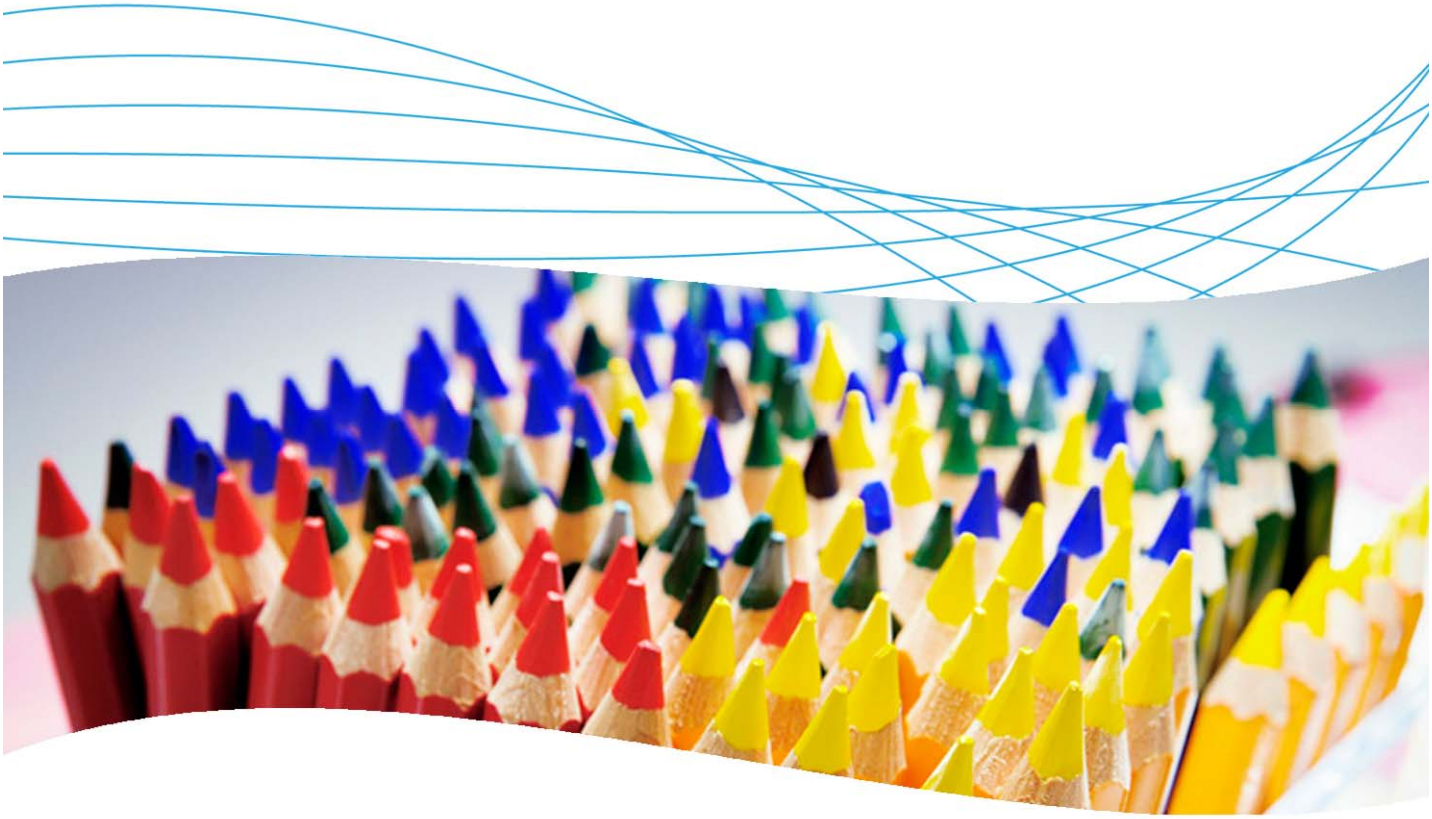
An HP ProCurve Networking Application Note

Achieving regulatory compliance with reports from ProCurve PCM, IDM, and NIM



Contents

1. Introduction **2**

2. Prerequisites **2**

3. Network diagram **2**

4. Instructions for generating reports **2**

4.1 Customize the report header 2

4.2 Create a report on the change history for a device's credentials 3

4.3 Create a report on device access security 9

4.4 Create a device access password audit report 9

4.5 Create a report of IDM user session history 12

4.6 Confirm network immunity with a report on actions by policy name 14

4.7 Confirm network immunity with reports on offenders 16

5. Reference documents **17**

1. Introduction

The reporting capabilities of ProCurve Manager (PCM), Identity-Driven Manager (IDM) and Network Immunity Manager (NIM) can be of great help in achieving compliance with governmental regulations and reporting requirements. This document describes how to set up features of this software to generate reports for auditing and regulatory compliance.

2. Prerequisites

This application note assumes you have a Windows Server 2003 installed, along with PCM, IDM and NIM. Examples are based on a configuration using a ProCurve Switch 5400zl and a ProCurve Switch 3500yl.

3. Network diagram

Figure 1 shows the network referenced in this application note.

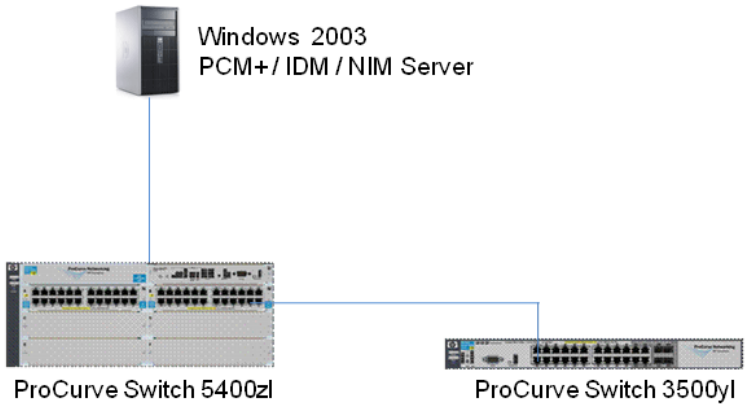


Figure 1. Network diagram used for generating reports in these examples

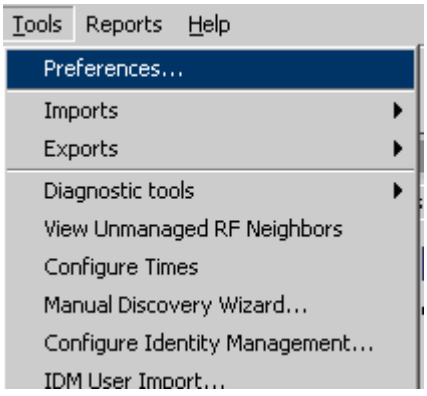
4. Instructions for generating reports

This sections consists of step-by-step instructions for generating useful reports

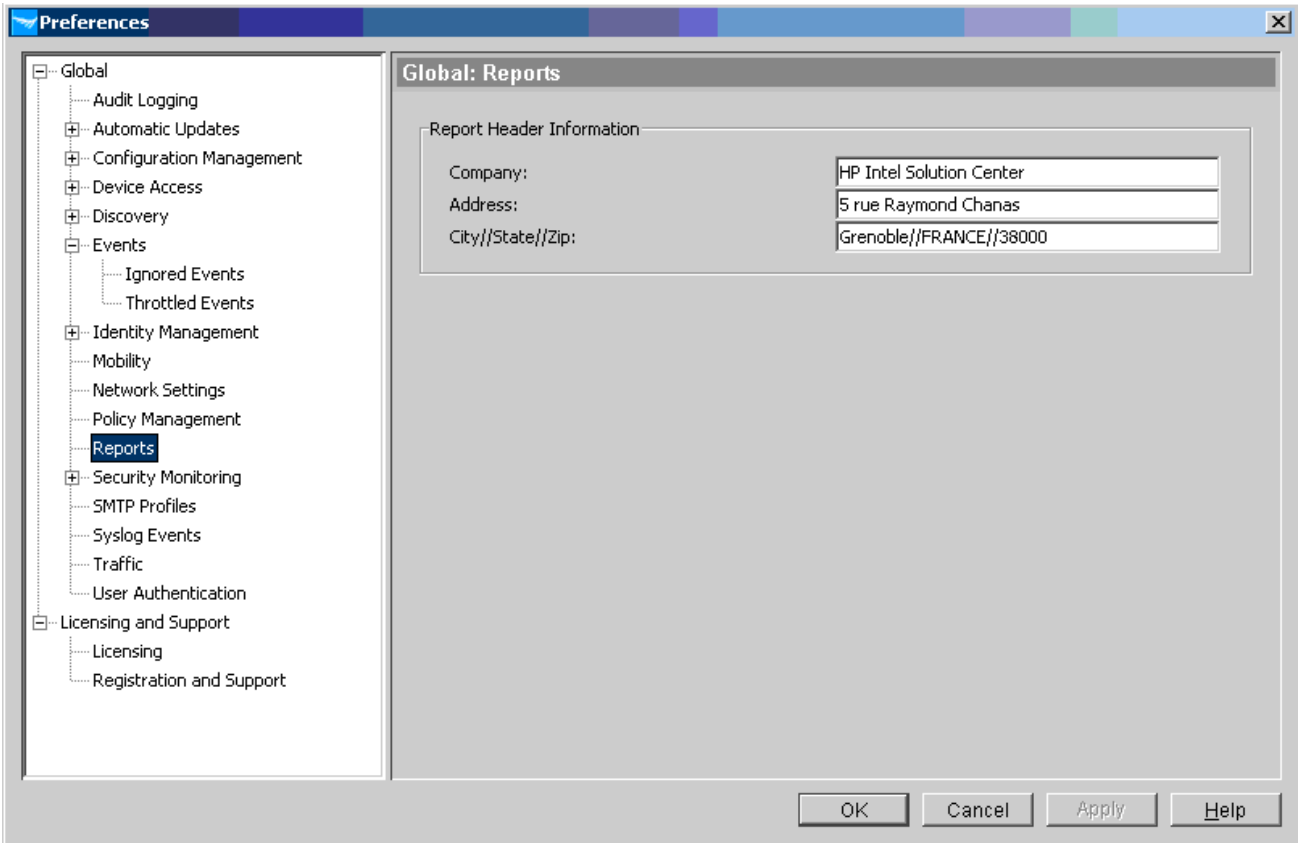
4.1 Customize the report header

You can customize the report header information that will appear on all reports. For example, you might wish to add the name and address of your company. To customize the report header:

