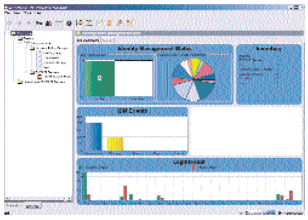
ProCurve Networking
HP Innovation

Identity Driven Manager 1.0

User's Guide



The safe and simple way to manage network policies

ProCurve
Identity Driven Manager

Software Release 1.0

User's Guide

Publication Number

5990-8851
November, 2004

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation. Cisco® is a trademark of Cisco Systems, Inc.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
http://www.hp.com/go/hpprocurve

Contents

1

About ProCurve Identity Driven Manager

Chapter Contents

Introduction

Network usage has skyrocketed with the expansion of the Internet, wireless, and convergence technologies. This increases the burden on network managers working to control network usage. Also, the complexity of large networks makes it difficult to control network access and usage by individual users.

ProCurve Identity Driven Manager (IDM) is an add-on module to the ProCurve Manager plus (PCM+) application that extends the functionality of PCM+ to include authorization control features for edge devices in networks using RADIUS servers and Web-Authentication, MAC-Authentication, or 802.1x security protocols.

Using IDM simplifies user access configuration by automatically discovering Microsoft IAS RADIUS Servers, Realms, and users. You can use IDM to monitor users on the network, and to create and assign "access policies" that work to dynamically configure edge switches and manage network resources available to individual users. Using IDM, access rights, quality of service (QoS), and VLAN enrollment are associated with a user and applied at the point of entry or "edge" of the network.

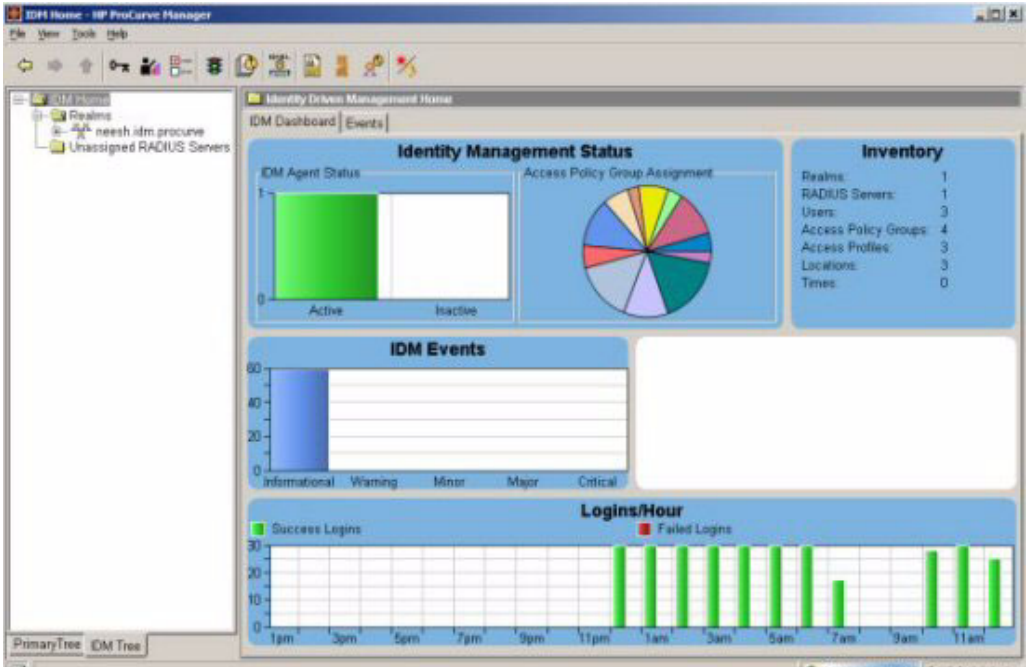


Figure 1-1. ProCurve Identity Driven Manager, Client Interface

Why IDM?

Today, access control using a RADIUS system and ProCurve devices (switches or wireless access points) is typically made up of several steps.

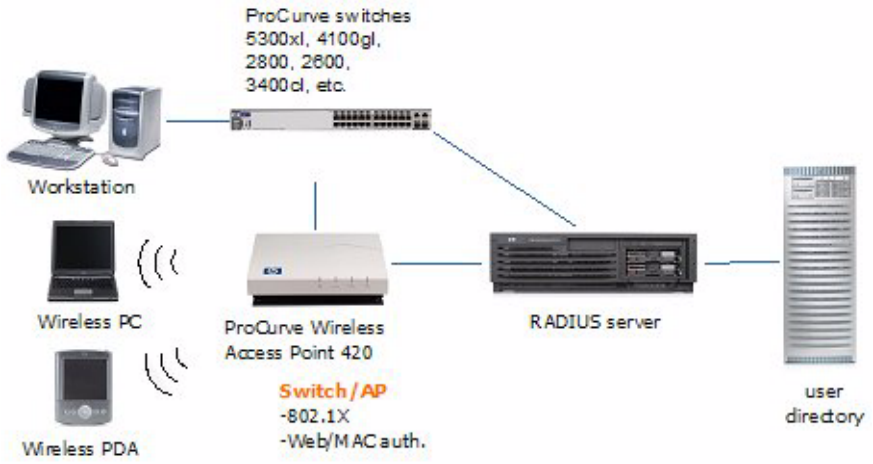


Figure 1-2. Current Access Control process

1. A client (user) attempts to connect to the network.
2. The edge device recognizes a connection state change, and requests identifying information about the client. This can include MAC address, username and password, or more complex information.
3. The switch forwards an access request, including the client information to the authentication server (RADIUS).
4. The RADIUS server validates the user's identity in the user directory, which can be an Active Directory, database or flat file. Based on the validation result received from the user directory, the authentication server returns an accept or deny response to the switch.
5. If the user is authenticated, the ProCurve device grants the user access to the network. If the user is not authenticated, access is denied.

For networks using IDM, access control is enhanced to include authorization parameters along with the authentication response. IDM enhances existing network security by adding network authorization information, with access and resource usage parameters, to the existing authentication process. Using IDM you can assign access rights and connection attributes at the network switch, with dynamic configuration based on the time, place, and client that is generating the access request.

When using IDM, the authentication process proceeds as described in the first three steps, but from that point the process changes as follows:

4. The RADIUS server validates the user's identity in the user directory. Based on the validation result received from the user directory, the authentication server returns an accept or deny response to the switch. If the user is accepted (authenticated), the IDM Agent on the RADIUS server processes the user information. IDM then inserts the network access rights configured for the user into the Authentication response sent to the switch.

5. If the user is authenticated, the switch grants the user access to the network. The (IDM) authorization information included in the authentication response is used to configure VLAN access, QoS, and Bandwidth parameters for the user, based on time and location of the user's login.

   If the user is authenticated by the RADIUS server, but IDM's authorization data indicates that the user is attempting to access the network at the wrong time, or from the wrong location or system, the user's access request is denied by IDM.

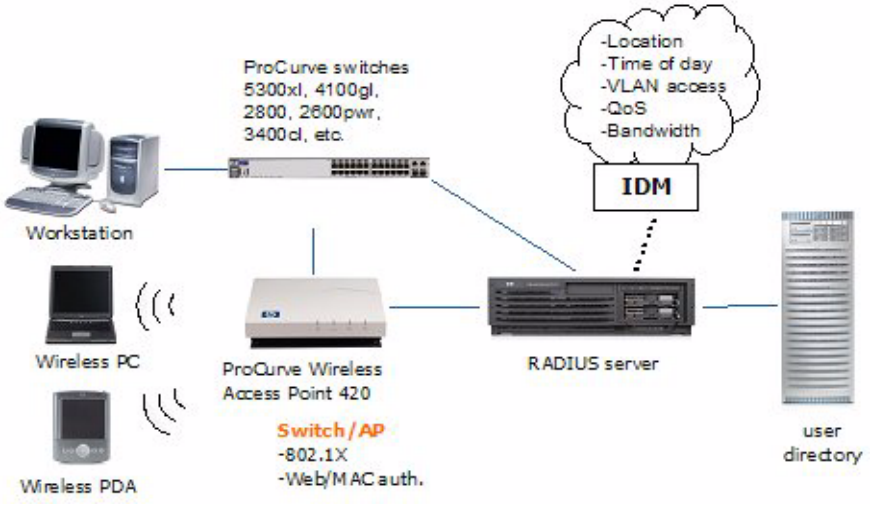


Figure 1-3. Access Control using IDM

If a user is authenticated in RADIUS, but is unknown to IDM, IDM will not override RADIUS authentication and default switch settings, unless you configure it to do so. You can create a "guest" profile in IDM to provide limited access for unknown users.

IDM Architecture

In IDM, when a user attempts to connect to the network through an edge switch, the user is authenticated via the RADIUS Server and user directory. Then, IDM is used to return the user's "access profile" along with the authentication response from RADIUS to the switch. The IDM information is used to dynamically configure the edge switch to provide the appropriate authorizations to the user, that is, what VLAN the user can access, and what resources (QoS, bandwidth) the user gets.

The following figure illustrates the IDM architecture and how it fits in with RADIUS.

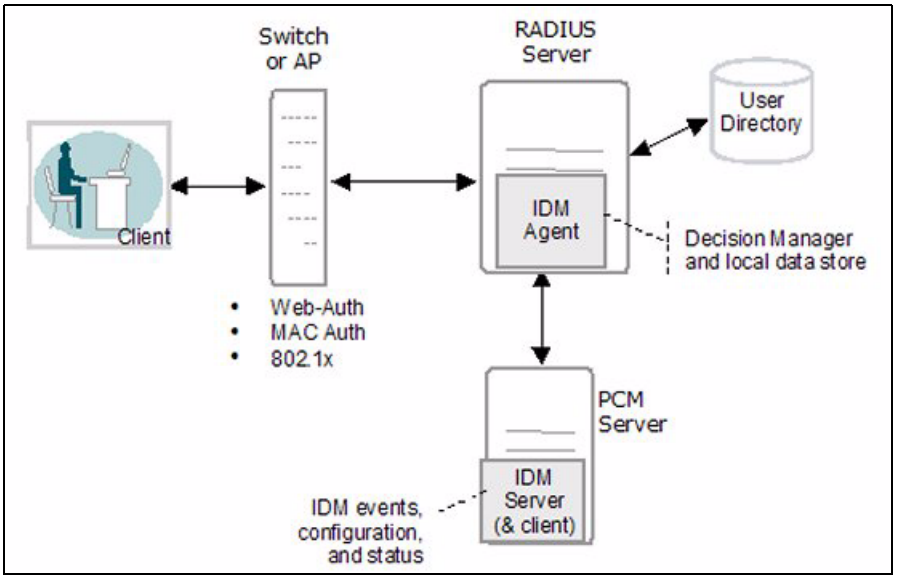


Figure 1-4. IDM Architecture

IDM consists of an IDM Agent that is co-resident on the RADIUS server, and an IDM Server that is co-resident with PCM+. Configuration and access management tasks are handled via the IDM GUI on the PCM+ management workstation.

The IDM agent includes:

- A RADIUS interface that captures user authentication information from the RADIUS server and passes the applicable user data (username, location, time of request) to the IDM Decision Manager. The interface also passes user access parameters from IDM to the RADIUS server.

- A Decision Manager that receives the user data and checks it against user data in the local IDM data store. Based on the parameters defined in the data store for the user data received, the Decision Manager outputs access parameters for VLAN, QoS, and bandwidth to the RADIUS interface component.
- A Local Data Store that contains information on Users and the Access Policy Groups to which the user belongs. The Access Policy Group defines the rules that determine the user's access rights.

The IDM Server provides configuration and monitoring of Identity Driven Manager. It operates as an add-on module to PCM+, using the PCM model database to store IDM data, and a Windows GUI (client) to provide access to configuration and monitoring tools for IDM.

You use the IDM GUI to monitor IDM Agent status and users logged into the network, and to manage IDM configuration, including:

- Defining access parameters for the network, such as locations, times, and access profiles.
- Creating access profiles that define the resources (VLAN, QoS, bandwidth) given to users in an Access Policy Group.
- Creating Access Policy Groups with rules (access policies) that will be assigned to users in that Group.
- Assigning users to Access Policy Groups.
- Deploying IDM configuration data to the IDM Agent on the RADIUS server.

Terminology

Authentication The process of proving the user's identity. In networks this involves the use of usernames and passwords, network cards (smartcards, token cards, etc.), and a device's MAC address to determine who and/or what the "user" is.

Authentication Server Authentication servers are responsible for granting or denying access to the network. Also referred to as RADIUS servers because most current authentication servers implement the RADIUS protocol.

Authorization The process that determines what an authenticated user can do. It establishes what network resources the user is, or is not permitted to use.

Bandwidth Amount of network resources available. Generally used to define the amount of network resources a specific user can consume at any given time. Also referred to as rate-limiting.

Client An end-node device such as a management station, workstation, or mobile PC attempting to access the network. Clients are linked to the switch through a point-to-point LAN link, either wired or wireless.

Edge Device A network device (switch or wireless access point) that connects the user to the rest of the network. The edge devices can be engaged in the process of granting user access and assigning a user's access rights and restrictions.

IDM Agent The IDM Agent resides on the RADIUS server. It inspects incoming authentication requests, and inserts appropriate authorization information (IDM Access Profiles) into the outgoing authentication reply.

QoS Quality of Service, relates to the priority given to outbound traffic sent from the user to the rest of the network.

