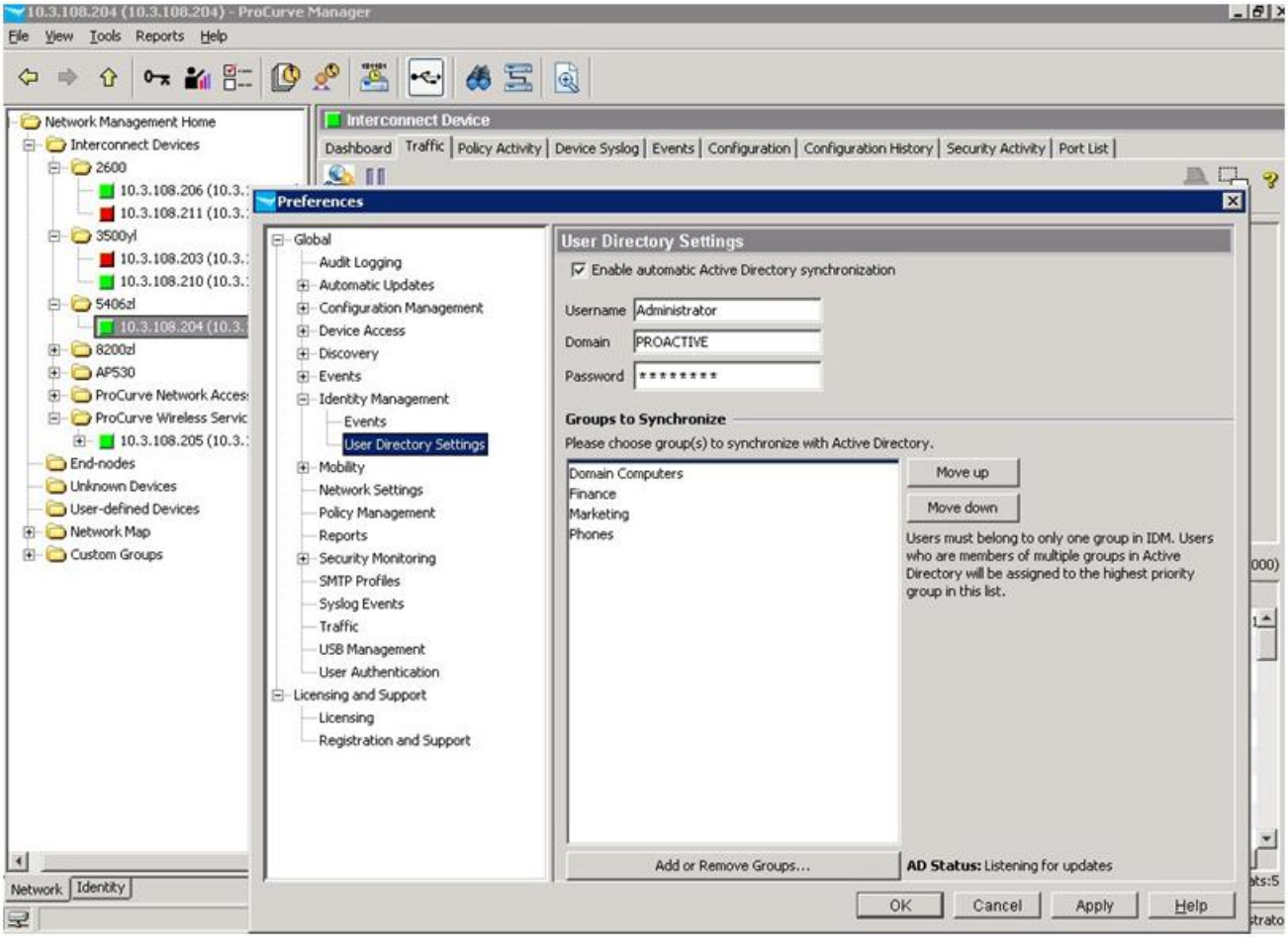
5. Using IDM with Active Directory

This section shows how to configure PCM/IDM for use with Active Directory.