- In ProCurve Manager, go to Tools > Preferences > Global > Reports. You see the Global: Reports panel where you can customize the Report Header Information. This header information will appear on all reports:



For example:

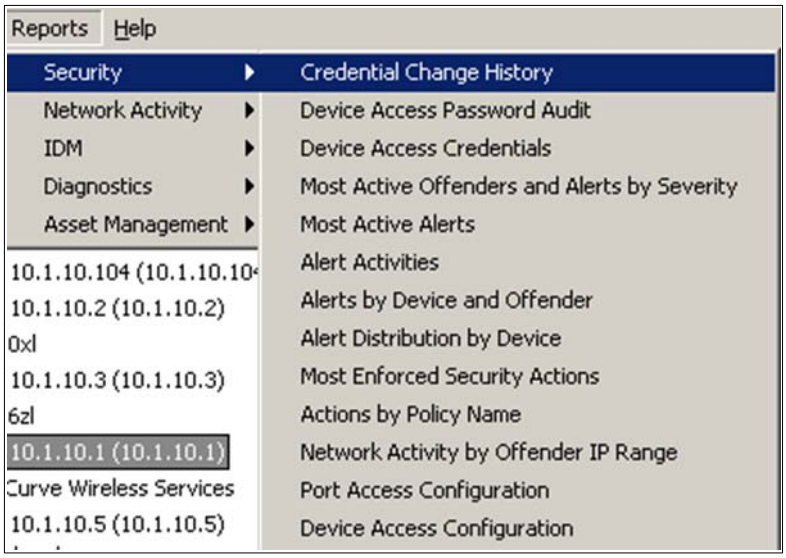


4.2 Create a report on the change history for a device's credentials

You can easily create a report documenting the change history for access credentials such as login names and passwords. The access credentials include SNMP community names (read and write and SNMPv3 credentials, if specified), and Telnet manager and operator usernames and passwords. This report can be on a per-device basis. The following example illustrates how to create the report.

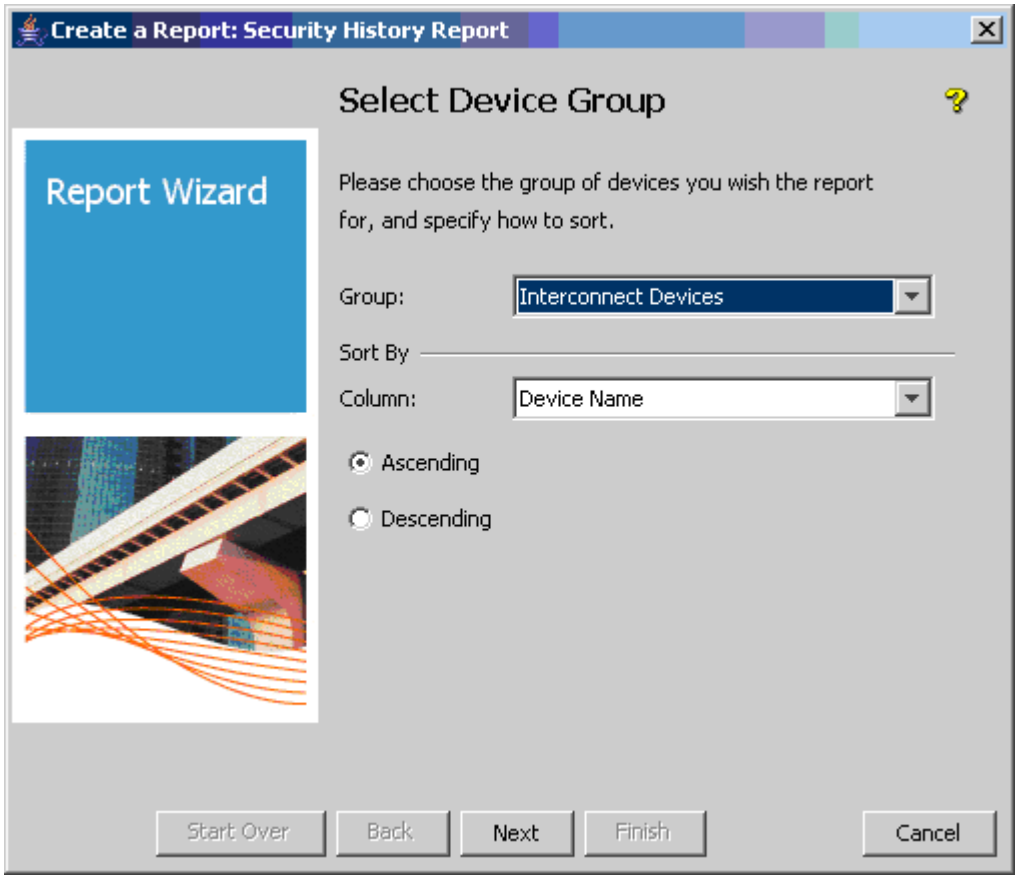
4.2.1 To generate the initial report:

1. Connect the Windows 2003/PCM server to port A2 on the ProCurve Switch 5400.
2. Open Reports > Security > Credential Change History:

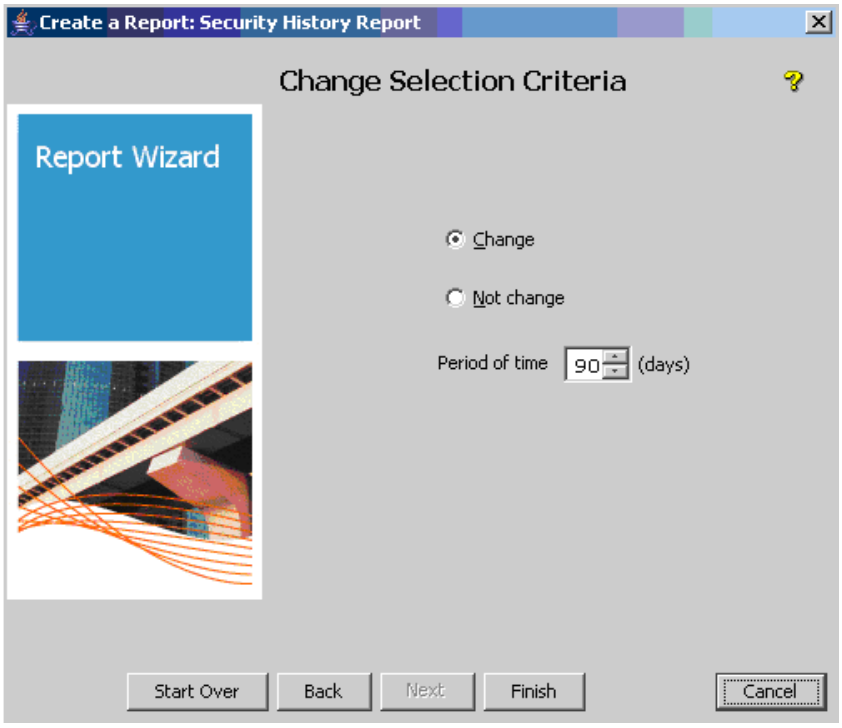


This launches the Report Wizard.

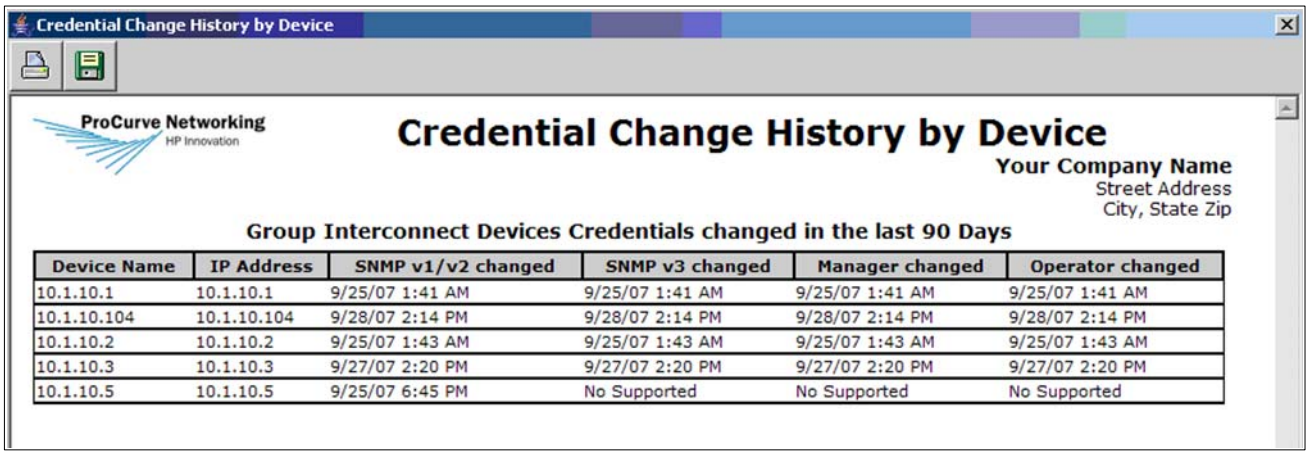
3. In the Report Wizard's Select Device Group window, choose the group Interconnect Devices:



4. In the Change Selection Criteria window, leave the selection criteria at the default setting: passwords that have changed in the last 90 days:



5. Click Finish to generate the report. You see for each password or community name the date and time of last change:

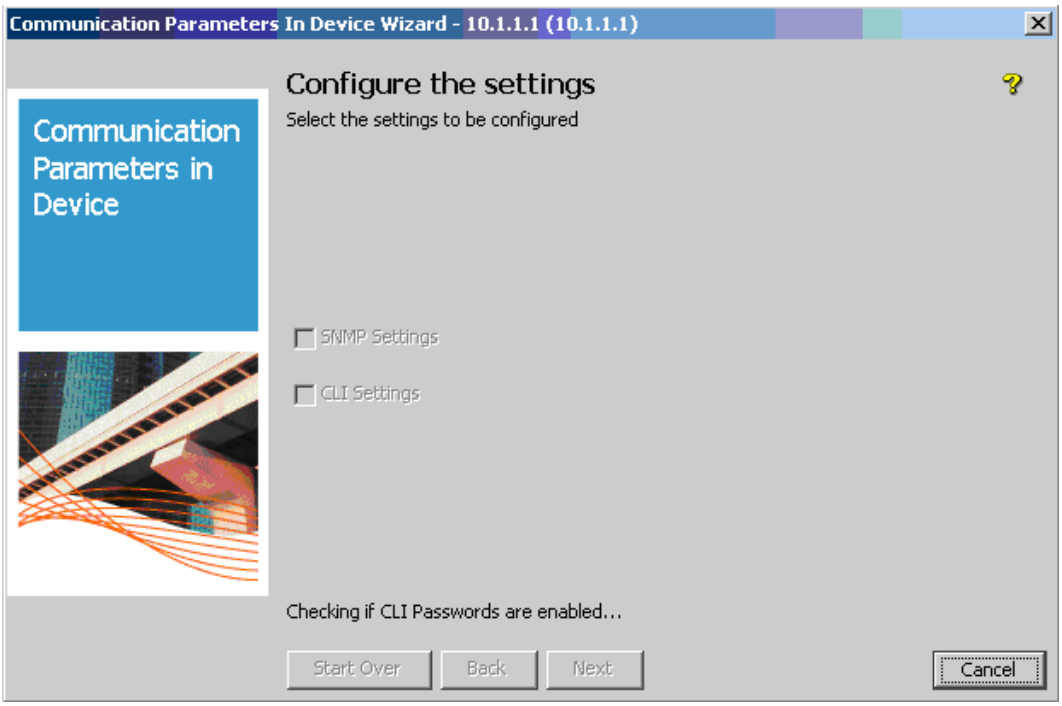


Device Name	IP Address	SNMP v1/v2 changed	SNMP v3 changed	Manager changed	Operator changed
10.1.10.1	10.1.10.1	9/25/07 1:41 AM	9/25/07 1:41 AM	9/25/07 1:41 AM	9/25/07 1:41 AM
10.1.10.104	10.1.10.104	9/28/07 2:14 PM	9/28/07 2:14 PM	9/28/07 2:14 PM	9/28/07 2:14 PM
10.1.10.2	10.1.10.2	9/25/07 1:43 AM	9/25/07 1:43 AM	9/25/07 1:43 AM	9/25/07 1:43 AM
10.1.10.3	10.1.10.3	9/27/07 2:20 PM	9/27/07 2:20 PM	9/27/07 2:20 PM	9/27/07 2:20 PM
10.1.10.5	10.1.10.5	9/25/07 6:45 PM	No Supported	No Supported	No Supported

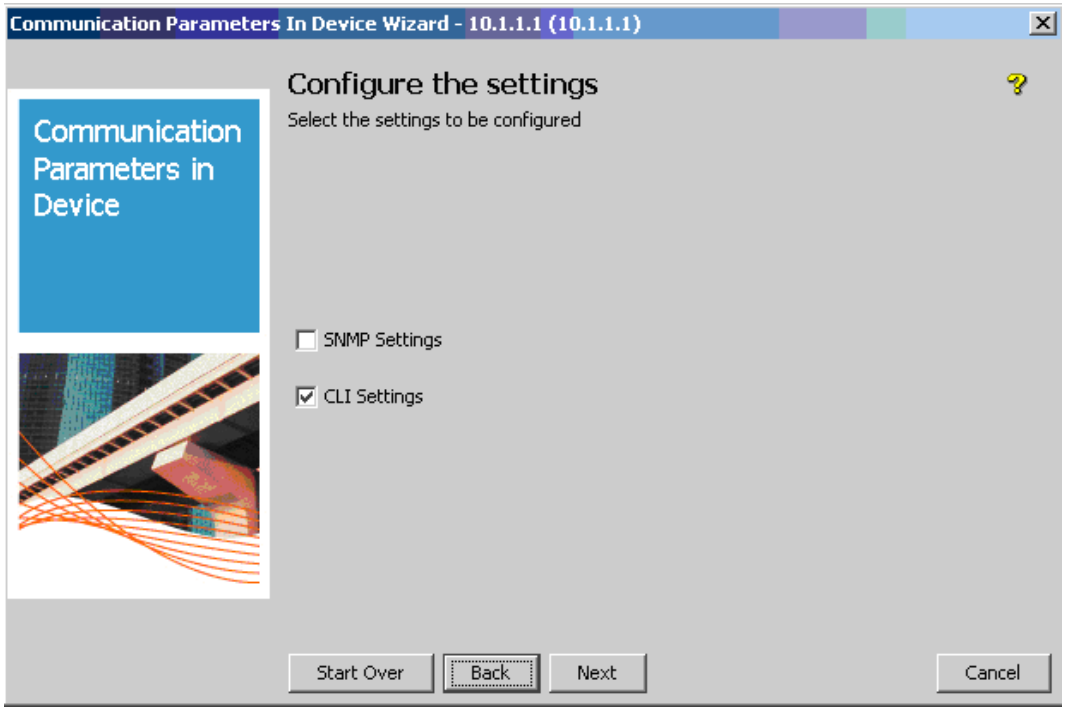
4.2.2 To change CLI credentials:

To use PCM to change CLI credentials for the ProCurve Switch 5400:

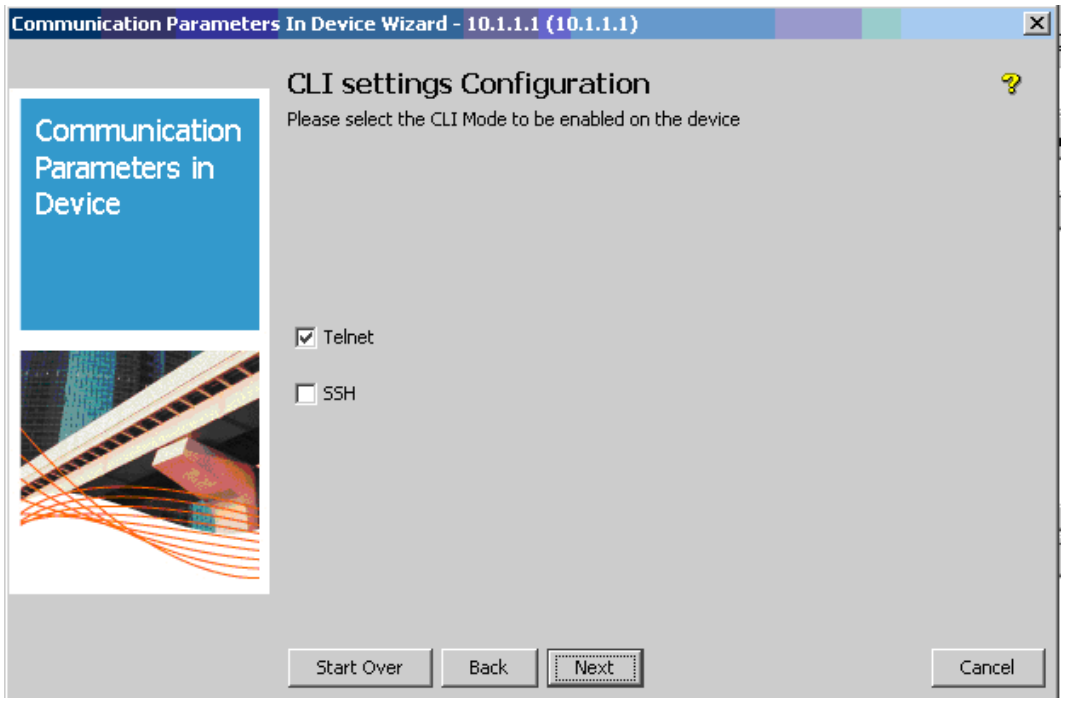
1. Highlight the 5400 (10.1.1.1) in the Devices List, then select the Communication Parameters in Device icon  from the Device Manager menu to launch the wizard for configuring communication parameters in the device. PCM checks whether CLI and SNMP passwords are enabled, a process that it takes about 15 seconds:



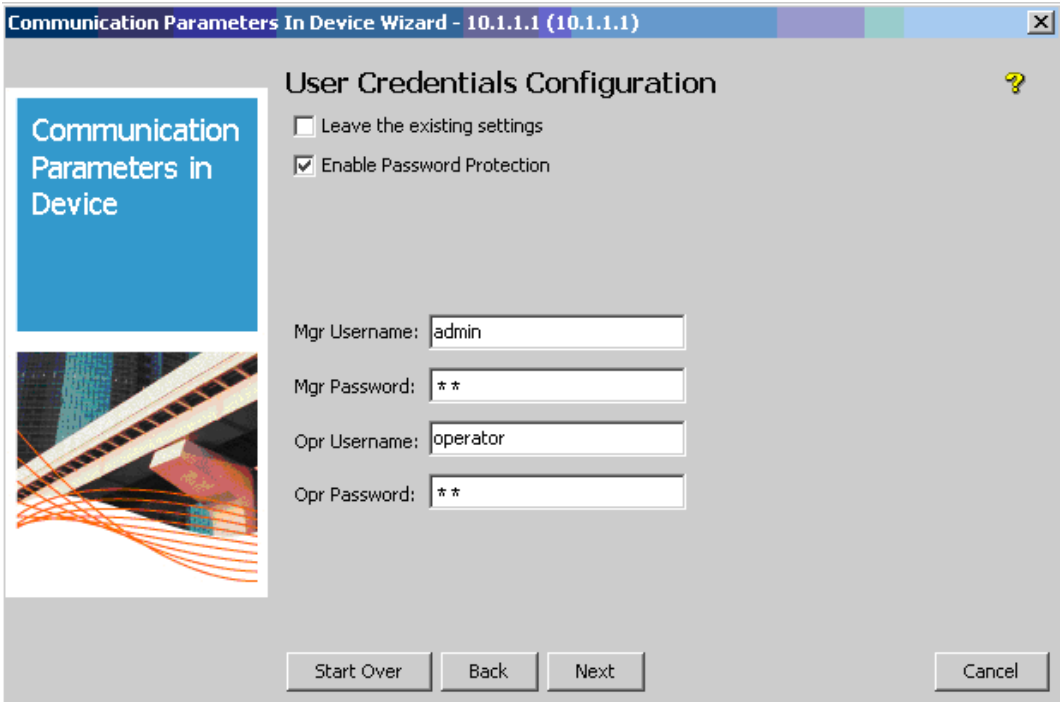
2. In the wizard, choose CLI Settings to be configured on the device:



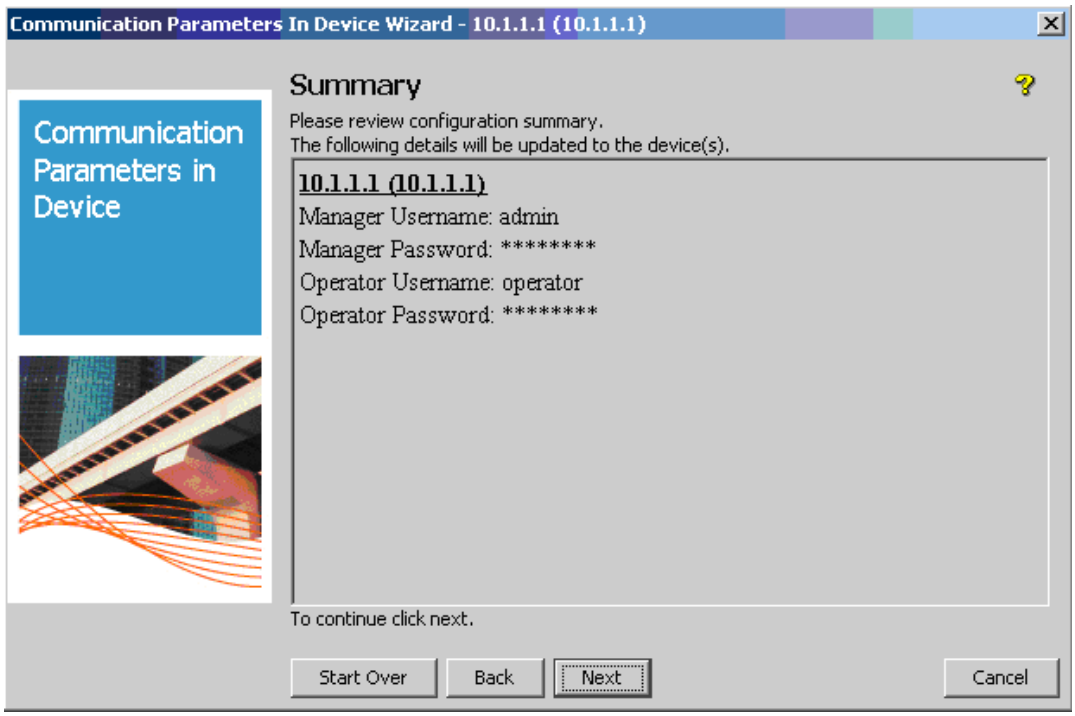
3. At the next screen, choose Telnet for the CLI Mode to be enabled on the device:



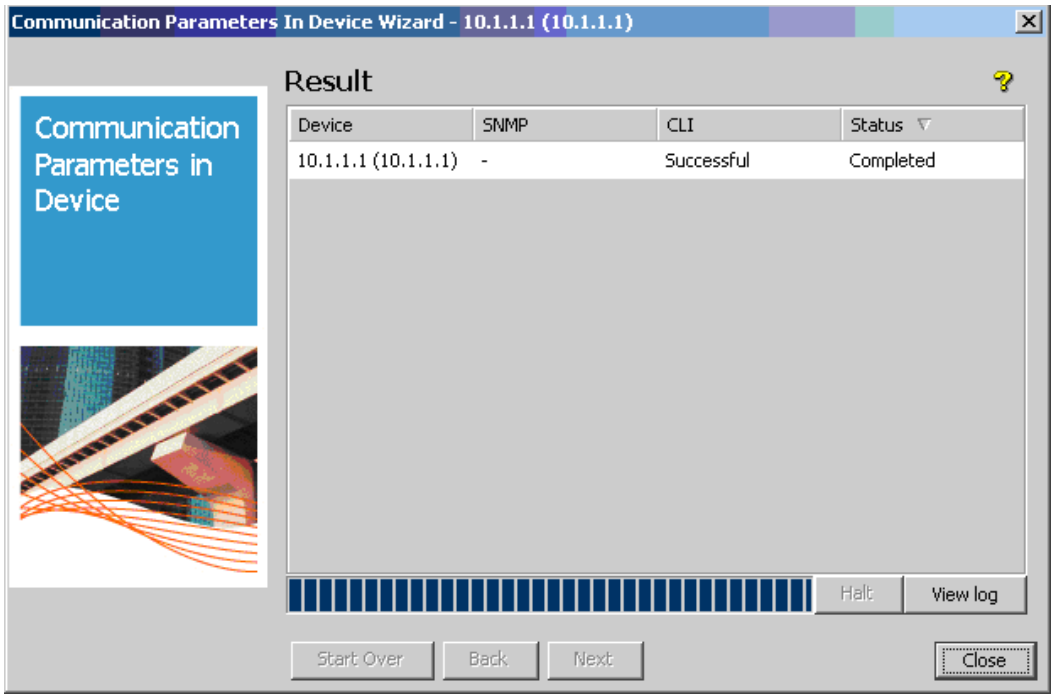
4. In the User Credentials Configuration window, ensure the Mgr Username is set to admin, and the Opr Username is set to operator. Then set the passwords for these users to hp:



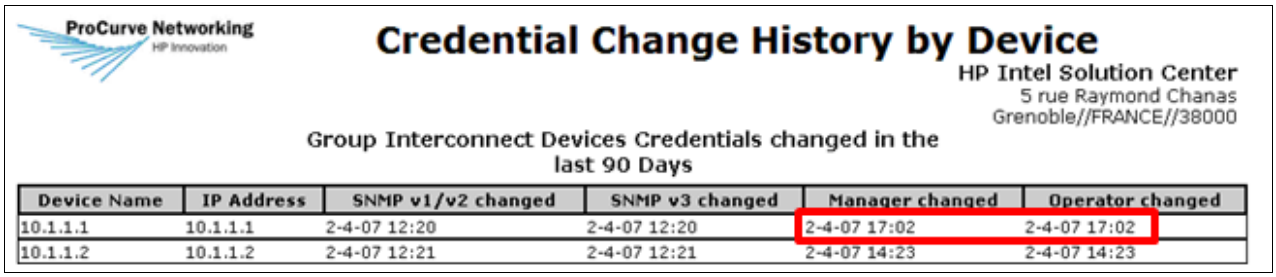
5. Review the configuration summary:



6. Finally, check the Result window and note that the new CLI parameters have been applied with success:

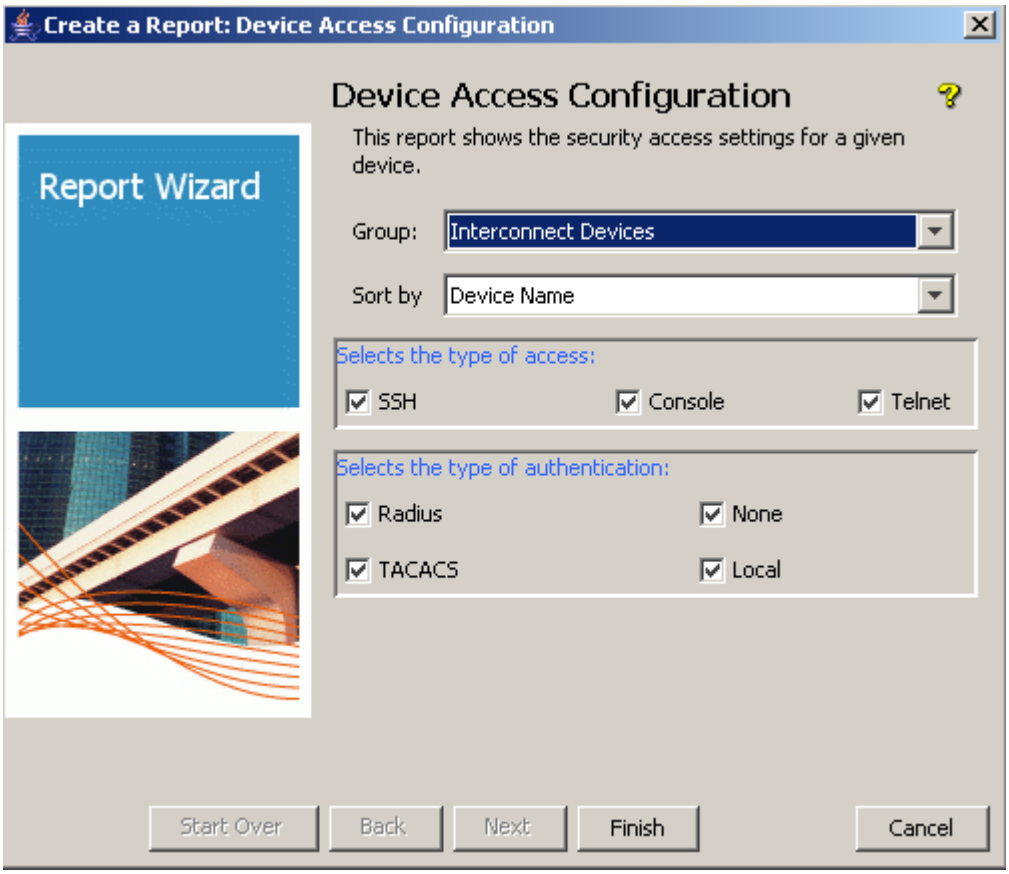


7. Now generate the report again. You see that manager and operator credentials for device 10.1.1.1 have changed:



4.3 Create a report on device access security

The Device Access Configuration Report shows the security settings for a device or a list of devices. It shows type of access (SSH, Console, Telnet), type of authentication (Radius, TACACs, Local), and the number of ports locked and running a secure protocol (Web-auth, MAC-auth, 802.1X). For example:



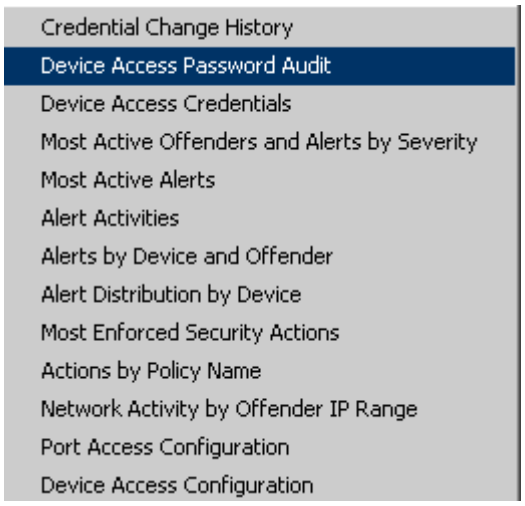
4.4 Create a device access password audit report

This audit and report enable the administrator to ensure that the passwords and community names configured on network equipment are adequately secure—that is, that they are at least the minimum length and contain at least the specified number of lowercase characters, uppercase characters, numbers, and special characters.

To create a device access password audit report:

1. Connect the server to port A2 on the 5400.

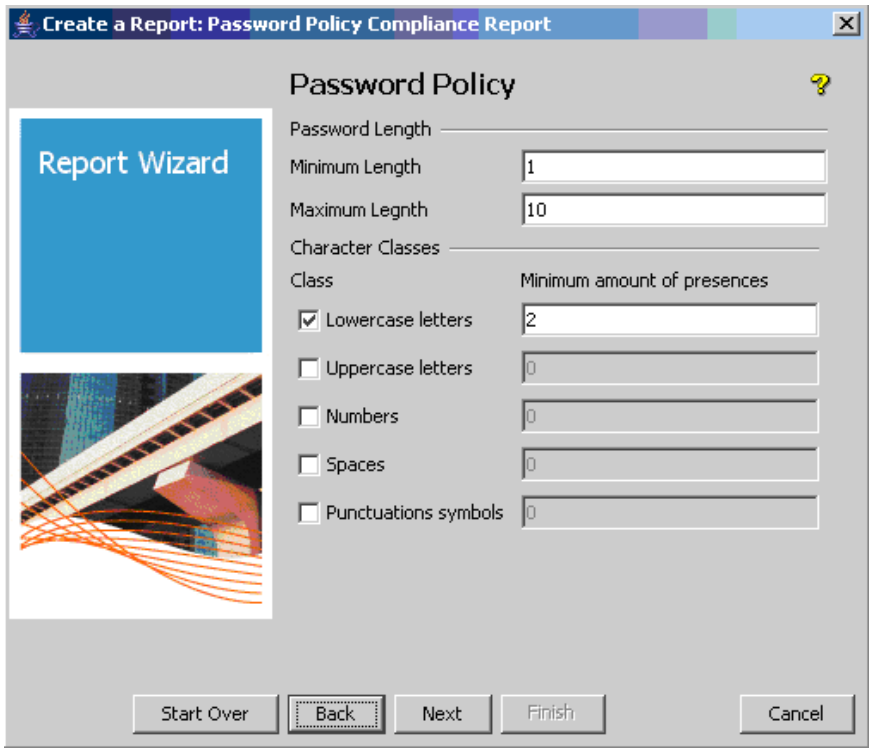
2. Open Reports > Security > Device Access Password Audit:



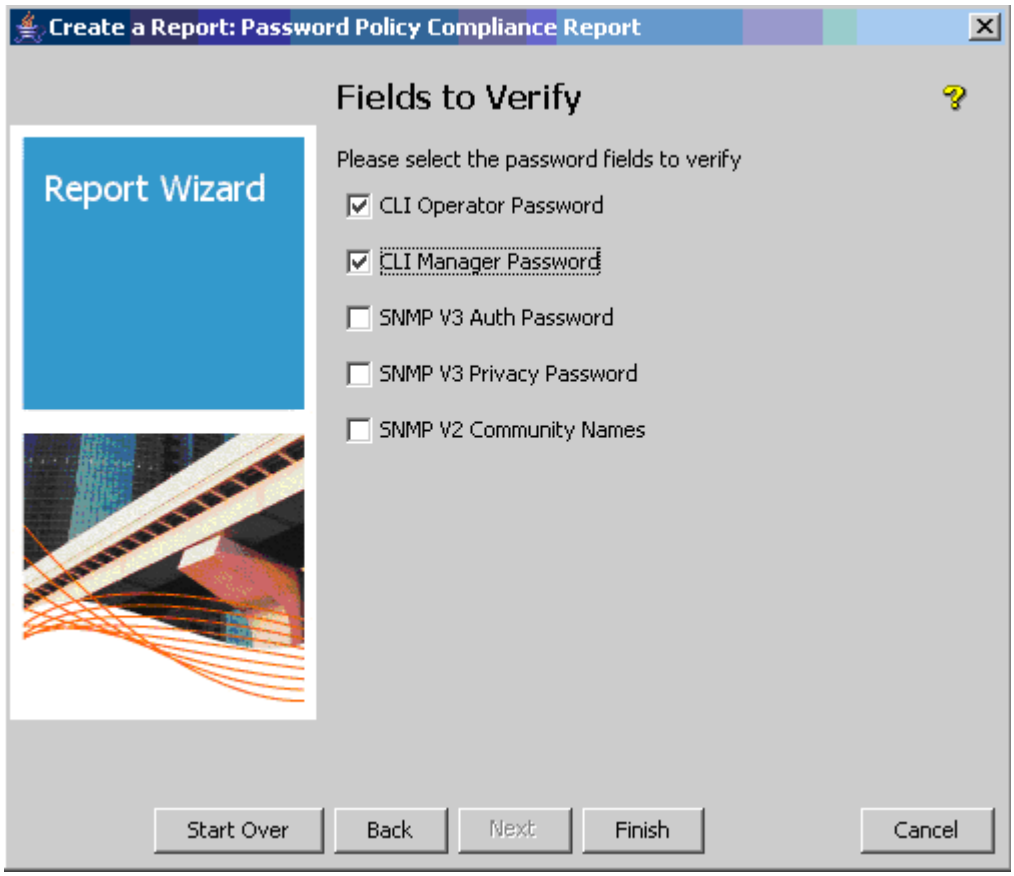
This launches the Report Wizard.