RADIUS Remote Authentication Dial-in User Service, (though it also applies to authentication service in non-dial-in environments)

RADIUS Server A server running the RADIUS application on your network. This server receives user connection requests from the switch, authenticates users, and then returns all necessary information to the edge device.

Realm A Realm is similar to an Active Directory Domain, but it works across non-Windows (Linux, etc.) systems. Generally specified in User-name as "user@realm."

VLAN A port-based Virtual LAN configured on the switch. When the client connection terminates, the port drops its membership in the VLAN.

IDM Specifications

Supported Devices

ProCurve Identity Driven Manager (IDM) supports authorization control functions on the following ProCurve devices*:

- ProCurve Switches:
  5300xl Series (5304, 5308, 5348, 5372)
  3400cl Series (3424, 3448)
  4100gl Series (4104, 4108, 4124)
  2800 Series (2824, 2848)
  2600 Series (2650, 2626, and 6108)
  2512, 2524
- ProCurve Wireless Access Points (520wl, 420)

* Not all devices support all features of IDM. Refer to Appendix A for details.

Operating Requirements

The system requirements for IDM (Server and Client installation) are:

- Minimum Processor: 2.0 GHz Intel Pentium, or equivalent
- Recommended Processor: 3.0 GHz Intel Pentium, or equivalent
- Minimum Memory: 1 GB RAM
- Recommended Memory: 2 GB RAM
- Disk Space: 500 MB free hard disk space minimum.
- Implementation of Microsoft's Internet Authentication Service, RADIUS authentication server on Windows 2003 Server (Enterprise or Standard Edition). The IDM agent will be installed on this system.
- Supported Operating Systems for PCM+ and IDM Remote Client:
  - MS Windows XP Pro (Service Pack 1 or better)
  - MS Windows 2000
    (Server, Advanced Server, or Pro with Service Pack 4 or better)
  - MS Windows 2003 (Server or Enterprise Edition)
- ProCurve Manager Plus software must be installed for IDM to operate. The IDM software cannot be installed as a separate component.

Additional processing power and additional disk space may be required for larger networks.

Additional Requirements

- Implementation of an access control method, using either MAC-auth, Web-auth, or an 802.1x supplicant application.

  For assistance with implementation of RADIUS and access control methods for use with ProCurve switches, refer to the *Access Security Guide* that came with your switch. All ProCurve Switch manuals can also be downloaded from the ProCurve web site.

  For assistance with using RADIUS and 802.1x access control methods, contact the ProCurve Elite Partner nearest you that can provide ProCurve Access Control Security solutions. You can find ProCurve Direct Elite partners on the web at:

  http://hp.via.infonow.net/locator/us_partner/index.jsp

- If you plan to restrict user access to specific network segments, you will need to configure VLANs within your network. For information on using VLANs, refer to the *ProCurve Manager Network Administrator's Guide*, or the configuration guides that came with your switch.

Registering Your IDM Software

The ProCurve Manager installation CD includes a fully operable version of the PCM application, and a 30 day trial version of the PCM+ application and the IDM application. Until you have registered your IDM application, an Expiring License warning will be displayed each time you log in, similar to the following.

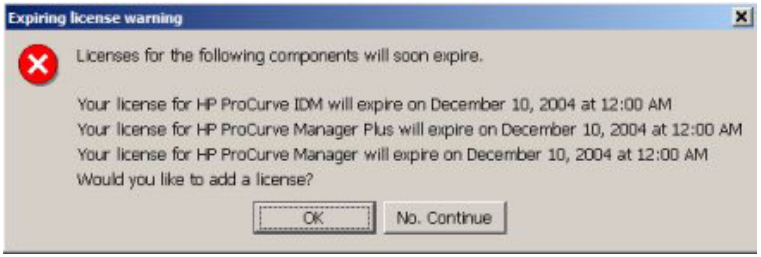


Figure 1-5. ProCurve Expiring License warning dialogue

Click **No, Continue** to close the dialogue and just start the program. Click **OK** to launch the Licensing administration screen.

NOTE: You must first purchase a copy of ProCurve Identity Driven Manager from your networking reseller to get the Registration ID. *You do not need to re-install the software from the purchased CD, but you need the Registration ID from that CD to complete the registration process.*

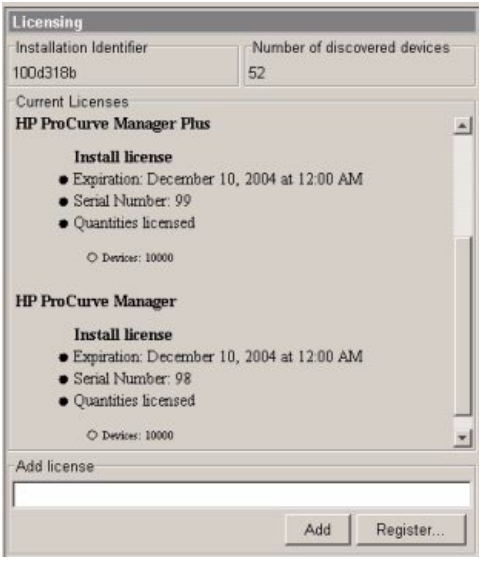


Figure 2. ProCurve License Administration dialogue

You can also get to this screen from the Preferences window which can be accessed from the PCM Tools menu or by clicking on the Preferences icon in the tool bar. 

To register the ProCurve Manager Plus software:

1. Make a note of the Installation Identifier in the upper left corner of the screen and of the Registration ID that is printed on the front of the ProCurve Manager Plus CD.

   Note: If you are attempting to register ProCurve IDM from the CD that came in the box with your ProCurve networking device, you must first purchase a copy of ProCurve Identity Driven Manager software from your networking reseller to get the Registration ID.

2. Click **Register** to go to the ProCurve Registration Web site.

3. Follow the instructions on the web site to complete the registration. For additional details, you can refer to the *ProCurve Manager Getting Started Guide*, under "Registering Your ProCurve Manager Software.

Learning to Use ProCurve IDM

The following information is available for learning to use ProCurve Identity Driven Manager (IDM):

- This User's Guide—helps you become familiar with using the application tools for access control management.
- Online help information—provides information through Help buttons in the application GUI that provide context-sensitive help, and a table of contents with hypertext links to additional procedures and reference information.
- *ProCurve Manager*, *Getting Started Guide*—provides details on installing the application and licensing, and an overview of ProCurve Manager functionality.
- For additional information on configuring your network, refer to the documentation that came with your switch.

Getting ProCurve Documentation From the Web

1. Go to the Procurve website at http://www.hp.com/go/hpprocurve.
2. Click on **Technical Support**.
3. Click on **Product manuals**.
4. Click on the product for which you want to view or download a manual.

ProCurve Support

Product support is available on the Web at: http://www.hp.com/go/hpprocurve Click on **Technical Support**. The information available at this site includes:

- Product Manuals
- Software updates
- Frequently asked questions (FAQs)
- Links to Additional Support information.

You can also call your HP Authorized Dealer or the nearest HP Sales and Support Office, or contact the ProCurve Elite Partner nearest you for information on ProCurve Access Control Security solutions.

You can find ProCurve Elite partners on the web at:
http://hp.via.infonow.net/locator/us_partner/index.jsp

2

Getting Started

Chapter Contents

Before You Begin

If you have not already done so, please review the list of supported devices and operating requirements under “IDM Specifications” on page 1-8.

If you intend to restrict user access to specific areas of the network using VLANs, make sure you have set up your network for use of VLANs. For details on configuring VLANs, refer to the *ProCurve Manager Network Administrator’s Guide*, or the *Advanced Traffic Management Guide* for your ProCurve switch

Installing the IDM Agent

The IDM application components are installed on your system when you select the IDM option from the PCM+ software CD. To install the IDM Agent on a RADIUS server:

1. If the PCM software is not on the same system as your RADIUS server, you need to configure "Client/Server" access permissions on the PCM server to allow the RADIUS server to communicate with IDM. This is done by adding the IP address of the RADIUS server to the **access.txt** file on the PCM server. For details, refer to the *ProCurve Manager Getting Started Guide*, under "Configuring Client/Server Access Permissions."
2. Open a Web browser window on the RADIUS server and for the URL, type in the IP address of the PCM server computer, followed by a colon and the port ID 8040.
   For example, if the IP address of the PCM server is 10.15.20.25, then on the RADIUS server, enter **http://10.15.20.25:8040** on the web browser address line.
3. In the install scripts page that appears, select the IDM Agent to download it to the RADIUS server system.
4. Run the Install.exe that is downloaded to the RADIUS server. The Install Wizard guides you through the installation process. During installation you will be prompted to enter the IP Address of the IDM Server, which is the same as the PCM Server.

You cannot install the IDM Agent on a system without the RADIUS server. Also, if the IP address of the RADIUS server is not in the access.txt file on the PCM server, you will get an alert message during the IDM Agent install.

Once installed the IDM Agent begins collecting User, Realm, and RADIUS data.

The IDM Client is included with the PCM+ software. To install a remote PCM/ IDM Client, download the PCM Client to a remote PC using the same process as for installing the IDM Agent, just select the PCM Client option from the PCM server. For details, see the *ProCurve Manager Getting Started Guide*.

Using the IDM Auto-Discover Feature

You can manually configure the RADIUS server, Realms, and Users in IDM, or you can let IDM do the hard work for you. Just install the IDM Agent on the system with the RADIUS Server, then let it run to collect the information as users log into the network. Even after you begin creating configurations in IDM, it will continue to collect information on new users, and Realms and pass that information to the IDM server.

If you are using multiple RADIUS servers, you need to install an IDM Agent on each of the servers. The IDM Agent collects information only on the system where it is installed. The IDM client can display information for all RADIUS servers where the IDM Agent is installed.

When you start the IDM Client and expand the navigation tree in the IDM Home tab, you will see any discovered or defined Realms found on the RADIUS server, along with the IP Address for the RADIUS Server(s).

IDM Configuration Process Overview

To configure IDM to provide access control on your network, first let IDM run long enough to "discover" the Realms, RADIUS servers, and users on your network. Once IDM has performed these tasks for you, your configuration process would be as follows:

1. If you intend to use them, define "locations" from which users will access the network. A location may relate to port-based VLANS, or to all ports on a device. (See page 3-4)
2. If you intend to use them, define "times" at which users are allowed or denied access. This can be by day, week or even hour. (See page 3-9)
3. If you intend to restrict a user access to specific systems, you need to set the User profile to include the MAC address for each system that the user is allowed to login on. (See page 3-28)
4. Create the Access Profiles, to set the VLAN, QoS, and rate-limits (band-width) that are applied to users in an Access Policy Group. (See page 3-13)

5. Create an Access Policy Group, with rules containing the Location, Time, System, and Access Profile that is applied to users when they login. (See page 3-16)
6. Assign Users to the appropriate Access Policy Group. (See page 3-20)
7. Deploy the configuration policies to the IDM Agent on the RADIUS server. (See page 3-22)

IDM Usage Strategies

You can use IDM to simply monitor user activity on the network, or to apply user authentication rules to improve network security and performance. The following table identifies the IDM configuration for various deployment and usage strategies for IDM.

Authentication	Authorization			Strategy Description
	VLAN	QoS	Rate-Limit	
				Monitor and report user activity.
x				Enhance normal RADIUS authentication with Location, Time, and System rules
x	x			Provide rudimentary VLAN segregation (Unknown Users, Guests, Visitors, Contractors)
x	x			Provide complete VLAN placement for all Users
x		x	x	Provide QoS and Rate-limits per User
x	x	x	x	VLAN, QoS, and Rate-limits for all users, based on Location, Time, and System

Table 1. IDM Deployment and Usage strategies

Understanding the IDM Model

The first thing to understand, is that IDM works within the general concept of ‘domains’ or ‘realms’. Basically, realms are very large organizational units; every user belongs to one, and only one, realm. While it is possible to have multiple realms, most organizations have only one, for example, hp.com or csuchico.edu.

In the IDM GUI, the top level of the navigation tree is the Realm, with all other information for APGs, RADIUS Servers, and Users arranged beneath. Users are linked to the Realm to which they belong, and the Access Policy Group to which they are assigned.

The fundamental configuration model of IDM involves Users and Groups. Every User belongs to a Group – in IDM these are called Access Policy Groups (APGs). Each APG has an Access Policy defined for it, which governs the access rights that are applied to its Users as they enter the network.

IDM GUI Overview

To use the IDM client, launch the PCM Client on your PC. Select the ProCurve Manager option from the Windows Program menu to launch the PCM Client.

The PCM Client will start up and the Login dialogue is launched.

Figure 2-1. PCM Client Login dialogue.

If you did not enter a Username or Password during install, type in the default Username, *Administrator*, then Click Login to complete the login and startup.

For additional information on using the PCM Client, refer to the *ProCurve Manager Network Administrator's Guide*.

Select the IDM Tree tab at the bottom left of the PCM window to display the IDM Home window.

