

# Synchronizing ProCurve IDM and Windows Active Directory



## Contents

1. Introduction	2
2. Prerequisites	2
3. Network and Active Directory tree diagrams	2
4. Synchronization and nested group capabilities in IDM 2.3	2
5. Using IDM with Active Directory	3
5.1 Synchronize IDM with Active Directory	3
5.2 Show behavior of adding or deleting a user in a subgroup	4
5.3 Show behavior of a user in multiple synchronized groups	7
7. Reference documents	10

## **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.



ProCurve Switch 5400zl

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:

₩10.3.108.204 (10.3.108.204) - ProCurve	e Manager			5
Ele Yew Iools Reports Help				
Image: Servic Broken Services         Image: Service Broken Service Broken Services         Image: Service Broken	Mobility     Meterorise     Source Access     Source     Source Access     Source     Sou	Wity       Device Syslog       Events       Configuration       Configuration       Configuration         User Directory Settings       Image: Configuration       Configuration       Configuration       Configuration         Image: Configuration       Image: Configuration       Configuration       Configuration       Configuration         Username       Administrator       Image: Configuration       PROACTIVE         Domain       PROACTIVE       Image: Configuration       PROACTIVE         Please choose group(s) to synchronize with       Domain Computers       Finance         Phones       Phones       Image: Configuration       Provide the synchronize with	Figuration History       Security Activity       Port List         Image: Security Active Directory.       Image: Security Active Directory         Move up       Move down         Users must belong to only one group in IDM. Users who are members of multiple groups in Active Directory will be assigned to the highest priority group in this list.	99 000)
A		Add or Remove Groups	AD Status: Listening for updates	ts:5
3			OK Cancel Apply Help	trate

- 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.

⊝Global	User Directory Settings	
	F Enable automatic Active Directory synch	ronization
Configuration Management     Device Access	Username Administrator	
Discovery     E-Events	Password ********	
Identity Management     Events     User Directory Settings	Groups to Synchronize	Active Directory.
Mobility     Network Settings     Policy Management     Reports     Security Monitoring     SMTP Profiles     Syden Events	Finance Marketing	Move up Move down Users must belong to only one group in IDM. Users who are members of multiple groups in Active Directory will be assigned to the highest priority group in this list.
Traffic     User Authentication     User Authentication     User Support     Ucensing     Registration and Support		
	Add or Remove Groups	AD Status: Listening for updates

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:

Groups in Active Directory	Groups to Synchronize
Accounting Account Operators Administration Administrators Allowed RODC Password Repli Backup Operators Certificate Service DCOM Acce	Finance Marketing
	OK Cancel

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

ie Action View Help					1
	10013	SUTES	8		
Active Directory Users and Comput	Nane	Type	Description		
Computers and Computer     Second Queries     Second Queries     Second Queries     Computers     Computers     Second Queries     Dense Controllers     Dense     Dense	Termine REAccurring REAccurring REAcounting Adversition REAcounting Adversition REAcounting REAcounting REAcounting REAcounting REAcounting REAcounting REAcounting REAcounting REAcounting REAcounting REACOUNTING REACOUNT	I Dee Security Group Security Group User Security Group User Security Group Security Group User	Delignment Bult-in account for admini Henders in this group can Henders in this group can Henders in this group can Henders who have adminis Drid Administrators Group Drid derts who are perm Drid derts who are perm Bal contrations and are-e Al domain controllers in th Al domain guests Al domain users Designated administrators Henders in this group can Bult-in account for guest	Deingate Control Find Al Taola Referat Export Lat Vers	Computer Contact Contact Contact MINQ Queue Alass Proter
veale a new object				Amange Icons +	Shared Folder
				Properties	
				Help	

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

New Object - User	X New Object - User
Create in: PCU01.edu/Users	Create in: PCU01.edu/Users
First name: sophie Initials:	Password:
Last name:	Confirm password:
Full name: sophie	User must change password at next logon
User logon name:	User cannot change password
sophie @PCU01.edu 🔻	Password never expires
User logon name (pre-Windows 2000):	Account is disabled
PCU01\ sophie	
< Back Next > Cancel	< Back Next >

x

Cancel

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

sophie	Heor	
Soprie	Copy	
a group you select.	Add to a group	
	Disable Account	J.