3. In the Report Wizard's Device Access Password Audit window, for Group, choose Interconnect Devices:

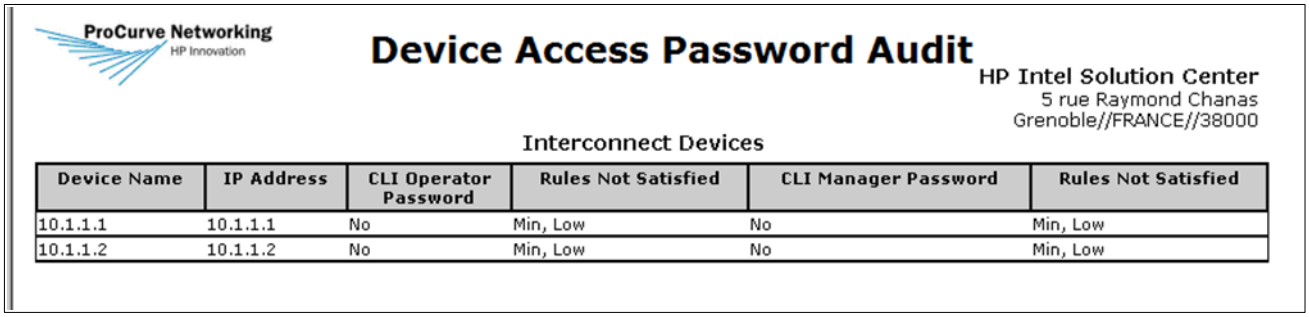
4. Then specify the Password Policy. Enter a Minimum Length, a Maximum Length, and the number of Lowercase letters:



5. Choose the fields to verify: here, CLI Operator Password and CLI Manager Password:



6. Click on Finish to generate the report:



ProCurve Networking
HP Innovation

Device Access Password Audit

HP Intel Solution Center
5 rue Raymond Chanas
Grenoble//FRANCE//38000

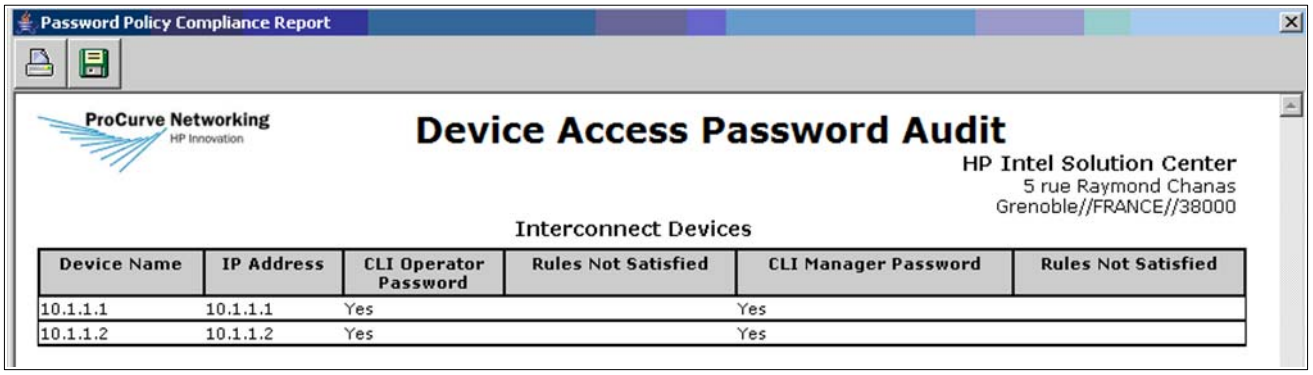
Interconnect Devices

Device Name	IP Address	CLI Operator Password	Rules Not Satisfied	CLI Manager Password	Rules Not Satisfied
10.1.1.1	10.1.1.1	No	Min, Low	No	Min, Low
10.1.1.2	10.1.1.2	No	Min, Low	No	Min, Low

In this case, the Rules Not Satisfied columns show that the passwords on the switch are not compliant.

7. Now modify the passwords on the switch using the Communication Parameters in PCM wizard: Highlight the switch in the Devices List, then select the Communication Parameters in PCM icon and change the passwords so their parameters are compliant.

8. Generate the report again. This time the passwords are in compliance with the rules:



Password Policy Compliance Report

ProCurve Networking
HP Innovation

Device Access Password Audit

HP Intel Solution Center
5 rue Raymond Chanas
Grenoble//FRANCE//38000

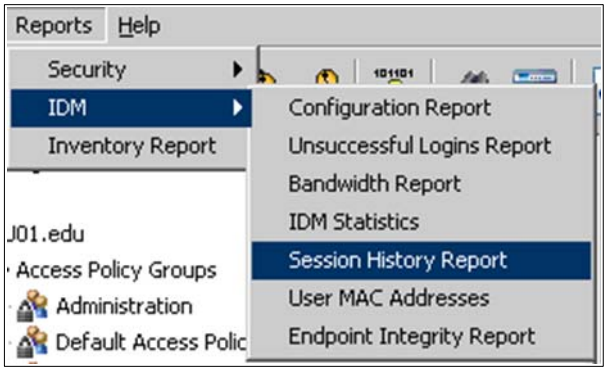
Interconnect Devices

Device Name	IP Address	CLI Operator Password	Rules Not Satisfied	CLI Manager Password	Rules Not Satisfied
10.1.1.1	10.1.1.1	Yes		Yes	
10.1.1.2	10.1.1.2	Yes		Yes	

4.5 Create a report of IDM user session history

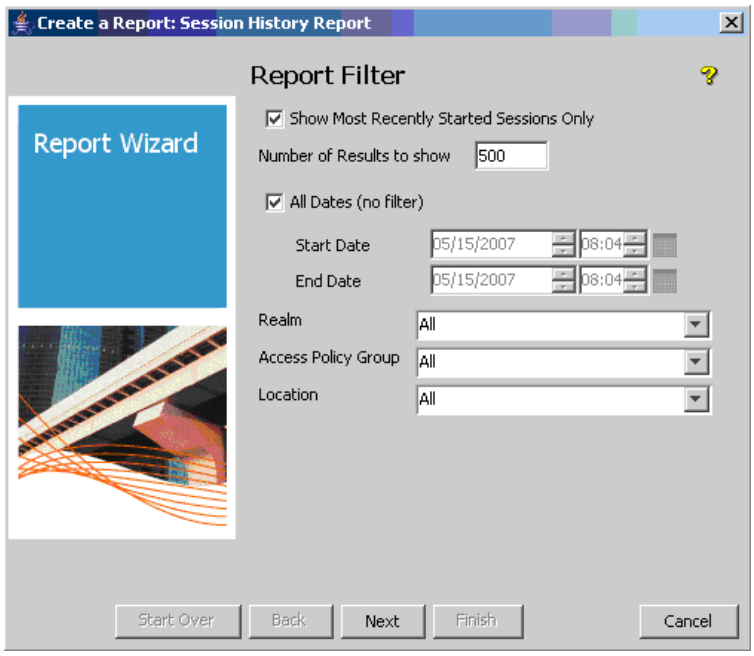
The IDM Session History Report shows information about the sessions of authenticated users. To generate an IDM user session history:

1. Open Reports > IDM > Session History Report:

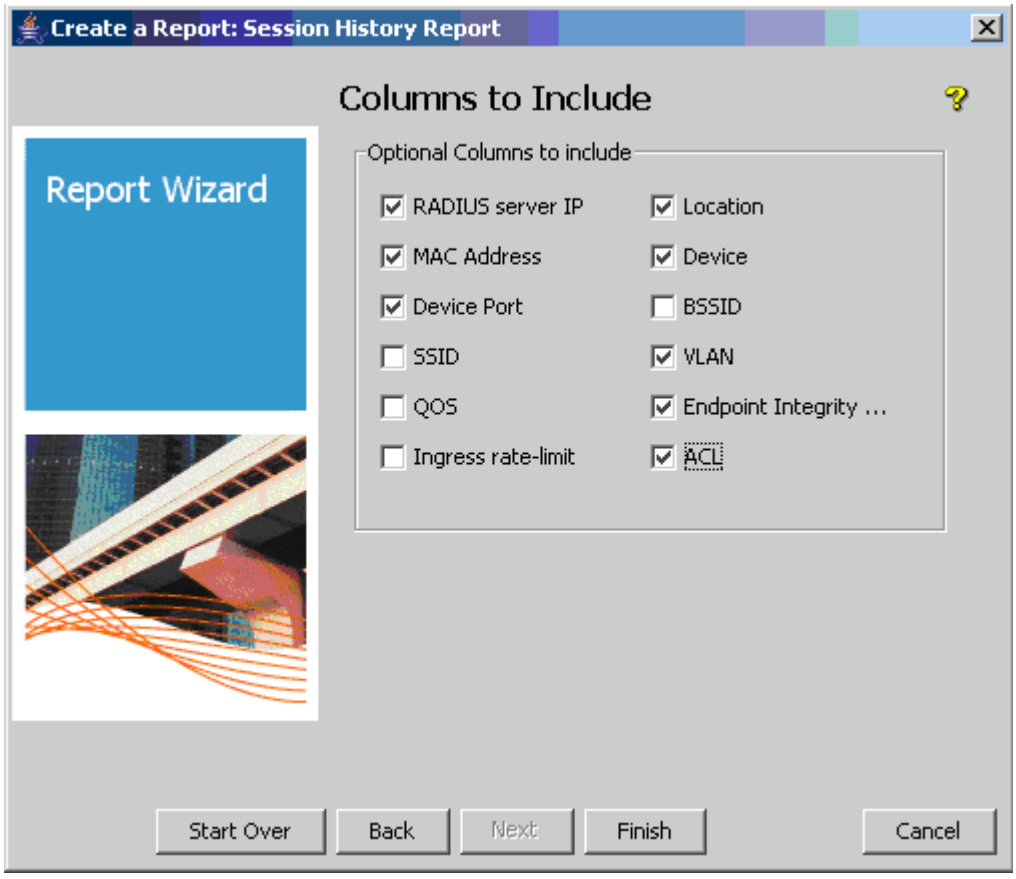


This launches the Report Wizard.