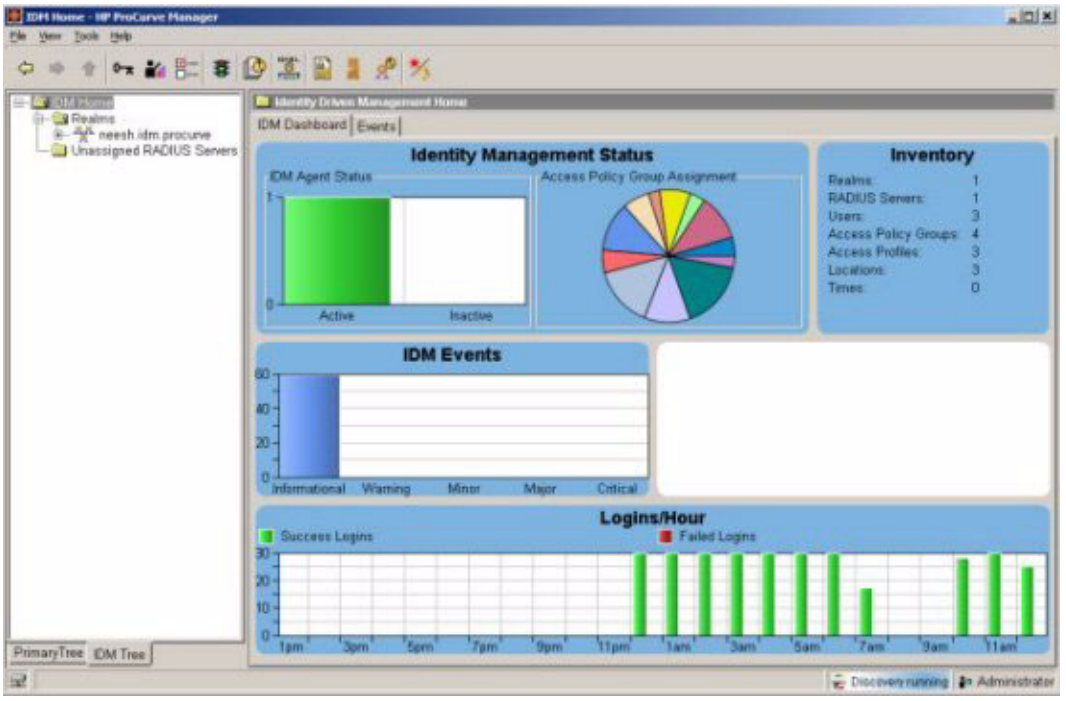


Figure 2-2. IDM Home Window

The IDM Home display provides a quick view of IDM status in the IDM Dashboard tab, along with a navigation tree and access to menu and toolbar functions. You can resize the entire window, and/or resize the panes (sub-windows) within the IDM Home window frame.

NOTE: If the dashboard shows the IDM Agent Status as inactive, and the Inventory and Logins panes show no data, check the PCM Events tab for the following: "PCM remote client authentication failure: <ip address>"
Check to make sure the **access.txt** file on the PCM (IDM) Server system includes an IP address entry for each RADIUS server where the IDM Agent is installed. See “Installing the IDM Agent” on page 2-2 for details.

IDM Dashboard

The IDM Dashboard tab (window) contains four separate panels, described below.

Identity Management Status: The IDM Agent Status pane uses a color-coded histogram to indicate the number of currently active (green) and inactive (red) IDM Agents. Hovering with the mouse pointer over the bar displays the specific number.

The Users per Access Policy Group pane uses a pie-chart to indicate the percentage users currently assigned to various APGs. You can hover with the mouse pointer over the segment to display the APG name and number of assigned users.

Inventory: The Inventory panel lists the current number of Realms, RADIUS Servers, Users, Access Policy Groups, Access Profiles, Locations, and Times that are defined in IDM.

IDM Events: The IDM Events panel provides a summary of IDM Events by severity type. Hovering with the mouse pointer over the event type displays the total number of events of that type currently in the log. Clicking on the Events panel will display the IDM Events tab, with a detailed event listing.

Logins/Hour: The Logins panel uses a color-coded histogram to provide a summary of the successful and unsuccessful user logins during each hour. The panel has a 24-hour display that is continuously updated. Hovering with the mouse pointer over the bar for a specific time period displays the specific number of logins.

Using the Navigation Tree

The navigation tree in the left pane of the IDM window provides access to IDM features using the standard Windows file navigation system. The IDM tree is organized as follows:

Realms: The top level of the tree lists each of the Realms that have been discovered by an IDM Agent or defined manually. Clicking on the Realms node in the tree displays the Realms list in the right panel of the window. Expanding the node displays each Realm name in the tree, and Unassigned RADIUS Servers if they exist.

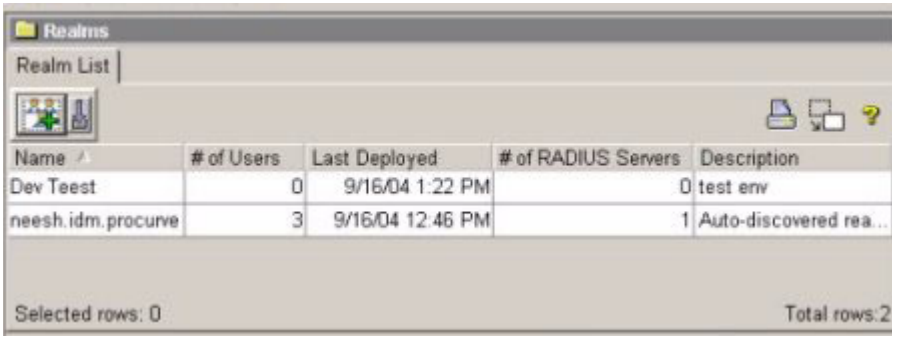


Figure 2-3. Realms List tab

Clicking on the individual realm name in the tree displays the Realm Properties tab in the right panel.

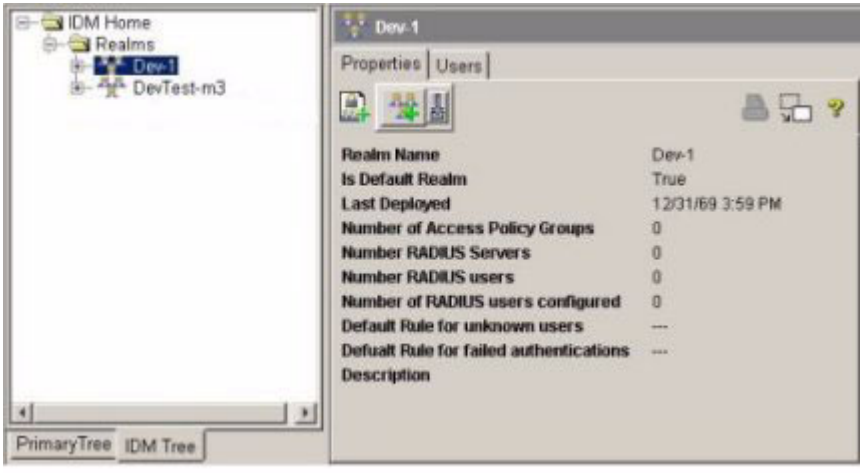


Figure 2-4. Realm Properties tab

Click the Users tab, underneath the realm Properties tab, to view a list of users in the Realm that were discovered by the IDM Agent, or defined manually.

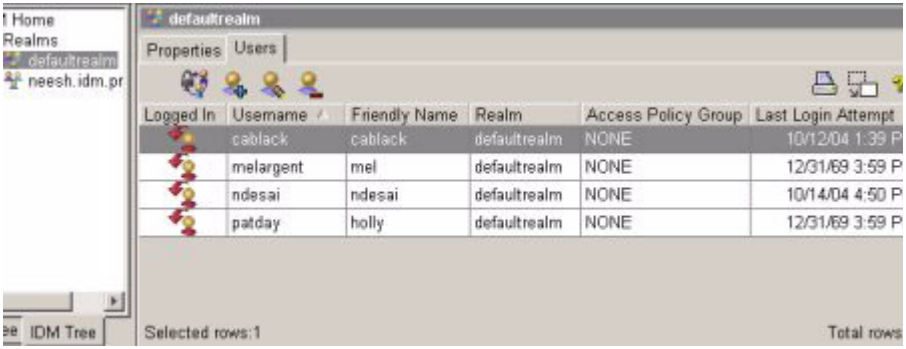


Figure 2-5. Realm Users tab

NOTE: There will be no auto-discovered Realm, Users, or RADIUS server until a user has logged in to the network.

Expanding the Realm node in the tree will display the Access Policy Groups and RADIUS server nodes for the Realm.

Access Policy Groups: Click the Access Policy Group node to display the Access Policy Groups tab with a list of currently configured groups. You can also expand the node to view the APGs in the tree.

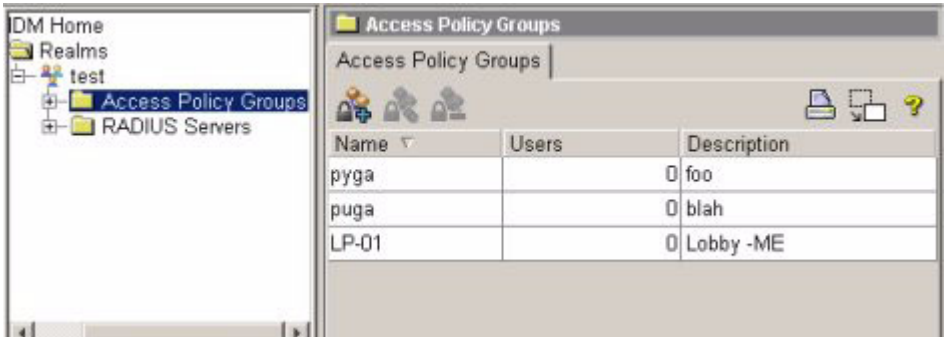


Figure 2-6. Access Policy Groups tab

Click the individual group node in the tree to display the properties.

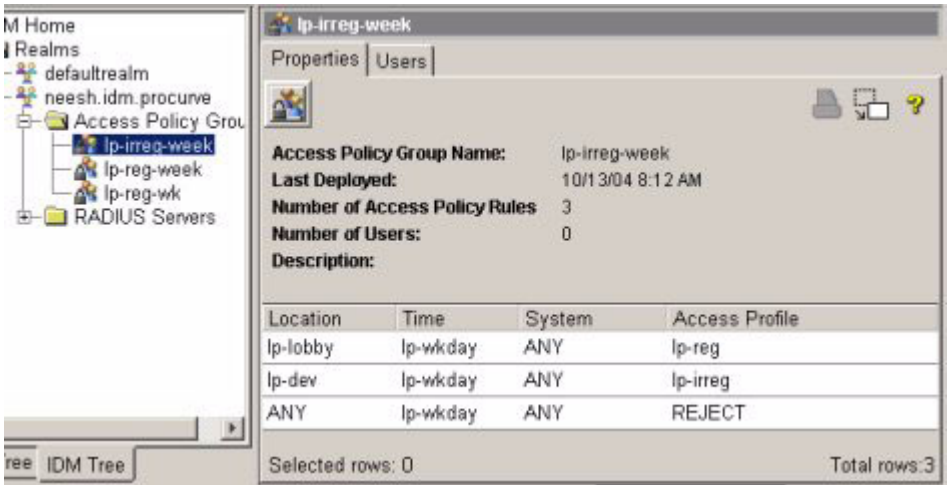


Figure 2-7. Access Policy Group Properties tab

The Users tab underneath contains the list of users currently assigned to the Access Policy Group.

RADIUS Servers: Clicking the RADIUS Servers node displays the RADIUS List tab, with status and configuration information for each RADIUS Server in the Realm that has an IDM Agent installed, or that is manually defined.

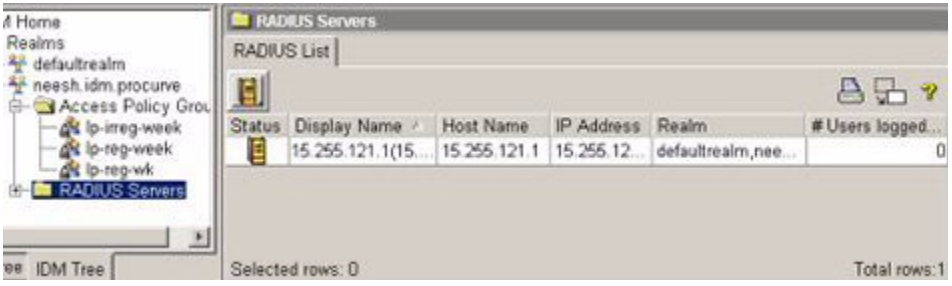


Figure 2-8. RADIUS List tab

NOTE: If the RADIUS server is not in the IDM tree, check in the PCM Events for the following: "PCM remote client authentication failure: *<ip address>*"
Make sure the IP address for the RADIUS server is included in the **access.txt** file on the PCM server. See “Installing the IDM Agent” on page 2-2 for details.

You can expand the RADIUS Servers node to view the servers in the tree. Click the individual server to display the RADIUS Server Properties.

Figure 2-9. RADIUS Server Properties tab

The Activity Log tab underneath the properties display contains a listing of IDM application events for that RADIUS server such as server startup, server connections, user logins, IDM configuration deployment, etc.

Toolbars and Menus

Because IDM is a module within PCM, it uses the same Main Menu and Global toolbar functions. Individual tabs or windows within the IDM module also include separate component toolbars.

The functions available in the component toolbar vary based on applicable functions for that component. Toolbar icons for disabled functions are grayed out. The component toolbar options are described under the process they support in the next chapter. You can hover with the mouse to display 'Tooltips' for each icon.

Using Right-Click Menus

You can also access most of the functions provided with IDM via the "right-click" menus. To use the right-click menu, select an object (node) in the navigation tree on the left of the screen, then right-click your mouse to display the menu. You can also access the right-click menus when an item is selected in a List on the tab views.