5.1 Synchronize IDM with Active Directory

To synchronize ProCurve Manager with IDM with Active Directory:

1. Open PCM, and navigate to the Preferences > Identity Management > User Directory Settings window:

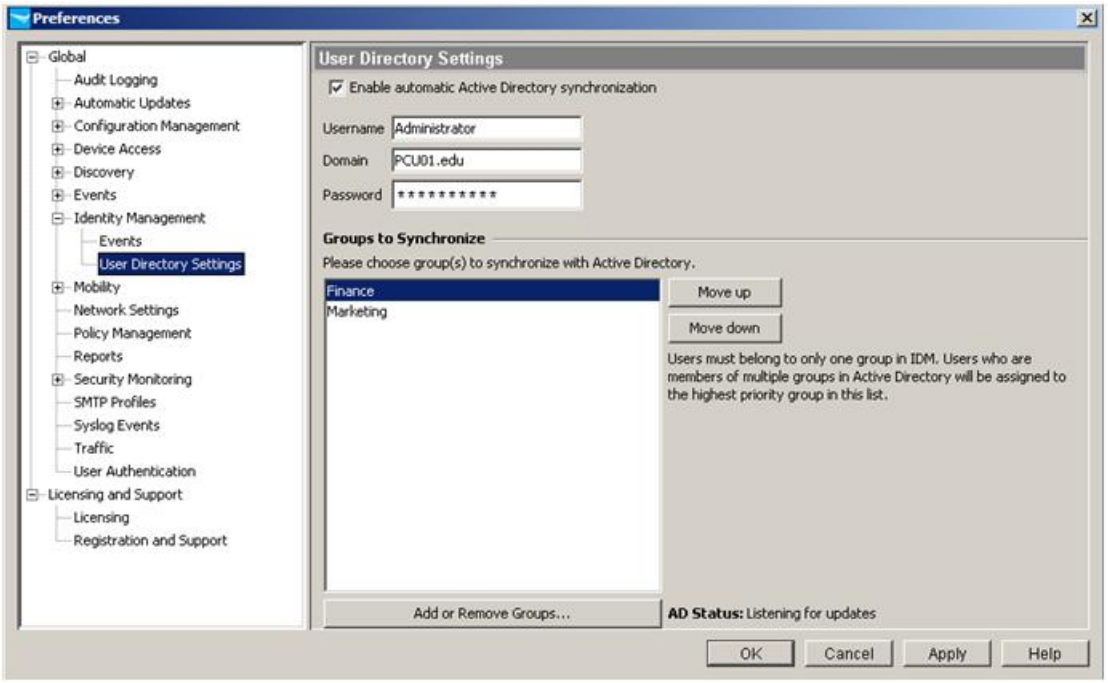


2. In the User Directory Settings window, ensure the Enable Active Directory synchronization box is checked.
3. Enter your credentials. IAS validates your credentials, and IDM is synchronized to Active Directory. IAS authentication occurs every time synchronization is performed.

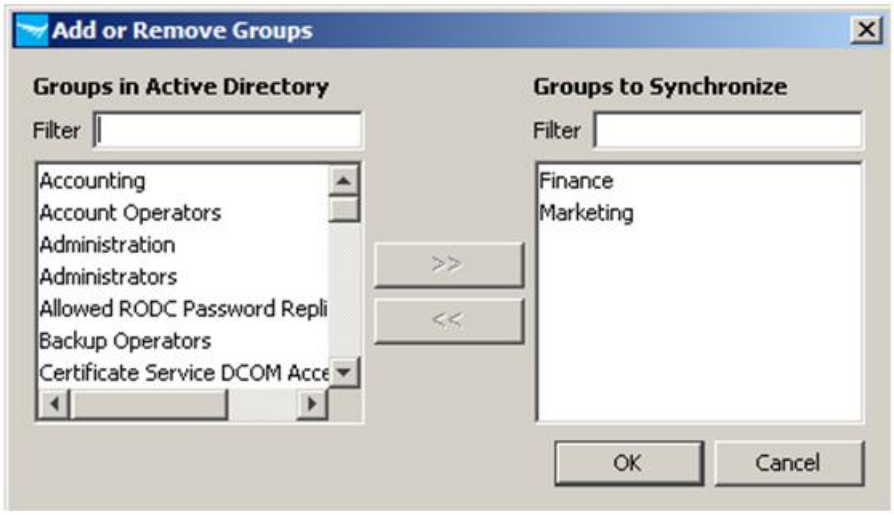
5.2 Show behavior of adding or deleting a user in a subgroup

Follow this example of adding and deleting a user to see how PCM/IDM is synchronized with AD.