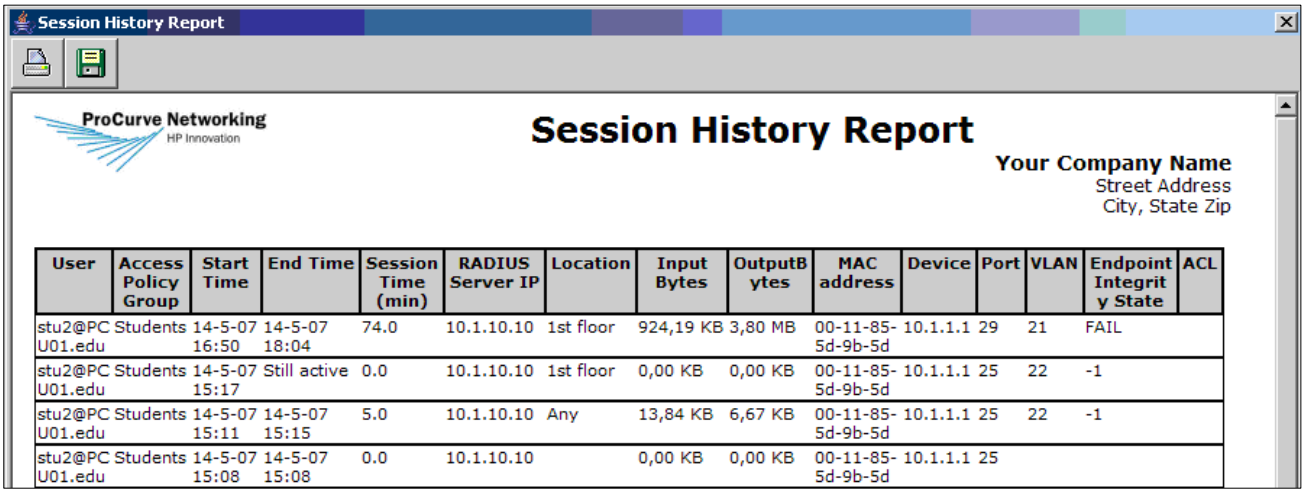
2. On the Report Filter window, choose Show Most Recently Started Sessions only, and All Dates:



3. Choose the columns that you want to see in the reports: for example, Radius Server IP, MAC Address, Device Port, Location, Device, VLAN, Endpoint Integrity and ACL:



4. Click Finish to generate the report. It gives you detailed info about a user session, including:
   - Start and end time, duration
   - User location (device, port) and VLAN
   - Input and output bytes, which can be useful for billing purposes
   - MAC address of the client, and the endpoint integrity state



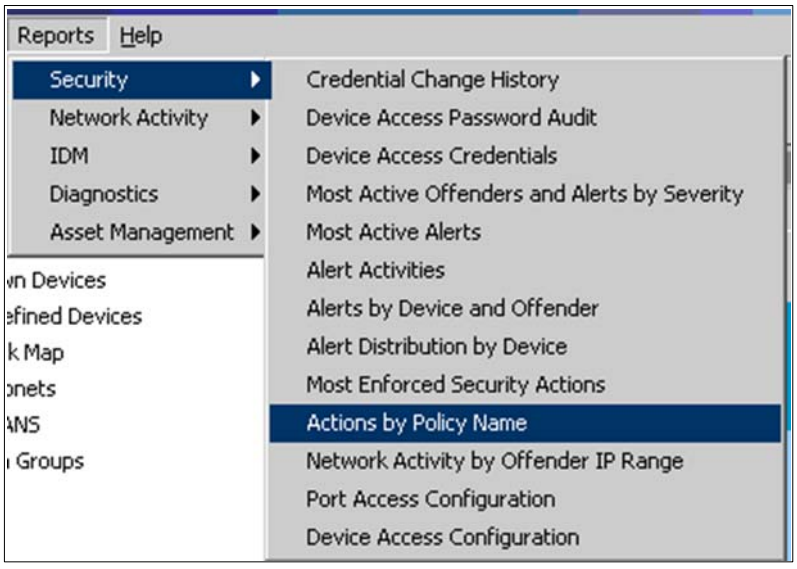
User	Access Policy Group	Start Time	End Time	Session Time (min)	RADIUS Server IP	Location	Input Bytes	OutputBytes	MAC address	Device	Port	VLAN	Endpoint Integrity State	ACL
stu2@PCU01.edu	Students	14-5-07 16:50	14-5-07 18:04	74.0	10.1.10.10	1st floor	924,19 KB	3,80 MB	00-11-85-5d-9b-5d	10.1.1.1	29	21	FAIL	
stu2@PCU01.edu	Students	14-5-07 15:17	Still active	0.0	10.1.10.10	1st floor	0,00 KB	0,00 KB	00-11-85-5d-9b-5d	10.1.1.1	25	22	-1	
stu2@PCU01.edu	Students	14-5-07 15:11	14-5-07 15:15	5.0	10.1.10.10	Any	13,84 KB	6,67 KB	00-11-85-5d-9b-5d	10.1.1.1	25	22	-1	
stu2@PCU01.edu	Students	14-5-07 15:08	14-5-07 15:08	0.0	10.1.10.10		0,00 KB	0,00 KB	00-11-85-5d-9b-5d	10.1.1.1	25			

4.6 Confirm network immunity with a report on actions by policy name

The Actions by Policy Name report shows the results of network actions taken to enforce policies. It gives an indication of your network's immunity.

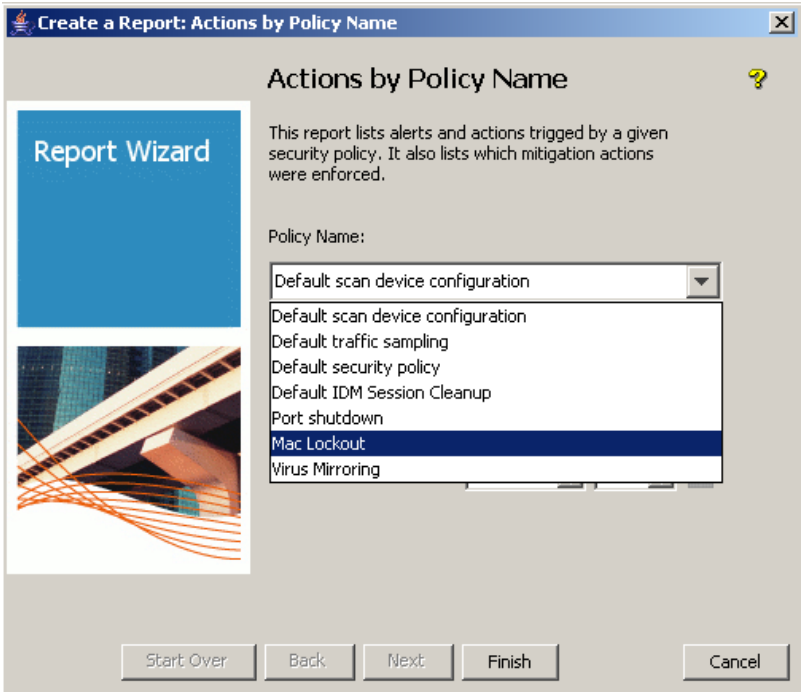
To generate the report:

1. Open Reports > Security > Actions by Policy Name:

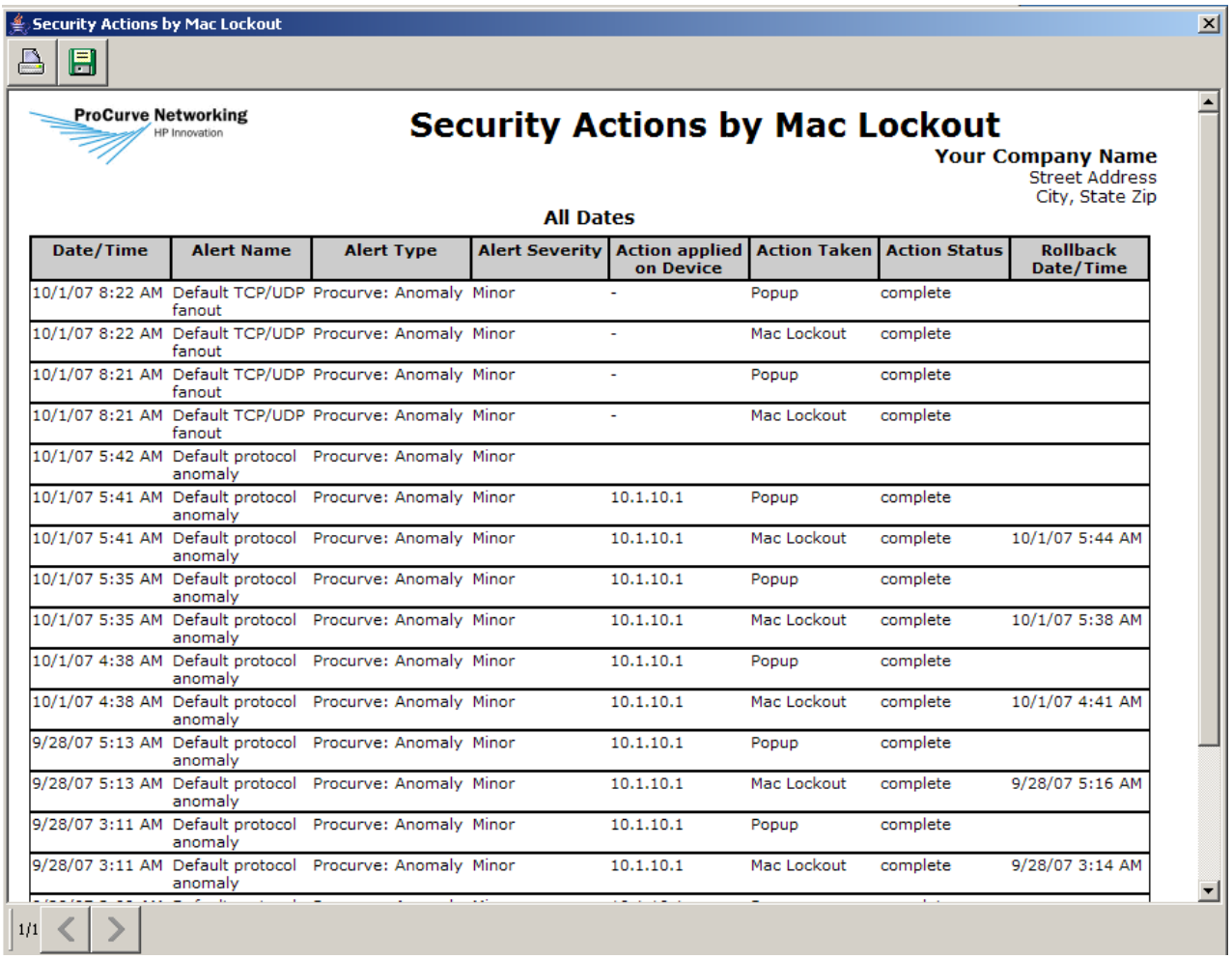


This launches the Report Wizard.