Figure 2-10. IDM Right-click menu

The options available in the right-click menu will vary based on the node or list item you have selected. Disabled functions are grayed out.

Using IDM as a Monitoring Tool

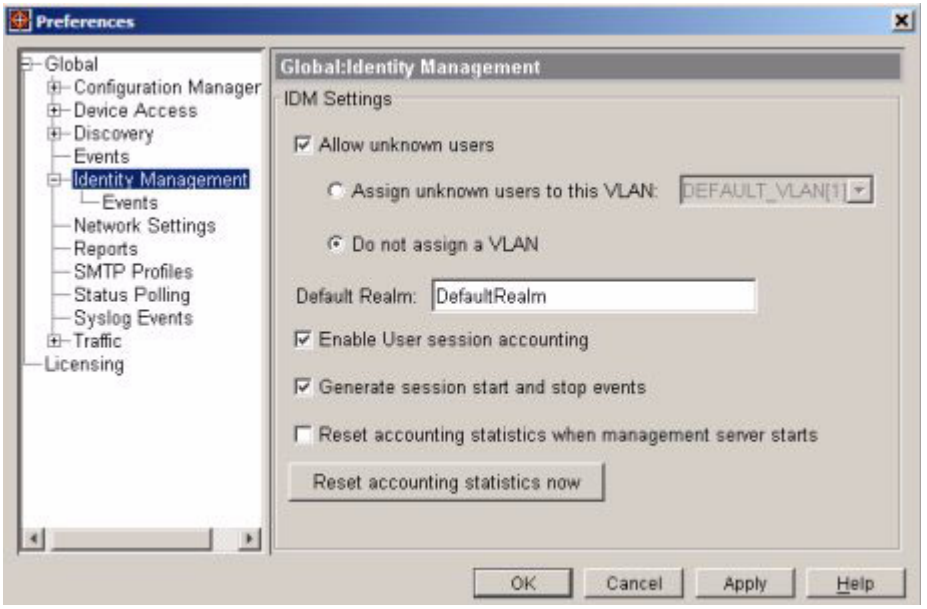
As we stated at the start of this chapter, it is best to install the IDM Agent and let it run to learn about the Realm, RADIUS server, and users on the network. By allowing IDM to run without defining access or authorization parameters, you can use IDM to monitor users on the network and generate usage reports. You can enable or disable IDM monitoring using the IDM Preferences.

NOTE: Session accounting must be enabled on the switch, and in IDM, for the monitoring and User session accounting in IDM to work. Refer to the section on "Radius Authentication and Accounting" in the *Access and Security Guide* provided with the ProCurve switch for details on enabling session accounting.

IDM Preferences

The IDM Preferences window is used to set up global attributes, such as establishing the default realm and how to handle unknown users.

Click the Tools menu and select Identity Management to display the Global Preferences-Identity Management window.



The default IDM settings are:

- "Allow unknown users to access the network", and "Do not assign a VLAN." This provides unknown user access (unrestricted by IDM) and allows IDM to learn information about users from the RADIUS server.

  You can configure IDM to restrict access by:
  - Selecting "Assign Unknown users to this VLAN" and specifying the VLAN the unknown user can access.
  - Deselect "Allow unknown users". This will deny network access to unknown users.
- "User session accounting" is also enabled so you can monitor users on the network, and collect data for User Login and Bandwidth usage reports in IDM. If you disable User session accounting, IDM will not collect data for the Bandwidth Usage and User Session reports.
- "Generate Session Start and Session Stop events" option is selected, which means user's session start and stop events will be displayed in the IDM Events list. If you de-select the option, session history and statistical information will still be collected, but the start and stop events are not displayed in the IDM Events list.
- "Reset accounting statisticswhen management server starts " option is disabled. If you click to enable this option, all session accounting information is reset when the PCM/IDM server is restarted. Any open sessions will be closed, and RADIUS Server totals are reset to zero.
- Click "Reset accounting statistics now" to reset all accounting information immediately (after confirmation). Any open sessions are closed, and RADIUS Server totals are reset to zero.

If the status of users -- whether they are logged on or off -- seems to be incorrect, it is possible that the session accounting has somehow gotten out of sync. You can correct this problem by using the "Reset accounting statics now" option. This will close any open session (this has no effect on the user, only on the IDM accounting), and it will reset login counts for users back to zero.

Once you have been running IDM long enough to capture and configure the necessary Realms, Access profiles, and assign users to Access Profile Groups, you can alter these Identity Management preferences to restrict access for unknown users.

If you are using Web-Auth or MAC-Auth for user authentication, the user session statistics are not collected, since the data is unavailable from the switch. User logins and Bandwidth Usage data is still available.

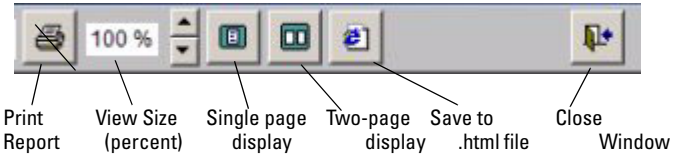
Using IDM Reports

IDM provides reports designed to help you monitor and analyze usage patterns for network resources. The report options are available from the Tools menu.

You can access User Reports by right-clicking on the user in the Users tab display, then select the report option.

The report statistics for each report type are cleared by the Session Statistics Cleanup policy (in PCM) on the first day of each month.

The Report display includes a toolbar with viewing and printing functions.



Bandwidth Usage Report: The Bandwidth Usage Report shows the top 25 bandwidth users. This report is helpful in identifying candidates for throttling.

The following information is provided for each of the top 25 users:

Number	Rank (1-25) within the top 25 users
Username	Username used to login
Realm	Realm (Access Policy Group and RADIUS server) to which the user is assigned
Friendly Name	Friendly name assigned by the Adminsitrator, optional.
Access Policy	Access Policy Group governing a user's login to the RADIUS server
Last Login	User's most recent successful login
Bandwidth	Bandwidth used during the reporting period, given in total Octets

The report period is from the first day of the month to the current date. The Session Statistics Cleanup policy in PCM clears resets the session total to zero on the first day of each month.

Configuration Report: The Configuration Report provides information for each Realm and RADIUS server the IDM Agent has learned, or that have been defined in IDM. Realm information includes the most recent configuration policy (access profile) deployment date and assigned RADIUS servers, access policy groups, and users. The RADIUS server section includes information similar to that shown on the RADIUS Server Properties window.

Unsuccessful Login Report: The Unsuccessful Login Report shows every failed login and contains the following information for each login:

Date	Date and time when the login failed
Username	Username entered to log in
Realm	Realm associated with the access policy group to which the user is assigned
Friendly Name	Name of user logging in with the username
Access Policy	Access policy group to which the user is assigned
Last Login	Date and time the user last log in successfully
Denial Reason	Reason the login failed. Denial reasons can be generated by IDM or the RADIUS server.

User Report: The User Report lists information for recent sessions in which the user participated. The following information is provided for each session:

Start	Date and time the user logged in (session started)
End	Date and time the user logged out (session ended)
RADIUS Server	RADIUS server where the user logged in.
ok?	???
Termination Reason	???
Octets in/out	???

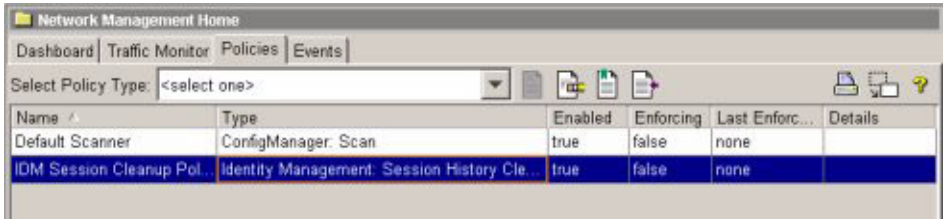
To display the User Report select a username in the Users tab of the Access Policy Group or RADIUS Server window, and then click the User Report icon in the toolbar.

IDM Session Cleanup Policy

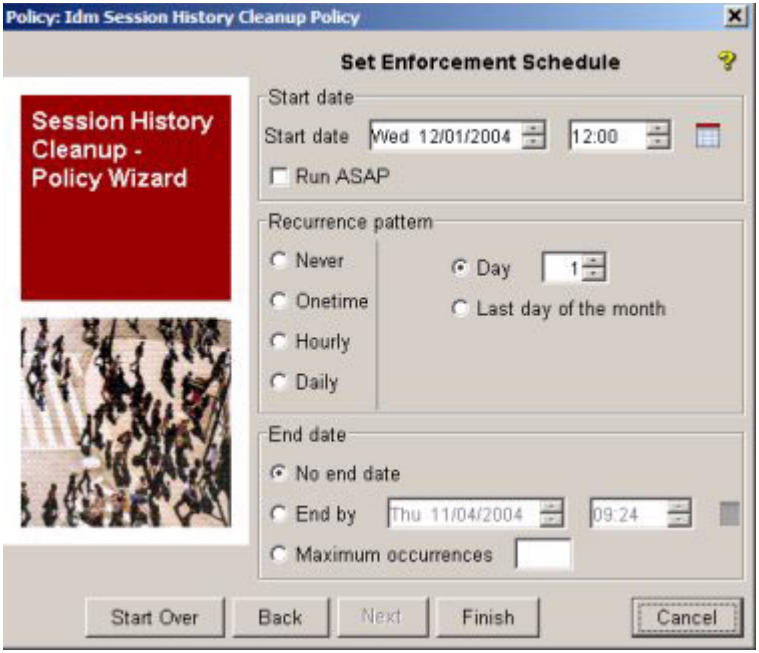
The IDM Session Cleanup Policy is included in the PCM+ policies by default when you install IDM. This policy works to reset the session accounting statistics at the start of each month.

To modify the IDM Session Cleanup Policy:

1. Click the Primary Tree tab at the bottom left of the window to display the "Network Management Home" window, and then click the Policies tab to display the list of Policies.



2. Select the IDM Cleanup policy and click the modify icon in the toolbar to start the policy wizard.
3. Click the Next button to continue to the Policy Enforcement dialog.



4. Set the Start Date for enforcement of the policy. The default is the start date and time for IDM.
   You can type in a new date and time, or use the arrows to increase or decrease the date and time entries. Note that the time clock uses 24 hour format; thus a time of 22:00 is used to indicate a start time of 10:00 pm.

   Check (click) the Run ASAP checkbox to reset the session statistics immediately.

5. You can change the session cleanup interval using the Recurrence pattern options:

   IDM Session Cleanup Recurrence Pattern Options

If you select...	The action is...
Never	No further action is required (Policy definition is saved, but will not be enforced).
One time	No further action is required (the currently scheduled time is used with no recurrences).
Hourly	Type the number of hours and minutes to wait between session cleanup. If you do not want the policy enforced on Saturdays and Sundays, check the Skip weekend checkbox.
Daily	Type the number of days to wait between session cleanups. If you do not want the policy enforced on Saturdays and Sundays, check the Skip weekend checkbox.
Weekly	Check the boxes for the days of the week you want to enforce the policy.
Monthly	Click the Last day of the month button to enforce the schedule on the last day of the month. OR Click the Day button and use the up or down arrows to select the day of the month.

6. Click the radio button to select No end date, End by, or Maximum occurrences to identify when the schedule should end.
   - If you select No end date, the schedule will run at the selected intervals until the policy is changed or deleted.
   - If you selected End by, click the up and down arrows in the End by field until the desired end date and time are shown.
   - If you selected Maximum occurrences, type the number of times the policy should be enforced before it is disabled automatically.
7. Click Finish to complete the process and exit the wizard.

3

Using Identity Driven Manager

Chapter Contents

IDM Configuration Model

As described in the IDM model on page 2-5, everything relates to the top level, or Realm. Each User in the Realm belongs to an Access Policy Group (APG). The APG has an Access Policy defined for it that governs the access rights that are applied to its Users as they enter the network.

The Access Policy is defined using a set of Access Rules. These rules take three inputs:

- Location (where is the user accessing the network from?)
- Time (what time is the user accessing the network?)
- System (from what system is the user accessing the network?)

Using these input parameters, IDM evaluates each of the rules. When a matching rule is found, then the access rights (called an Access Profile) associated with that rule are applied to the user. The Access Profile defines the VLAN, QoS, and rate-limits (Bandwidth) that are applied to the user as they access the network. Thus, based on the rules defined in the APG, the user gets the appropriate level of access to the network.

In summary, for identity driven management each user in a Realm belongs to an Access Policy Group. The Access Policy Group defines the rules that are evaluated to determine the access policies that are applied at the switch when the user connects to the network.

Configuration Process Review

Assuming that you opted to let IDM run long enough to discover the Realm, users, and RADIUS server, your configuration process will be:

1. Define "locations" (optional) from which users access the network. The location may relate to port-based VLANS, or to all ports on a switch.
2. Define "times" (optional) at which users will be allowed or denied access. This can be by day, week or even hour.
3. If you intend to restrict a user's access to specific systems, you need to modify the User profile to include the MAC address for each system from which the user is allowed to login.
4. Create the Access Profiles to set the VLAN, QoS, and rate-limits (Bandwidth) that will be applied to users in an APG.

5. Create an Access Policy Group, with rules containing the Location, Time, System, and Access Profile that will be applied to the user when they login.
6. Assign Users to the appropriate Access Policy Group.

Once the configuration has been completed on the IDM Client GUI, it needs to be deployed to the IDM Agent on the RADIUS Server. The authorization controls can then be applied when IDM detects an authenticated user login. If you do not deploy the IDM configuration to the Agent on the RADIUS server, it will not be applied.