Select Groups		? ×
Select this object type:		
Groups or Built-in security principals		Object Types
From this location:		
PCU01.edu		Locations
Enter the object names to select (examples):		
Marcom		Check Names
Advanced	ОК	Cancel

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

🔀 Marketing - ProCurve Manager						
File View Tools Reports Help						
♦ ♦ ♦ • ₩ ₩ ₩	🧟 🍇 🔄	- T				
🖃 🗁 Identity Management Home	🐴 Marketing					
🖻 🗁 Realms	Properties Users					
- 🍄 PCU01.edu     - 🗁 Access Policy Groups	2 2 2 4 4	- <del>Q</del> Z				🕒 🖓
- 🏰 Default Access Policy G	Logged In Usern 🛆	Friendly N	Realm	Access Po	Last Login Attempt	
- A Finance	Sophie sophie	sophie	PCU01.edu	Marketing	Never	
Marketing	Mark mark	Mark	PCU01.edu	Marketing	Never	
Procurve Network Access C     Access C     Access C     Access C	iohn 🖉	john	PCU01.edu	Marketing	Never	
	Net Adrian	Adrian	PCU01.edu	Marketing	Never	

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

	Copy Add to a group Disable Account Reset Password Move Open Home Page Send Mail
	All Tasks 🕨
	Cut
Selected rows: 0	Delete
	Rename

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

🖃 🗁 Identity Management Home	🏄 Market	ing					
🖻 🗁 Realms	Properties	Users					
🖻 – 🌺 PCU01.edu	& &	200	<b>Q</b>				🔓 🖓 💡
- 🔐 Default Access Policy Gi	Logged In	Usern 🛆	Friendly N	Realm	Access Po	Last Login Attempt	
Finance	€2	mark	Mark	PCU01.edu	Marketing	Never	
ProCurve Network Access C	<b>S</b>	john	john	PCU01.edu	Marketing	Never	
RADIUS Servers	<b>S</b>	Adrian	Adrian	PCU01.edu	Marketing	Never	

#### 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:
  - o Marcom, which is a subgroup of Marketing
  - $\circ$   $\;$  Administration, which is a subgroup of Finance

	1
Remote control General Address Member Of	Terminal Services Profile         COM+           Account         Profile         Telephones         Organization           Dial-in         Environment         Sessions
Member of:	
Name	Active Directory Domain Services Folder
Administration	PCU01.edu/Users
Domain Users	PCU01.edu/Users
Marcom	PCU01.edu/Users
, Add	Remove
Primary group: I	Domain Users
Primary group: I	Domain Users           P         There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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

·· Global	User Directory Settings	
<ul> <li>Audit Logging</li> <li>Automatic Updates</li> <li>Configuration Management</li> <li>Device Access</li> <li>Discovery</li> <li>Events</li> <li>Identity Management</li> <li>Events</li> <li>User Directory Settings</li> <li>Mobility</li> <li>Network Settings</li> <li>Policy Management</li> <li>Reports</li> <li>Switz System Setting</li> <li>System Setting</li> <li>Traffic</li> <li>User Authentication</li> <li>Licensing and Support</li> <li>Licensing</li> <li>Registration and Support</li> </ul>	Image: Section processing section of the section processing section of the secti	rectory. Move up Move down Users must belong to only one group in IDM. Users who are members of multiple groups in Active Directory will be assigned t the highest priority group in this list.
	Add or Remove Groups	AD Status: Listening for updates

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

- Contractive Management Home	Marketing						
E - ₩ PCU01.edu	Properties	Lisers	Q7				A . ?
🔐 Default Access Policy G	Logged In	Usern A	Friendly N	Realm	Access Po	Last Login Attempt	
Finance	€2	mark	Mark	PCU01.edu	Marketing	Never	
Marketing	1	john	john	PCU01.edu	Marketing	Never	
In Flocul ve Network Access C Image: A constraint of the second seco	4	Adrian	Adrian	PCU01.edu	Marketing	Never	

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

Market Preferences	<u>× and a second s</u>
GlobalAudit LoggingAutomatic UpdatesConfiguration ManagementDevice AccessCLISNMPSSH KeyWebAgentDiscovery	User Directory Settings         Image: Enable automatic Active Directory synchronization         Username       Administrator         Domain       PCU01.edu         Password       *********         Groups to Synchronize         Please choose group(s) to synchronize with Active Directory.
Events     Events     User Directory Settings     F-Mohility	Finance Move up Marketing Users must belong to only one group in IDM. Users who are members of multiple groups in Active Directory will be assigned to

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:



	Finance Properties	e Users					
	& &	200					₽ 🖓 🤞
Ar Default Access Policy Gr     Finance     Ar Marketing     ProCurve Network Access C     B     C ADIUS Servers	Logged In	Usern 🛆	Friendly N	Realm	Access Po	Last Login Attempt	
	<b>1</b>	jane	jane	PCU01.edu	Finance	Never	
	5	Axel	Axel	PCU01.edu	Finance	Never	
	1	Adrian	Adrian	PCU01.edu	Finance	Never	

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: <u>http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm</u> <u>http://www.hp.com/rnd/support/manuals/IDM.htm</u>
- 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: <u>http://www.hp.com/rnd/support/manuals/2610.htm</u>

For further information, please visit www.procurve.eu



© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft, Windows, and Active Directory are U.S. registered trademarks of Microsoft Corporation.

4AA2-1623EEE, July 2008