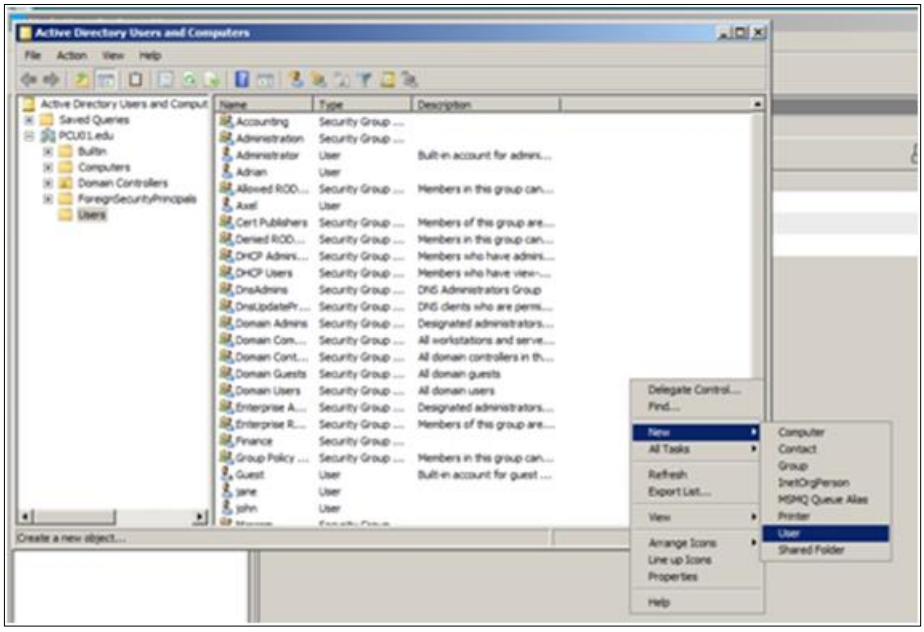
1. In IDM, in Tools | Preferences | User Directory settings, you can see groups to synchronize with Active Directory. This example shows that the two groups, Marketing and Finance, have been synchronized.



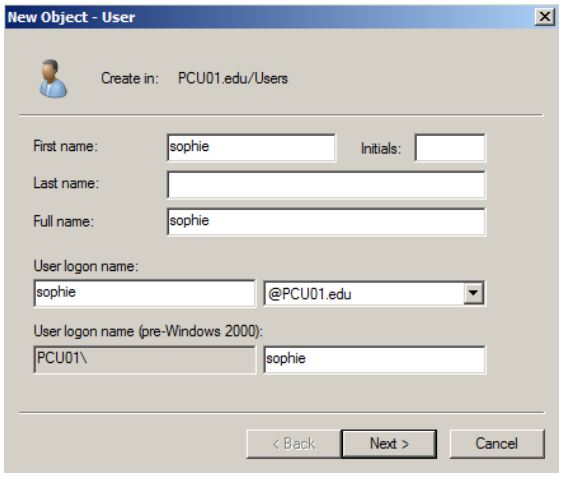
2. In IDM User Directory Settings, click the Add or Remove Groups button to show how groups from Active Directory are added or removed from the synchronization. For example:

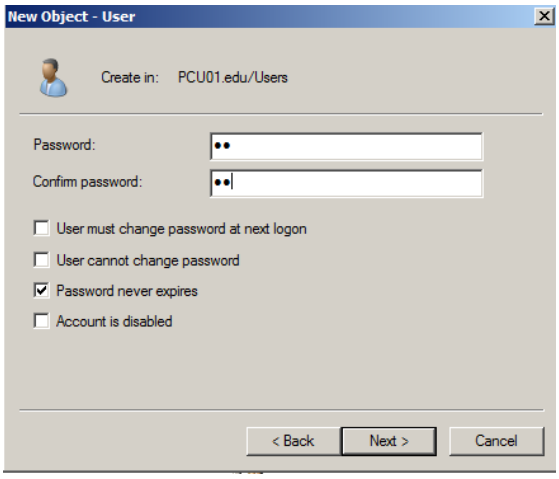


3. Now, go to Active Directory Users and Computers and create a new user:

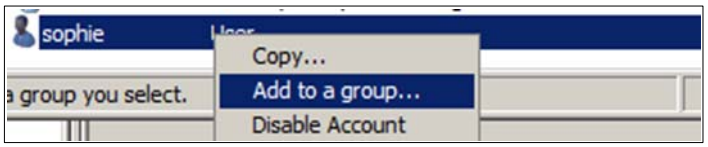


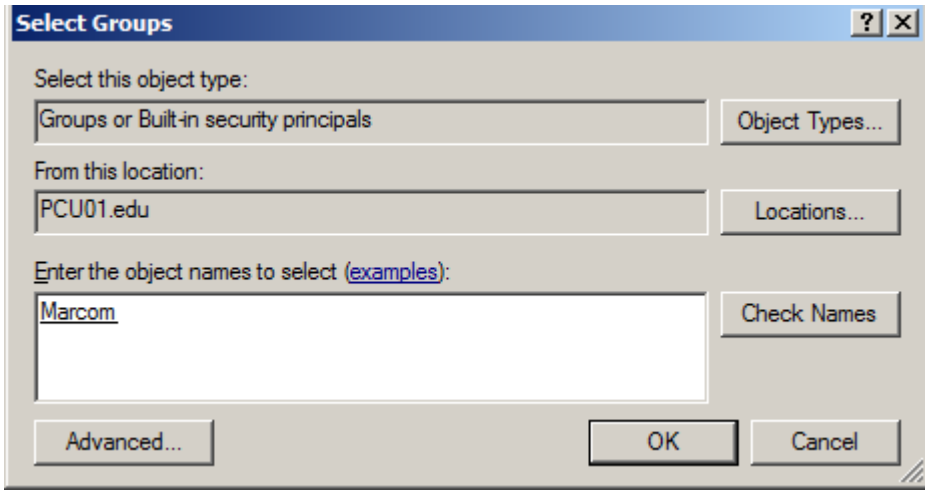
4. Give this new user a login name (sophie) and password:



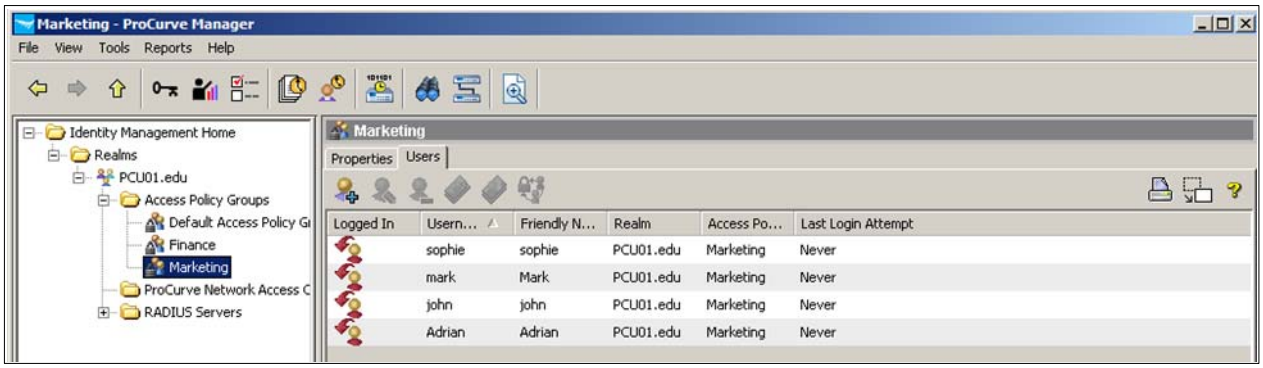


5. For this example, assign the new user sophie to the Marcom Group, which is a subgroup of the Marketing Group.

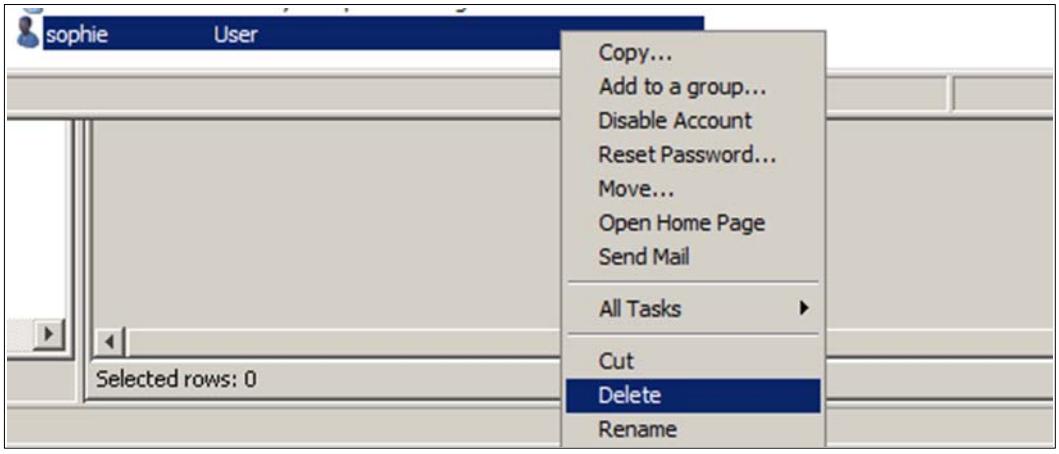




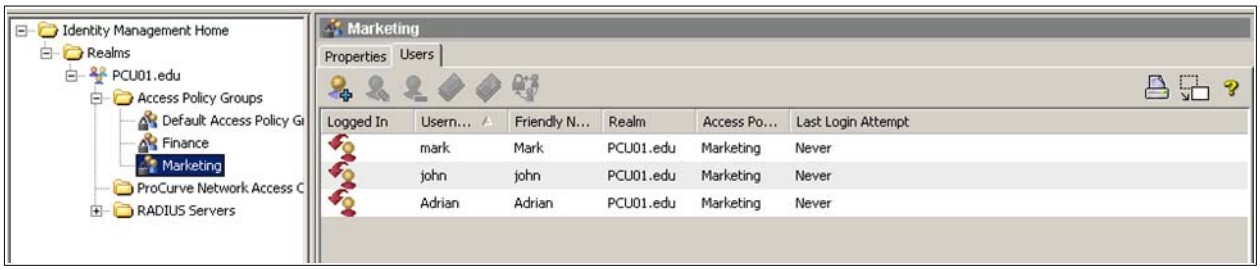
6. In IDM, you can confirm that this new user appears in the Marketing Group:



7. Now, for this example go to Active Directory and delete the user sophie:



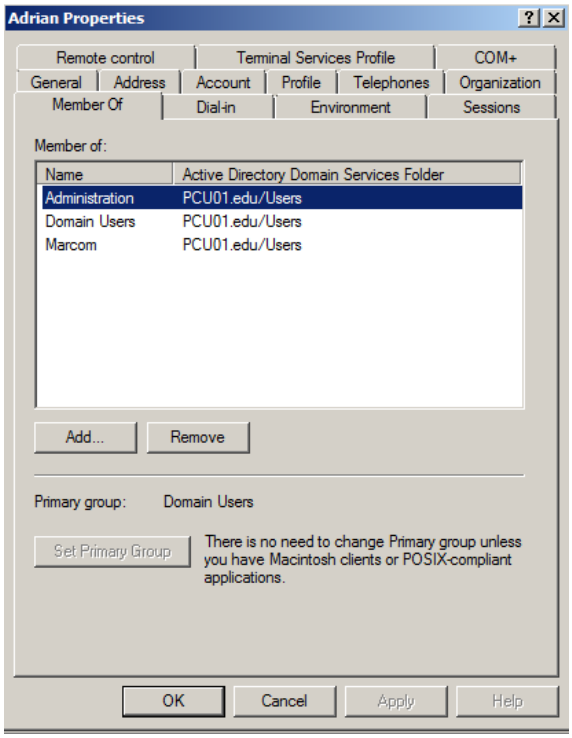
8. Return to IDM. Now you see the user sophie has disappeared from the Marketing group, indicating that IDM and Active Directory are synchronized:



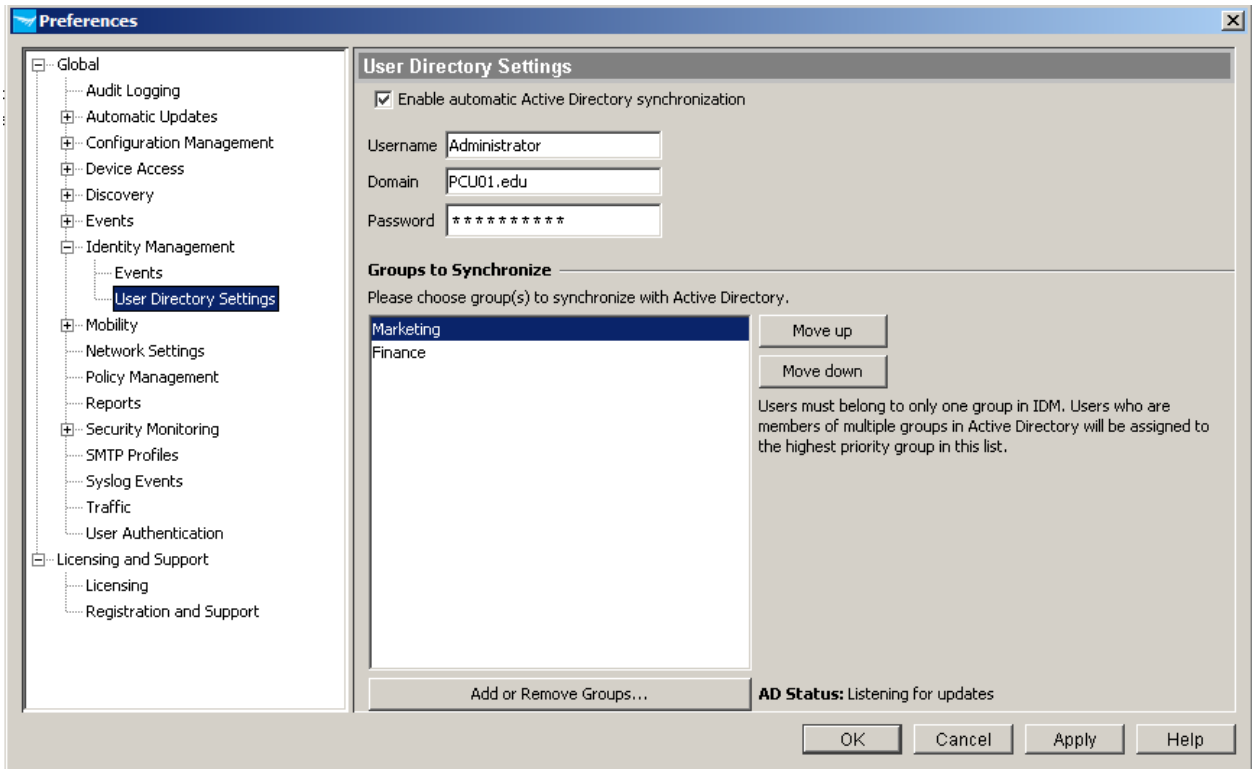
5.3 Show behavior of a user in multiple synchronized groups

In Active Directory, a user can be member of multiple groups. In IDM, a user can only belong to a single Access Policy Group. This raises a question: How does IDM handle a user that is a member of multiple synchronized groups? The following example illustrates a user in multiple subgroups.

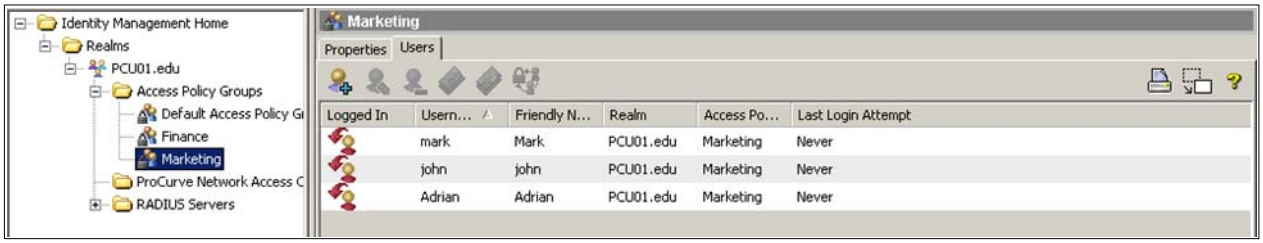
1. In Active Directory Users and Computers, the Member Of tab of user Adrian Properties shows that user Adrian belongs to two groups:
   - Marcom, which is a subgroup of Marketing
   - Administration, which is a subgroup of Finance