NOTE: If you want to modify or delete an Access Policy Group, or the locations, times, or access profiles used in the Access Policy Group, make sure your changes will not adversely affect users assigned to that group before you deploy the changes.

Configuring Locations

Locations in IDM identify the switch and/or ports on the switch where users connect to the network. Because users generally are allowed to log in to the network from a variety of locations, IDM allows you to create customized locations to match specific environments.

For example, a generalized company "location" may include all of the ports on a switch, or multiple switches through which users can connect to the network. You can define a lobby location as a single switch, or a single port on the switch, in order to restrict access to the network for visitors attaching to the network in the lobby.

To begin, click the "Show Locations" icon in the Global toolbar to display the "Locations" window.

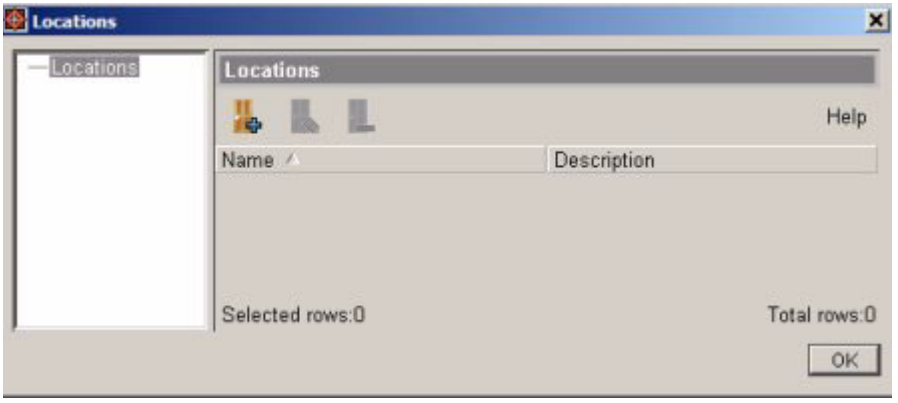
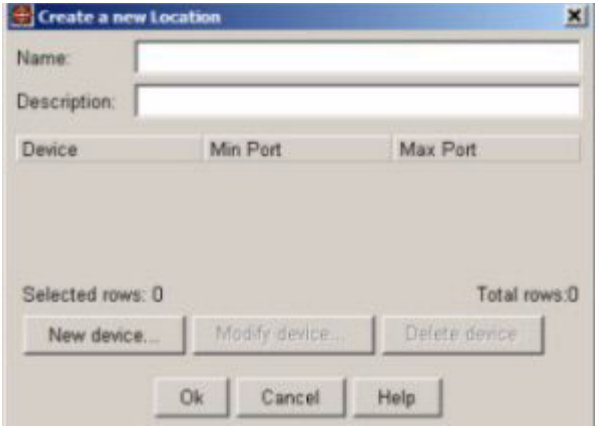


Figure 3-1. Locations window

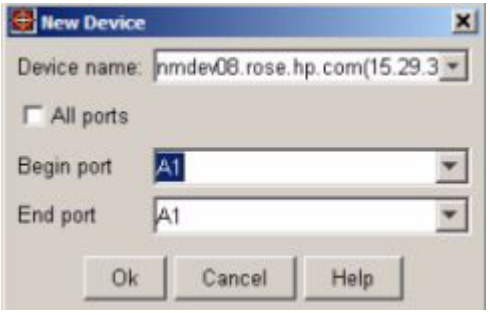
Adding a New Location

To create a new location:

1. Click the "New Location" icon in the toolbar to display the new locations window.



2. Type in a Name for the location
3. Type in a Description for the location
4. Click "New device..." to open the New Device window.



5. Type in the IP address for the device (switch), or select a device from the pull down list in the "Device name" field. The list includes the ProCurve switches from the PCM Devices list.
6. Click to select "All ports" on the switch, or use the pull down lists to select the ports on the device that will be associated with the new location.

NOTE: If a switch in the device list is not configured to authenticate with the RADIUS server, the settings in IDM will have no affect.

You can type in an IP address for non-ProCurve devices; however, HP does not provide support for IDM configurations with non-ProCurve devices.

7. Click Ok to save the New Device settings to the Location, and close the window.
8. The Device address and ports information is displayed in the "New Location" window.
9. Repeat steps 4 through 7 to add additional devices to the Location, or click OK to save the new Location and close the window.

Modifying a Location

To edit the information for an existing Location:

1. Click the "Show Location" icon in the toolbar to display the Locations window, with the list of defined locations.

2. Click on a location in the list to select it.

3. Click the "Modify Location" icon in the toolbar to display the Modify Location window.

4. Edit the Name and Description as needed.
   - To delete a device, select the device in the list, then click Delete Device.
   - To Modify the device settings, select the device in the list, then click Modify device... to display the Modify Device window.

     The Modify Device window contains the same fields as the New Device window. You can edit the ports associated with the location, or you can choose a different device and reset the ports for the new device. Click OK to save your changes and close the window.

   The changes are displayed in the Modify Location window.
5. Click OK to save the location changes and close the Modify Locations window.

   Click Cancel to close the window without saving the changes. The original location configuration will be maintained.

NOTE: When modifying Locations, make sure all devices for the location are configured with the appropriate VLANs. If you Modify a Location that is part of a VLAN (subnet) and that Location is currently used in an Access Policy Group rule, IDM will check to make sure that the VLAN exists. If not, an error message is displayed.

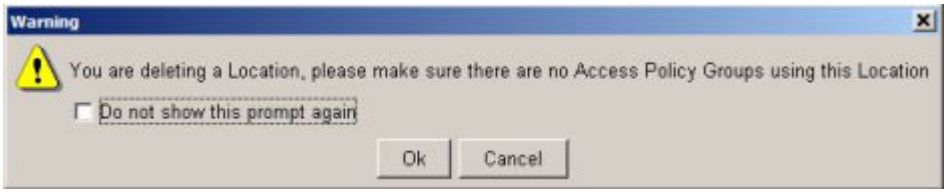
Deleting a Location

To remove an existing Location:

1. Click the "Show Location" icon in the toolbar to display the Locations window, with the list of defined locations.
2. Click on a location in the list to select it.

3. Click on the "Delete Location" icon in the toolbar to remove the location.

   The first time you use the Delete Location option, a warning pop-up is displayed. Click Ok to continue, or Cancel to stop the delete process.



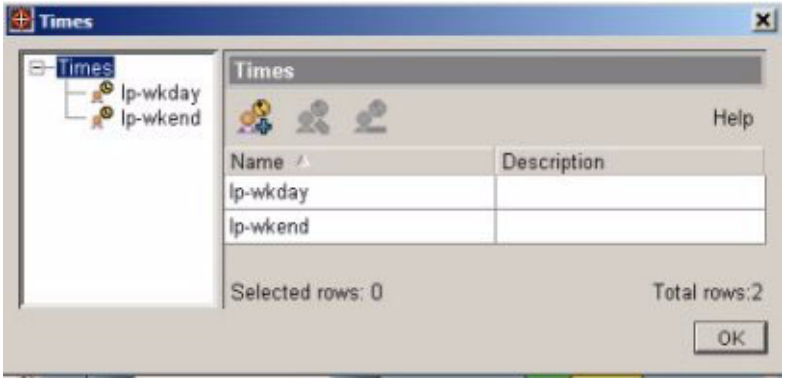
4. The location is removed from the Locations list.

NOTE: If you modify or delete a Location, check to make sure that the changes do not adversely affect users in Access Policy Groups where the Location is used.

Configuring Times

Times are used to define the hours and days when a user can connect to the network. When included in the Access Policy Group rules, the time can be used to allow or deny access from specific locations at specific time. For example, students might be allowed network access from the "Classroom" location during weekdays, from 9:00 am to 5:00 pm, but denied access from the Classroom at any other time.

To begin, click the "Show Times" icon on the Global toolbar to display the Times window.



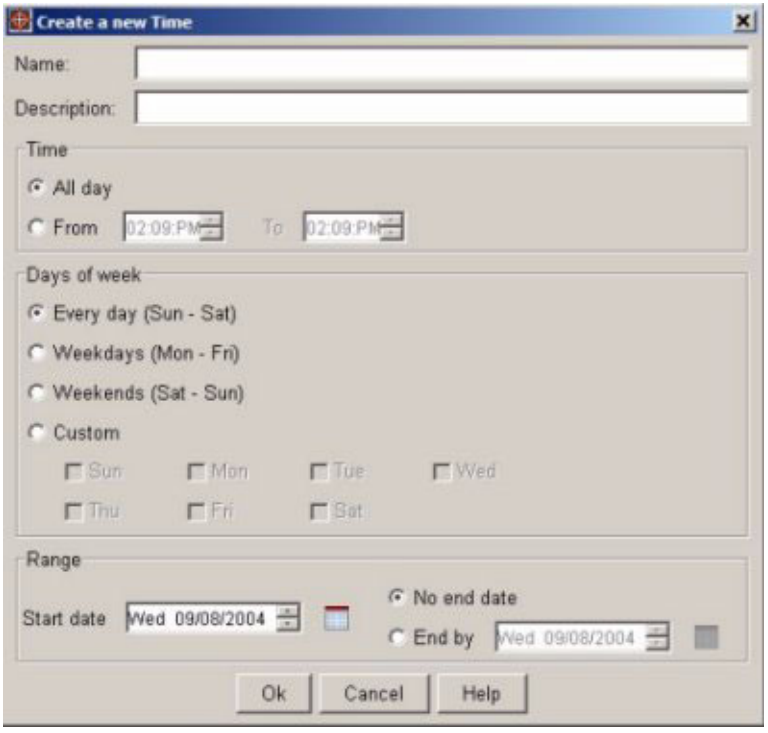
The Times window lists the name and description of defined times. Click the time node on the left to display the Time's properties, including:

Name	Name used to identify the time
Description	Brief description of the time
Time	Time of day when the access policy group is active.
Days of week	Days of the week when the access policy group is active
Range	Dates during which the "Time" will be in effect. A start date must be specified.

Creating a New Time

1. Click the "Show Times" icon on the Global toolbar to display the Times window.

2. Click the "Create new Time" toolbar icon to display the "Create a new Time" window.



3. Define the properties for the new time.

Name	Name used to identify the time
Description	Brief description of the time
Time	Time of day when user will be accepted on the network. To allow access the entire day, click the **All day** radio button. To restrict access to specific hours of the day, click the **From** radio button and type the beginning and ending times. The ending time must be later than the beginning time. AM or PM must be specified.
Days of week	Days of the week that a user will be accepted or rejected on the network. Click the radio button next to the desired days. Click the Custom radio button to enable the day(s) of the week check boxes.
Range	Dates during which the time will be in effect. Select the **Start Date** and then click the **No End Date** radio button, or select the **End Date**.

IDM Time parameters

4. Click Ok to save the new "Time" and close the window.
   The new time appears in the Show Times window.

Modifying a Time

1. Click the "Show Times" icon on the Global toolbar to display the Times window.
2. Click on a time in the list to select it.

3. Click the "Modify Time" icon in the toolbar to display the Modify Time window. The Modify Time window shows the details of time, similar to the Create a new Time window.
4. Modify the time parameters, as described in Table on page 3-10.
5. Click Ok to save your changes and close the window

NOTE: If you modify or delete a Time, check to make sure that the changes do not adversely affect users in Access Policy Groups where the Time is used.

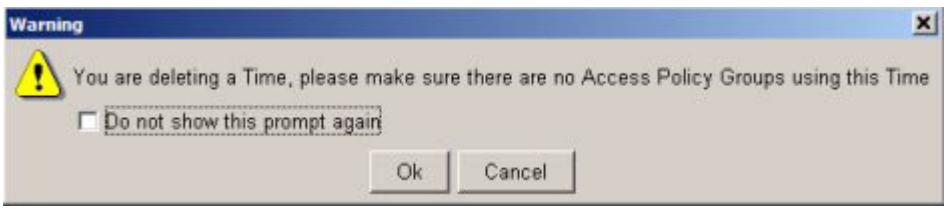
Deleting a Time

To remove an existing "Time":

1. Click the "Show Times" icon in the toolbar to display the Times window, with the list of defined Times.
2. Click on a Time in the list to select it.

3. Click on the "Delete Time" icon in the toolbar to remove the location.

   The first time you use the Delete Time option, a warning pop-up is displayed. Click Ok to continue, or Cancel to stop the delete process.

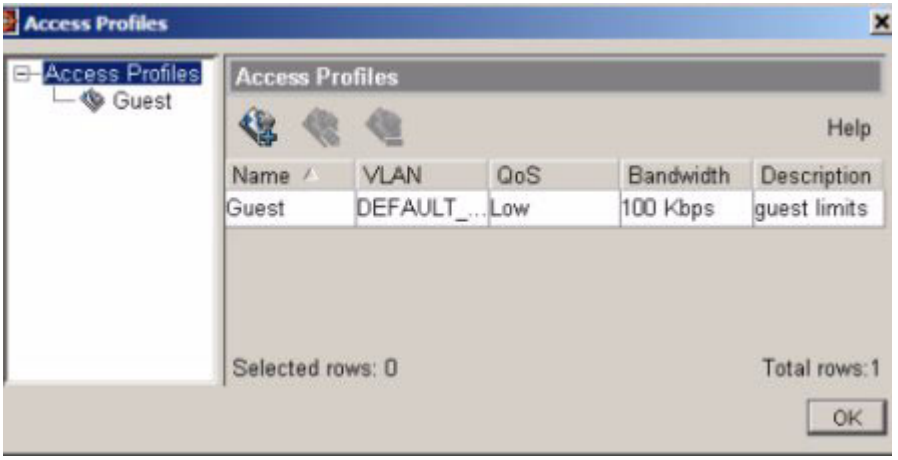


4. The Time is removed from the Times list.

Configuring Access Profiles

IDM uses an Access Profile to set the VLAN, QoS, and Bandwidth (rate-limits) that are applied to the user when they are authenticated on the network. This is where the real benefits of "access control" are realized. When users log in, the Access Profile dynamically configures the switch settings to provide the proper network access and resources.