2. In the Actions by Policy name window, choose the Policy for which you want to generate the report, for example, MAC lockout:



3. Click Finish to view the results. You see the different actions associated with each application of the policy, the device on which they occurred, their status, and whether the policy was rolled back:



Security Actions by Mac Lockout

ProCurve Networking
HP Innovation

Security Actions by Mac Lockout

Your Company Name
Street Address
City, State Zip

All Dates

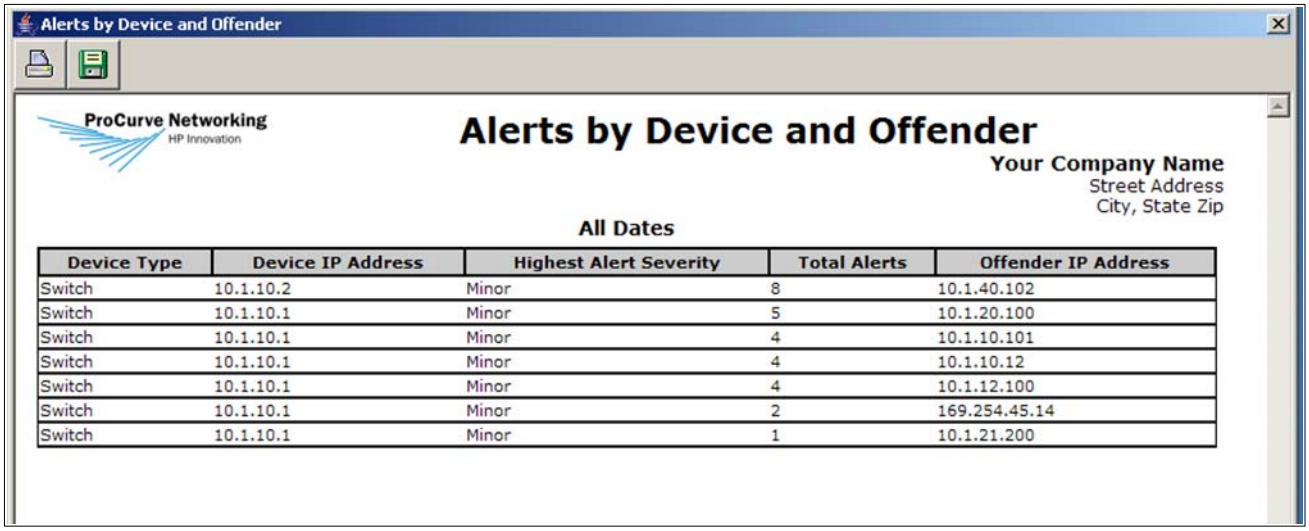
Date/Time	Alert Name	Alert Type	Alert Severity	Action applied on Device	Action Taken	Action Status	Rollback Date/Time
10/1/07 8:22 AM	Default TCP/UDP fanout	Procurve: Anomaly	Minor	-	Popup	complete	
10/1/07 8:22 AM	Default TCP/UDP fanout	Procurve: Anomaly	Minor	-	Mac Lockout	complete	
10/1/07 8:21 AM	Default TCP/UDP fanout	Procurve: Anomaly	Minor	-	Popup	complete	
10/1/07 8:21 AM	Default TCP/UDP fanout	Procurve: Anomaly	Minor	-	Mac Lockout	complete	
10/1/07 5:42 AM	Default protocol anomaly	Procurve: Anomaly	Minor				
10/1/07 5:41 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Popup	complete	
10/1/07 5:41 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Mac Lockout	complete	10/1/07 5:44 AM
10/1/07 5:35 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Popup	complete	
10/1/07 5:35 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Mac Lockout	complete	10/1/07 5:38 AM
10/1/07 4:38 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Popup	complete	
10/1/07 4:38 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Mac Lockout	complete	10/1/07 4:41 AM
9/28/07 5:13 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Popup	complete	
9/28/07 5:13 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Mac Lockout	complete	9/28/07 5:16 AM
9/28/07 3:11 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Popup	complete	
9/28/07 3:11 AM	Default protocol anomaly	Procurve: Anomaly	Minor	10.1.10.1	Mac Lockout	complete	9/28/07 3:14 AM

1/1

4.7 Confirm network immunity with reports on offenders

There are two types of reports about offenders in Reports > Security:

- **Alerts by Device and Offender**: Shows for each switch the list of offenders, classified by the number of alerts they generated. For example:



Alerts by Device and Offender

ProCurve Networking
HP Innovation

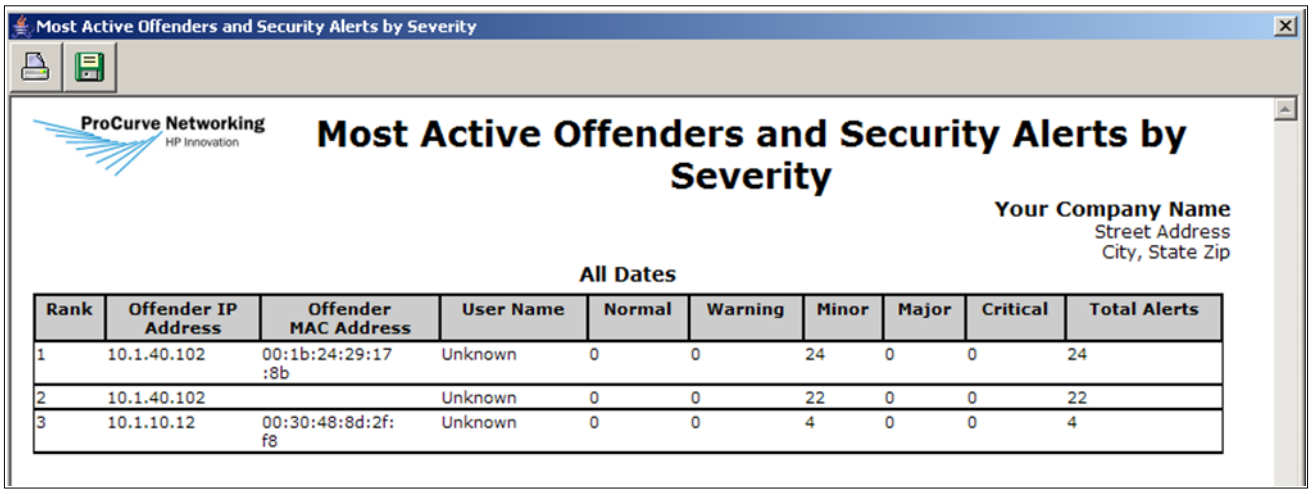
Alerts by Device and Offender

Your Company Name
Street Address
City, State Zip

All Dates

Device Type	Device IP Address	Highest Alert Severity	Total Alerts	Offender IP Address
Switch	10.1.10.2	Minor	8	10.1.40.102
Switch	10.1.10.1	Minor	5	10.1.20.100
Switch	10.1.10.1	Minor	4	10.1.10.101
Switch	10.1.10.1	Minor	4	10.1.10.12
Switch	10.1.10.1	Minor	4	10.1.12.100
Switch	10.1.10.1	Minor	2	169.254.45.14
Switch	10.1.10.1	Minor	1	10.1.21.200

- **Most Active Offenders and Security Alerts by Severity**: This gives you a list of offenders, showing their IP and MAC addresses and Usernames. This report gives you the ability to correlate information from IDM and NIM. For example:



Rank	Offender IP Address	Offender MAC Address	User Name	Normal	Warning	Minor	Major	Critical	Total Alerts
1	10.1.40.102	00:1b:24:29:17 :8b	Unknown	0	0	24	0	0	24
2	10.1.40.102		Unknown	0	0	22	0	0	22
3	10.1.10.12	00:30:48:8d:2f: f8	Unknown	0	0	4	0	0	4

5. Reference documents

This concludes the procedures for using ProCurve Manager, Identity-Driven Manager, and Network Immunity Manager to generate reports 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+, IDM, and NIM manuals:
  http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm
  http://www.hp.com/rnd/support/manuals/IDM.htm
  http://www.hp.com/rnd/support/manuals/NIM.htm

For further information, please visit www.procurve.eu

4AA2-1970EEE, July 2008