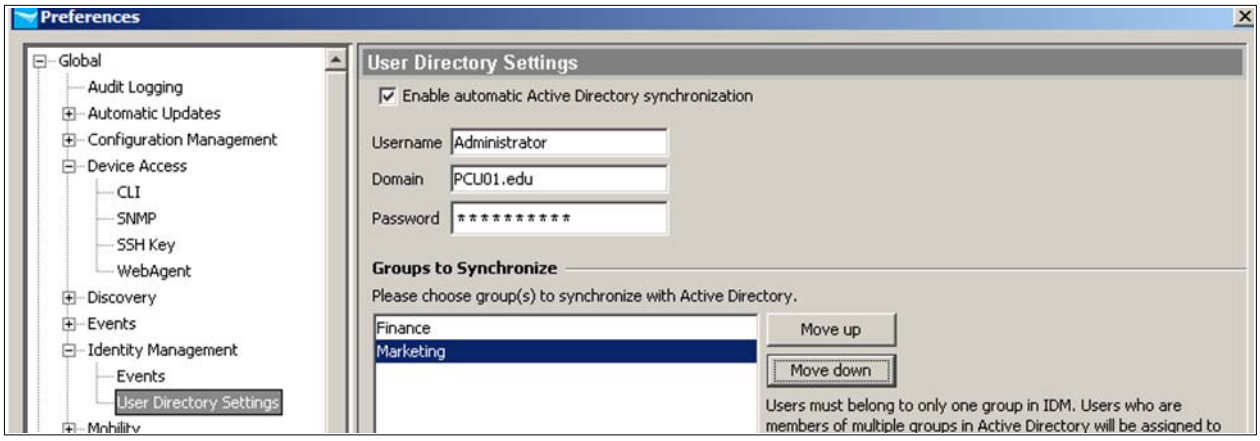
2. IDM's User Directory Settings shows the order in which the two groups have been synchronized. Marketing was first, followed by Finance:



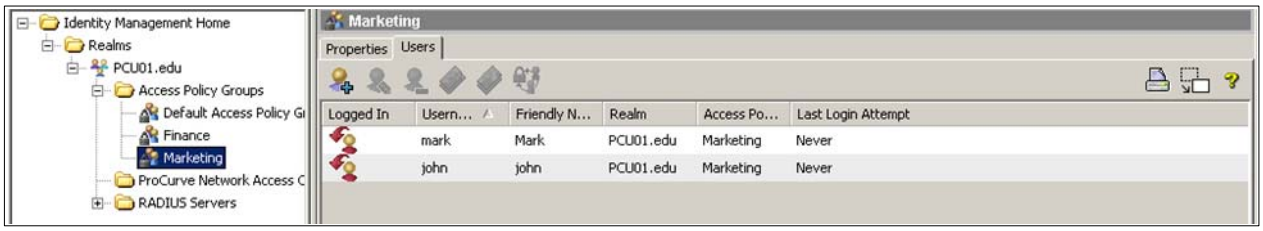
3. Looking at the Users shows that Adrian appears in Marketing, the first group on the list:

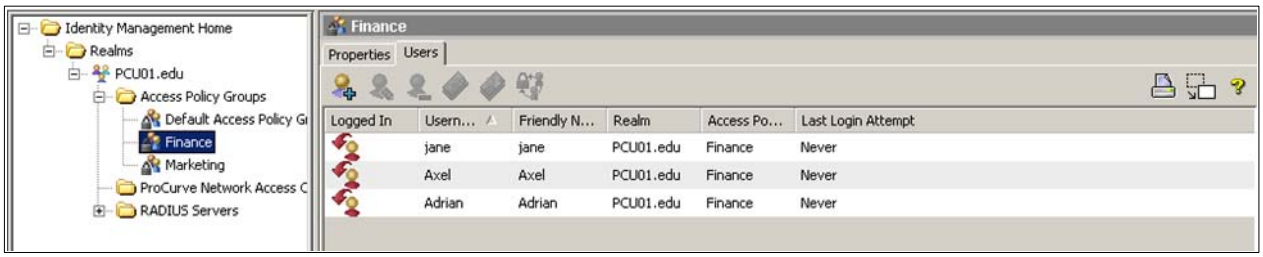


4. Now use the Move up and Move down buttons to change the order of the two groups, so that Finance appears *before* Marketing:



5. Look at the Marketing and Finance groups again. You can see that Adrian has disappeared from the group he was in, and now appears in the group that has been moved at the top of the list:





This demonstration illustrates that when a user belongs to multiple synchronized groups, IDM always places the user in the *first* group on the synchronization list. Remember to take this behavior into account when planning synchronization of IDM with Active Directory.

7. Reference documents

This concludes the procedure for configuring 802.1X authentication.

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

- For the *ProCurve Identity Driven Manager User's Guide* for Software Release 2.3:
  http://cdn.procurve.com/training/Manuals/IDM_UG-59908851-0508.pdf

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

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

- For ProCurve Switch 2610 series manuals:
  http://www.hp.com/rnd/support/manuals/2610.htm

For further information, please visit www.procurve.eu

4AA2-1623EEE, July 2008