To begin, click the "Show Access Profiles" icon on the Global toolbar to display the Access Profiles window.



The Access Profiles window lists defined Access Profiles. Click the Access Profile node on the left to display the details, including:

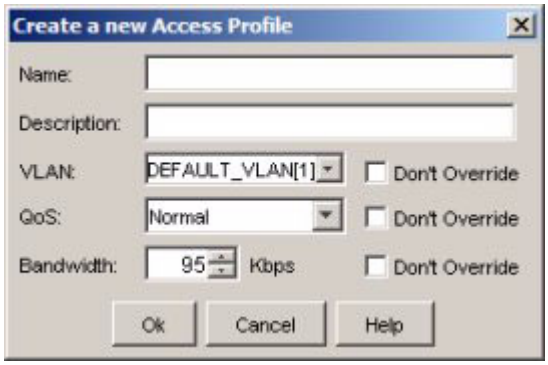
Name	Name used to identify the profile
Description	Brief description of the profile
VLAN	VLAN the access is set for.
QoS	The "Quality of Service" setting
Bandwidth	The rate limits for outbound traffic

The Access Profile tells the switch to override any local settings for the port the user is accessing with the settings specified in IDM.

Creating a New Access Profile

1. Click the "Show Access Profiles" icon on the Global toolbar to display the Access Profiles window.

2. Click the "Create new Access Profile" icon in the toolbar to display the "Create a new Access Profile" window.



3. Define the following attributes for the Access Profile.

Name	Name used to identify the Access Profile
Description	Brief description of the Access Profile
VLAN	The VLAN to which access is given. You can type in the VLAN or select one from the pull-down menu, which lists VLANs configured in PCM. The DEFAULT_VLAN(1) is equivalent to allowing access across all segments and switches on the network. If another VLAN is specified, the user is only allowed access to that network segment.
QoS	The Quality of Service, or "priority" that will be given to outbound traffic under this profile. Select the setting from the pull-down menu.
Bandwidth	The rate- limits that will be applied for this profile. Use the up-down arrows to increase or decrease the Bandwidth. The default setting is1000 Kbps (1 Mbps) NOTE: This value will get translated into a percentage of bandwidth at the switch.
Don't Override	Select this option for any of the Access Profile parameters to use the current settings at the switch when the user logs in.

Access Profile parameters

4. Click Ok to save the Access Profile and close the window.

NOTE: If you set a VLAN in the Access Profile that is applied to a user during the authentication process, that VLAN will take precedence over "auth-vid" or "unauth-vid" settings on the switch. If the user is rejected by IDM for any reason, and if you have an "unauth-vid" set, the port will be opened and the VLAN will be set to the "unauth-vid."

Modifying an Access Profile

To modify an existing Access Profile:

1. Click the "Show Access Profiles" icon on the Global toolbar to display the Access Profiles window.
2. Click on an Access Profile in the list to select it.

3. Click the "Modify Access Profile" icon in the toolbar to display the Modify Access Profile window. The Modify window shows the details of the Access Profile, similar to the Create a new Access Profile window.
4. Modify the access profile parameters, as described in Table on page 3-13.
5. Click Ok to save your changes and close the window

The changes are displayed in the Access Profiles list.

NOTE: When modifying Access Profiles, make sure the appropriate VLANs are configured on the network and at the switch. If you Modify the VLAN attribute in an Access Profile that is currently used in an Access Policy Group rule, IDM will check that the VLAN exists. If not, an error message is displayed.

Deleting an Access Profile

To remove an existing Access Profile:

1. Click the "Show Access Profiles" icon on the Global toolbar to display the Access Profiles window.
2. Click on an Access Profile in the list to select it.

3. Click on the "Delete Access Profile" icon in the toolbar to remove it.

   The first time you use the Delete option, a warning pop-up is displayed. Click Ok to continue, or Cancel to stop the delete process.

NOTE: If you modify or delete an Access Profile, make sure that your changes do not adversely affect users in Access Policy Groups where the profile is used.

Defining Access Policy Groups

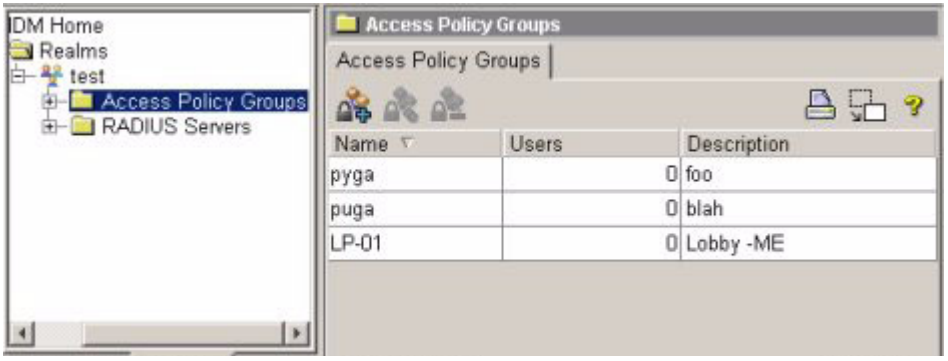
An Access Policy Group (APG) consists of a set of rules that are used to determine the authorization [access controls] that are applied to an authenticated user. Each rule in an Access Policy includes the following parameters:

- Location
- Time
- System
- Access Profile

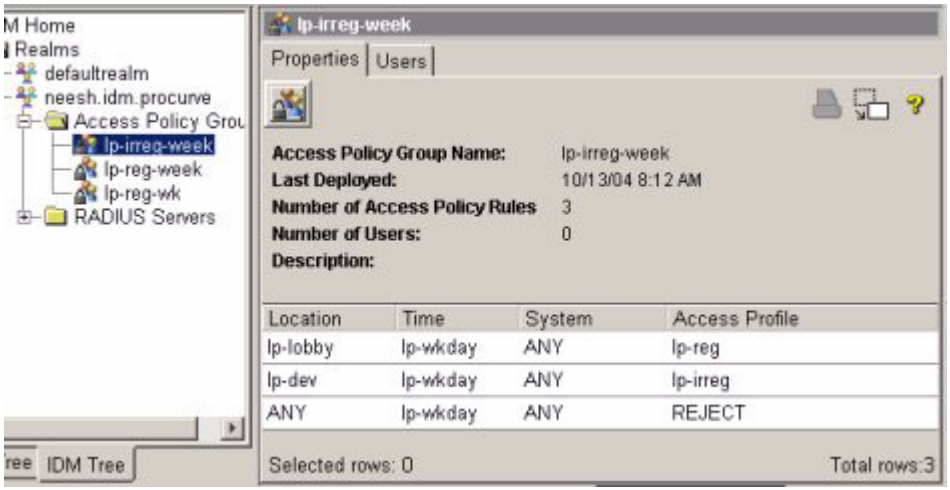
When a user assigned to the APG is authenticated on the RADIUS Server, the IDM Agent applies the appropriate rule, which can cause the switch to accept or reject the user, and modify the switch configuration to provide the appropriate network resources to the accepted user.

You can create an APG that does not have any limitations, that is, it allows "Any" location, time, system, and accepts the default switch settings for VLAN, QoS, and Bandwidth. This would allow you to use IDM to monitor logins and network resource usage by user, without limiting user access to the network.

To begin, click the Access Policy Group node in the IDM tree to display the Access Policy Groups tab.



You can expand the Access Policy Group node in the tree, and click the individual APG node to display the Policy properties.



Creating an Access Policy Group

1. Click the Access Policy Group node in the IDM tree to display the Access Policy Groups tab.
2. Click the "Create new Policy Group" icon in the toolbar to display the "New Access Policy Group" window.

3. Type in a Name and Description for the Access Policy Group.

4. Click "New Rule" to enable the Rule fields.

5. Select an option from the pull down menu for each field.

Location	Lists the Locations you created by name, and the "ANY" option.
Time	Lists the Times you created by name, and the ANY option.
System	Systems from which the user can log in. ANY allows user to login in on any system. OWN restricts users to systems defined for that user. See “Configuring User Systems” on page 3-28 for detail.
Access Profile	Lists the Access Profiles you created by name, and the REJECT option.

6. Repeat the process for each rule you want to apply to the APG.
7. Once you’ve entered all the rules for the APG, use "Move Up" or "Move Down" buttons to arrange the rules in the order you want them to be applied. IDM checks each rule in the list until a match on all parameters is found, then applies the matching rule to the user.

   The Access Policy rules are evaluated in the order they are listed in the rules table. For example, if you want to allow a user to login in from any system during the work week (Mon. - Fri.), but you want to deny access to users on the weekend, you would:
   - Create a Time for the weekend,
   - Create an Access Profile to be applied during weekdays, "Default"
   - Define two rules for the APG, similar to the following:

Location	Time	System	Access Profile
ANY	weekend	ANY	REJECT
ANY	weekday	ANY	Default

When the user is authenticated, IDM checks the Access Policies in the order listed. If it is Saturday or Sunday, the user's access is denied. On any other day, the user is allowed on the network. If the order were reversed, IDM would never read the second rule because the first rule would provide a match every day of the week.

8. Click OK to save the Access Policy Group and close the window.

   IDM will verify that the rules in the APG are valid. If a rule includes a defined VLAN (from the Access Profile) and the VLAN does not exist on the network or devices for the location(s), an error message is returned and you must fix the problem before the APG can be saved.

   Click Cancel to close the window without saving the Access Policy Group configuration.

9. The new Access Policy Group is listed in the Access Policy Groups tab

Modifying an Access Policy Group

1. Click the Access Policy Group node in the IDM tree to display the Access Policy Groups tab.
2. Click on an Access Policy Group Name to select it.

3. Click the "Modify Policy Group" icon in the toolbar to display the "Modify Access Policy Group" window.
4. Modify the Rules as needed by selecting different options from the pull-down menus for each field. (see page 3-16 for field definitions).
5. Click Ok to save your changes and close the window.

   Click Cancel to close the window without saving the Access Policy Group changes.

Deleting an Access Policy Group

1. Click the Access Policy Group node in the IDM tree to display the Access Policy Groups tab.
2. Click on an Access Policy Group Name to select it.

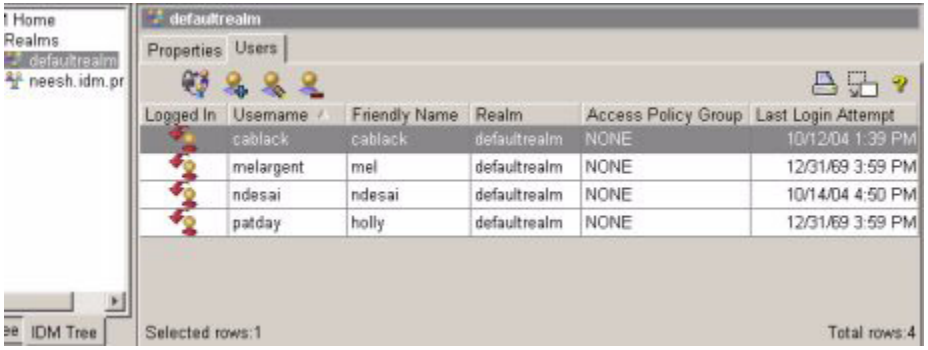
3. Click the "Delete Policy Group" icon in the toolbar to delete the Access Policy Group.

Configuring User Access

The process of configuring User access to network resources using IDM is simplified through IDM's ability to learn User information from the RADIUS server, and the use of Access Policy Groups.

Once you have configured the Access Policy Groups, you simply assign users to an APG. The next time the user attempts to log in to the network, IDM uses the rules in the user's Access Policy Group to dynamically configure the edge switch to provide the appropriate access to the network.

Click the Users tab on the Access Policy Group or Realm window to display the Users List.



The Users List identifies every defined user and contains the following information for each user:

Logged In	Icon indicates whether the user is currently logged in: User is logged in. User is logged out. The icon is greyed out if session accounting is disabled.
Username	Name given to User's login account.
Friendly Name	User's friendly name, if defined, else this is same as Username.
Realm	Realm in which the user logs in.
Access Policy Group	Access policy group to which the user is assigned. NONE indicates the user is "unassigned."

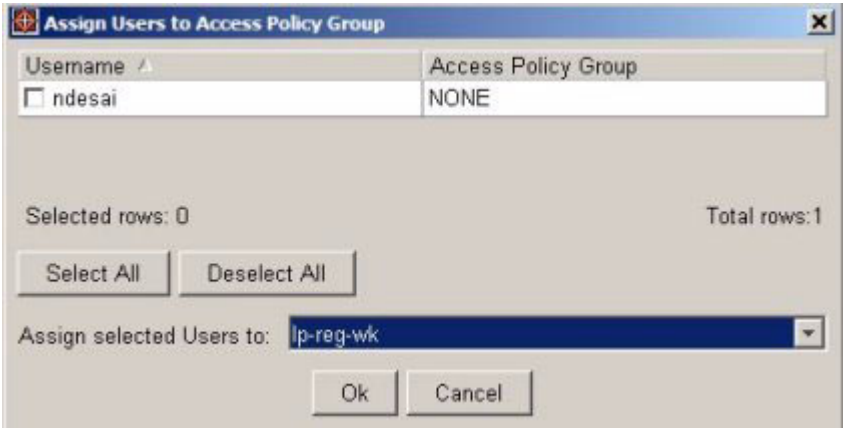
Last Login Attempt	Date and time the user last attempted to log in, regardless if the login failed or succeeded.

Adding Users to an Access Policy Group

To assign a user to an access policy group:

1. Click the access policy group or realm in the IDM tree, and then click the Users tab in the Access Policy Group or Realm window.

2. Click the Add Users to APG icon in the toolbar to display the Assign Users to Access Policy Group window.



3. To assign one or more selected users to an access policy group, check the box next to each user you want to assign to the access policy group.

   To assign all displayed users to the access policy group, click the Select All button.

4. In the "Assign selected Users to:" field, use the pull-down menu to select the access policy group to which you want to assign the user(s).

5. Click Ok to save the assignments and close the window.

   The new APG assignments are displayed in the Users list.

Changing Access Policy Group Assignments

To re-assign users to a different APG:

1. Click the access policy group or realm in the IDM tree, and then click the Users tab in the Access Policy Group or Realm window.

2. Click the Add Users to APG icon in the toolbar to display the Assign Users to Access Policy Group window.
3. Select the users to be re-assigned by clicking the checkbox for each user, or use the "Select All button"
4. In the "Assign selected Users to:" field, use the pull-down menu to select the access policy group to which you want to assign the user(s).

   If you select NONE from the menu, then the user is Unassigned. Unassigned users can still log into RADIUS servers, but they are not governed by access policy group rules. IDM will still collect and display event information for unassigned users, as long as they are authenticated by the RADIUS server.
5. Click Ok to save your changes and close the window.

   The new APG assignments are displayed in the Users list.

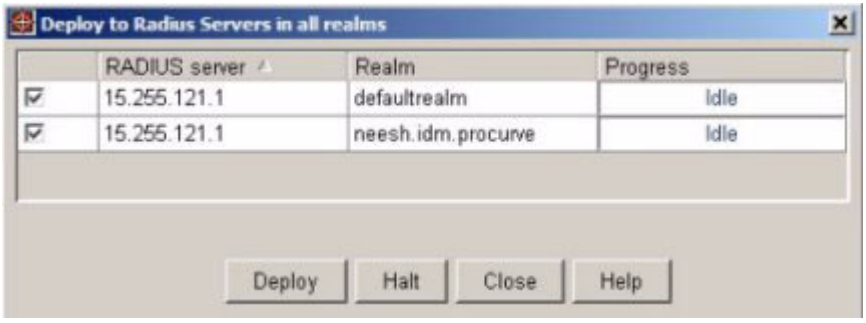
Deploying Configurations to the Agent

Once you have configured the Access Policy Groups and assigned users, you need to deploy the configuration information to the IDM Agent. The Access Policy Group assignments (including the locations, times, and Access Profiles) are not applied until they get deployed to the IDM Agent on the RADIUS server, and the user logs in again.

If you have added or changed any of the parameters included in the APG, the IDM dashboard display will include a warning note in red text indicating that you need to deploy the new configuration before changes will take effect.

To deploy the IDM authorization policy configuration:

1. Right-click on the Realm in the IDM tree
2. Select the "Deploy current policy to this realm" option to display the "Deploy to RADIUS Server" window.



3. Click "Deploy" to write the access policy information to the IDM Agent for the selected Realms and the respective RADIUS Servers.
4. Click "Close" to exit the window.

After the new access policy configurations are deployed, the deployment warning on the IDM Dashboard display is removed.

Using Manual Configuration

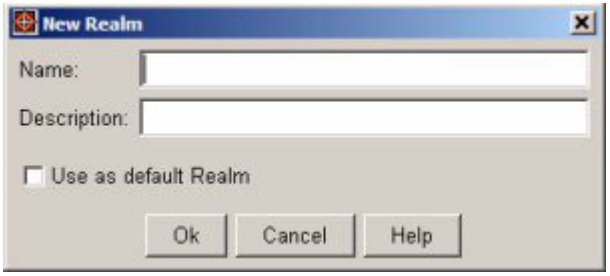
It is simplest to let the IDM Agent run and collect information about Realms, including RADIUS servers and users in the Realm from the RADIUS server, but you can also manually define information about the Realm, RADIUS servers, and users in the IDM GUI.

Defining New Realms

If you have configured a new Realm that uses the RADIUS server on which you have installed the IDM Agent, you can let the agent learn the Realm information automatically, or you can define the Realm in the IDM Client.

To define a realm:

1. Click the New Realm icon on the Realm List toolbar to display the "New Realm" window.



2. Enter the information for the Realm:
   - Type the name used to identify the realm.
   - Type a brief description of the realm in the Description field.
   - To set the realm as the default realm, click the "Use as default Realm" check box.
     The default realm is used when IDM cannot determine the realm for a RADIUS server or user login.
3. Click Ok to save the Realm information and close the window.

The new Realm appears in the Realm List, and the IDM Tree.

Modifying and Deleting Realms

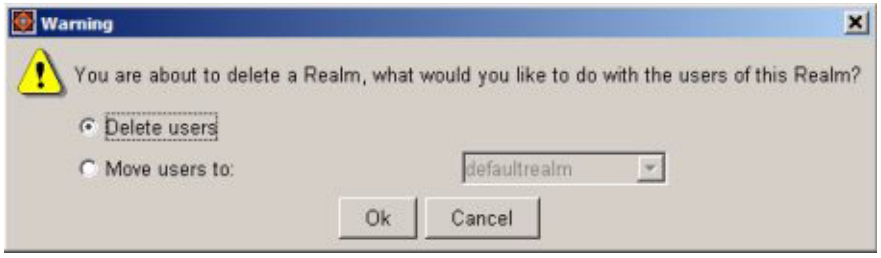
To modify an existing Realm:

1. Select the Realm in the Realm List.
2.  Click the Modify Realm icon on the Realm List toolbar to display the "Modify Realm" window. (similar to the New Realm window).
3. Edit entries as needed for the Realm:
   - Type the name used to identify the realm.
   - Type a brief description of the realm in the Description field.
   - To set the realm as the default realm, click the "Use as default Realm" check box.
     The default realm is used when IDM cannot determine the realm for a RADIUS server or user login.
4. Click Ok to save the Realm information and close the window.

The new Realm information appears in the Realm Properties tab, and the Realm List.

To delete a Realm:

1. Select the Realm in the Realm List.
2.  Click the Delete Realm icon in the toolbar.
3. A pop-up confirmation window is displayed.



Click one of the radio buttons (defined below), and then click Ok to delete the selected realm and close the window.

Delete users: Delete all users currently assigned to the access policy group used by the realm.

Move users to: Reassign all users in the Realm to a different (new) Realm (use the drop-down menu to select a new Realm for the user)

The selected realm is removed from the Realm List and IDM Tree.

Defining RADIUS Servers

You can let the IDM Agent learn about the RADIUS server on which it is installed, or you can define the RADIUS Server in the IDM Client.

NOTE: You can have multiple RADIUS servers within your Realm. If you want IDM to monitor and provide access control on each server, you need to install an IDM Agent on each RADIUS server. The IDM Client displays information received from each of the RADIUS + IDM Agents in the Realm.

To define a new RADIUS Server:

1. Right-click the RADIUS Servers folder in the IDM tree and select "New RADIUS server..." from the drop-down menu to display the Define New RADIUS Server window.

2. In the IP Address field of the new RADIUS Server window, type the IP address of the server being defined.
3. In the Hostname field, type the name used to identify the server in reports and displays.
4. The Realm field defaults to the Realm where you selected the RADIUS Server folder. If you have more than one Realm, you can select the realm assignment for the RADIUS server from the drop down menu.
5. In the Description field, type a brief description of the server.
6. Click Ok to save the RADIUS Server information and close the window.

The new RADIUS Server appears in the IDM Tree, and the RADIUS List.

Modifying and Deleting RADIUS Servers

To modify an existing RADIUS Server:

1. Use the IDM Tree to navigate to the RADIUS List window, and select the RADIUS Server you want to edit in the list.

2. Click the Modify RADIUS icon on the Radius List toolbar to display the "Modify RADIUS" window. (similar to the New RADIUS window).
3. Edit entries as needed for the RADIUS Server:
   - Edit the IP address of the server being defined.
   - Edit the Hostname used to identify the server in reports and displays.
   - If you have more than one Realm, you can select the realm to which you want to assign the RADIUS server from the drop down menu.
   - Edit the description of the server.
4. Click Ok to save the RADIUS Server information and close the window.

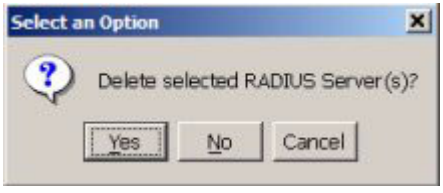
The edited RADIUS Server information appears in the RADIUS List, and the Properties tab for the server.

To delete an existing RADIUS Server:

NOTE: Before you can completely delete the RADIUS server, you need to uninstall the IDM Agent on the server. Otherwise, the RADIUS server may be re-discovered, causing it to re-appear in the IDM tree.

1. Use the IDM Tree to navigate to the RADIUS List window, and select the RADIUS Server you want to delete in the list.

2. Click the Delete RADIUS icon on the Radius List toolbar.
3. A pop-up confirmation dialog is displayed:



4. Click Yes to complete the delete process and close the window.

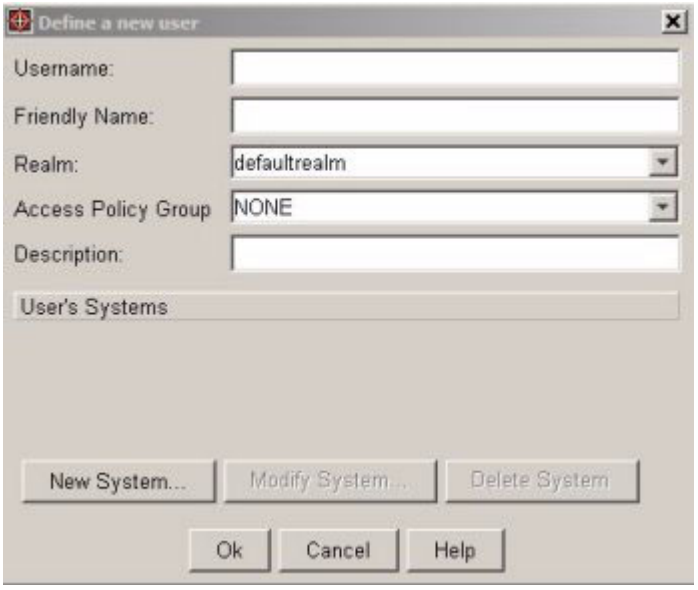
The RADIUS Server is removed from the RADIUS List and the IDM Tree.

Adding New Users

You can let the IDM Agent automatically learn about the users from the RADIUS server on which it is installed, or you can define user accounts in the IDM Client.

To add a new User in IDM:

1. Click the Users tab on the Access Policy Groups or Realms window, and then click the New User button to display the New User window.

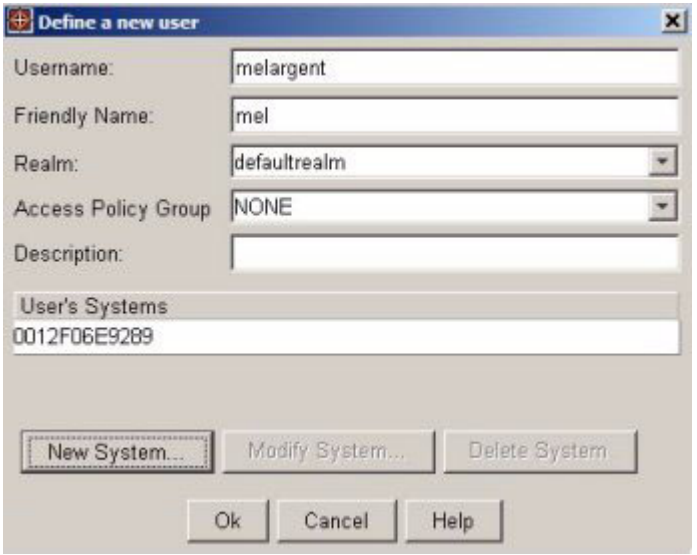


2. Enter the information for the User
   - Username: The user's login name (required).
   - Friendly Name: Friendly name for the user.
   - Realm: Select the Realm the user "belongs" to, if different from the default realm.
   - Access Policy Group: Select the Access Policy Group to which the user belongs. This sets the access profile that is applied when the user logs in to the network. The default is NONE.
   - Description: Enter additional text describing the user if needed.
3. If you want to restrict the user's access to specific systems, click "New System..." to display the User's System dialog.
   Otherwise click OK to save the user and close the window.

Configuring User Systems

4. To restrict the user's access to specific systems, click "New System..." to display the New User System dialog.

5. Enter the MAC Address of the system (in any format) from which the user is allowed to login to the network, then click OK. The system information is displayed in the New User window.



   If the user is allowed to login from more than one system, repeat the process for each system.

6. When the User's Systems are defined, click OK to save the new user information and close the window.

The new user appears in the Users List.

NOTE: Access Policy Group settings are not applied to the user until you deploy the new configuration to the IDM Agent on the RADIUS server. See "Deploying Configurations to the Agent" on page 3-22 for details.

Modifying and Deleting Users

To modify an existing User:

1. Select the User in the User List and click the Modify User icon in the toolbar.
2. The "Modify User" window (similar to the New User window) is displayed.
3. Edit entries as needed for the User:
   - Username: The user's login name (required).
   - Friendly Name: Friendly name for the user.
   - Realm: Select the Realm the user "belongs" to, if different from the default realm.
   - Access Policy Group: Select the Access Policy Group to which the user belongs. This sets the access profile that is applied when the user logs in to the network. The default is NONE.
   - Description: Enter additional text describing the user if needed.
   - Add, Modify, or Delete User System information as needed.
     – To edit User Systems information, select the System in the list, then click Modify to display the Systems window and change the MAC Address.
     – To delete a User System, select the System in the list, then click Delete.

     The changes appear in the System's List for the user.
4. Click OK to save the new user information and close the window.

NOTE: Changes in Access Policy Group settings are not applied to the user until you Deploy the new configuration to the IDM Agent on the RADIUS server. See "Deploying Configurations to the Agent" on page 3-22 for details.

To delete a User:

1. Select the User in the User List

2. Click the Delete User icon in the toolbar.
3. Click Yes in the Confirmation pop-up to complete the process.

The user is removed from the User List.

(This page is intentionally unsused)

4

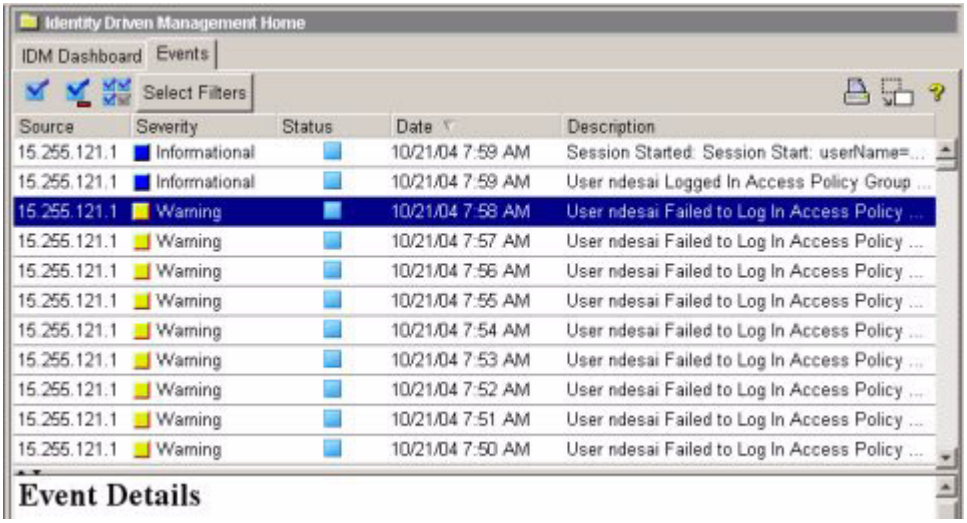
Troubleshooting IDM

Chapter Contents

IDM Events

The IDM Events window is used to view and manage IDM events generated by the IDM application or the IDM Agent installed on a RADIUS server. This window helps you quickly identify IDM-related problems in your network.

To view the IDM events, click the Events tab in the IDM Home display.



The Events window works similarly to the PCM Events window. It lists IDM events currently contained in the database. The default listing event is categorized by the level of severity.

Sortable columns of information are available for each event:

Column Heading	Description
Source	This column contains the name or IP address of the component or device that generated the event.
Severity	The Severity column shows the severity of each event. Events are categorized into five levels of severity.
Status	The Status column identifies whether the event has been acknowledged. A check mark in the blue square indicates that the event has been acknowledged. **NOTE**: The Status column shows only unacknowledged events if events are deleted automatically after being acknowledged. See IDM Event Settings for additional information.

Date	The Date column lists the date and time when the event occurred, given in MM/DD/YY/HH:MM format.
Description	The Description column provides a short description of the event. The description is derived from a list of predefined descriptions based on the event type.

You can sort the Events listing by Source, Severity, Status or Date. Click the desired column heading to sort events in descending order. Click the column heading again to sort events in ascending order. A down pointer in the column heading indicates descending order, and an up pointer indicates ascending order.

Select an event in the Events listing to display the Event Details at the bottom of the window.

The details provide additional event description information. The details will vary based on the type of event. Use the scroll bar or drag the top border of the Event Details section to review the entire event description.

Acknowledging an event indicates that you are aware of the event but it has not been resolved. Depending on the IDM event settings, the event is then removed from the event list or the status of the event is updated in the Events window.

To acknowledge an event:

1. Click the Events tab on the IDM Dashboard window to navigate to the IDM Events window.
2. Select the events to be acknowledged.
3. Click the Acknowledge Event icon in the toolbar.

To delete an IDM event:

1. Click the Events tab on the IDM Dashboard window to display the IDM Events window.
2. Select the event(s) to be deleted.
3.  Click the Delete Event icon in the toolbar.

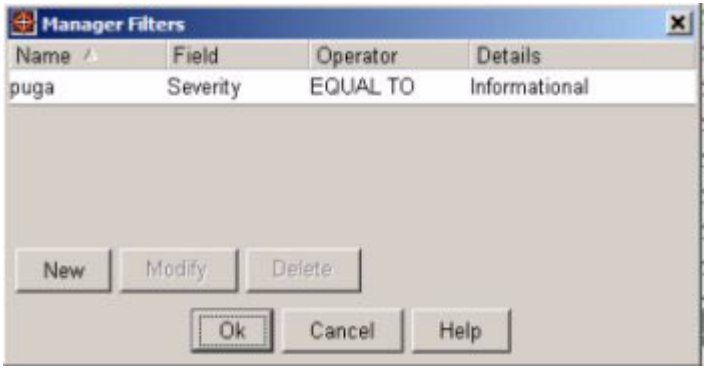
Deleting an event removes the event from the Events list and reduces the Event count in the IDM Dashboard window.

Using Event Filters

The events shown in the Events window can be filtered to show only specific types of events based on the device that generated the event, severity, date of occurrence, or description.

To create an event filter:

1.  Click the Configure Filters icon on the Events toolbar to display the Manage Filters window.



2. In the Manage Filters window, click "New" to display the New Filter window.

3. Click the Filter Type drop-down arrow and select the type of filter to be created. Possible types are:

Severity	Use this parameter to filter out lower or higher severity events, or to view events for only one severity level.
Source	Use this parameter to filter out events from a specific device, or to filter out all events except a specific device.
Description	Type the text for an event descriptions that you want to filter. Use this parameter to filter out events by specific event description text.
Date	Use this parameter to filter events for a specific date and time.
Status	Use this parameter to display acknowledged or unacknowledged events only. [True=acknowledged, False=unacknowledged]

4. Type in a Name for the event filter.
5. Select the Operator to be applied from the drop-down menu. The list will vary based on the filter type. The operators list includes one or more of the following:

Operator	Action
EQUAL TO	Display only events that match the criteria
NOT EQUAL TO	Do not display events that match the criteria
GREATER THAN	Display events of matching or greater value than criteria.
LESS THAN	Display events of matching or lesser value than criteria.
CONTAINS	Display only events that match criteria
DOES NOT CONTAIN	Do not display events that match criteria

6. In the Criteria field, enter the criteria used to select events. The Criteria field works in conjunction with the Operator field.

   For example, to filter out Informational events, the Filter options would look like this:

   When the filter is activated, only events with a severity greater than Informational are displayed.

NOTE: In "Severity" filters, events matching the criteria will be filtered out along with events of greater or lesser value. In "Date" filters, only events of greater or lesser value than the criteria are filtered.

7. Click Ok to save the filter definition and exit the New Filters window.

   The new filter appears in the "Manage Filters" list.

8. Click Ok to close the Manage Filters window.

9. Click "Select Filters" on the Events toolbar to display the list of filters, then click to select the filter to be applied. A check indicates the filter is "on."

To modify an event filter:

1. Click the Configure Filters icon on the Events toolbar to display the Manage Filters window.

2. In the Manage Filters window, select the filter to be modified and click "Modify" to display the Modify Filter window (similar to New Filter).

4. Modify the filter attributes.
5. Click Ok to save your changes and close the Modify Filters window.

   The changes to the filter appear in the "Manage Filters" list.
3. Click Ok to close the Manage Filters window.

To delete an event filter:

1. Click the Configure Filters icon on the Events toolbar to display the Manage Filters window.
2. In the Manage Filters window, select the filter to be deleted and click "Delete".

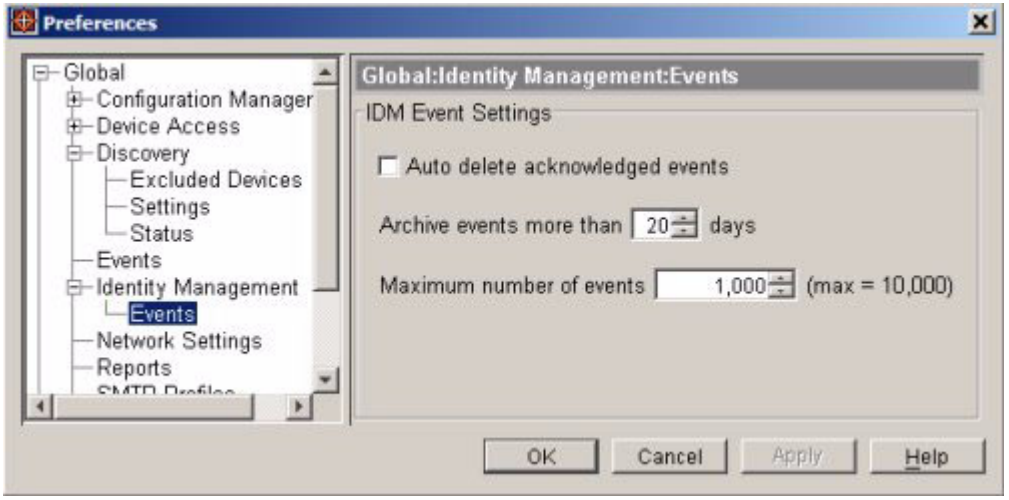
   The selected filter is deleted and the associated option is removed from the Select Filters drop-down menu on the Events tab.
5. Click Ok to exit the Manage Filters window.

Setting IDM Event Preferences

Use the IDM Event Preferences to set up archiving and automatic deletion of events from the IDM Events tab and RADIUS Server Activity Logs.

To configure preference settings for IDM events:

1. Select the Identity Management, Events option in the Global Preferences window (Tools->Preferences->Identity Management->Events) to display the IDM Events Settings window.



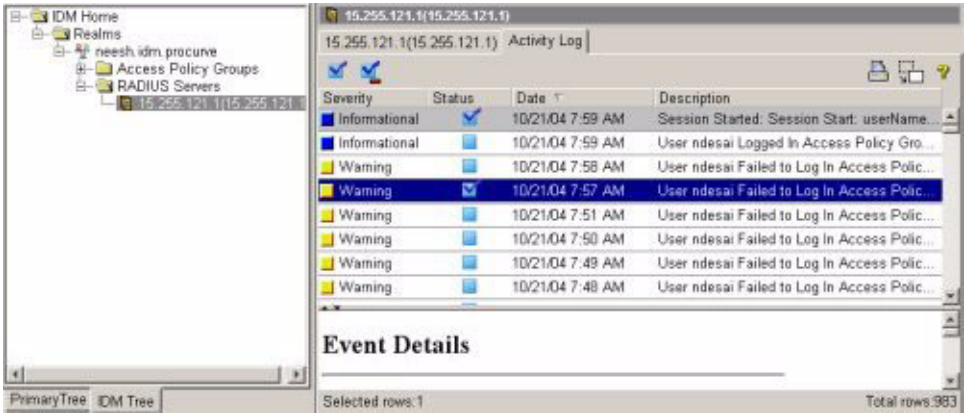
2. To delete IDM events once they are acknowledged, select the "Auto delete acknowledged events" checkbox.
3. In the Archive events more than "x" days field, click the up or down arrows or type the number of days to list events in the IDM Events window. Events are moved from the IDM Events window to the IDM Events archive when events reach the specified age.
4. In the Maximum number of events field, click the up or down arrows or type the maximum events retained before automatically archiving events. The oldest events are archived first.
5. Click Ok to save the IDM Event Settings and close the window.

IDM's event archive is /server/logs/IDMEventMgrServer-ServerArchivedEvents.log In a default installation the directory is /Program Files/Hewlett-Packard/PNM.

Using Activity Logs

IDM also provides an Activity Log you can use to monitor events for specific RADIUS servers. To view the Activity Log for a RADIUS Server,

1. Expand the IDM tree to display the RADIUS Server node.
2. Select the RADIUS server, then click the Activity Log tab.



The Activity Log provides information similar to the IDM Events, except that the entries are specific to the selected server. See "IDM Events" on page 4-2 for additional information. You can acknowledge and delete events, but you cannot "filter" entries in the Activity Log.

Using Decision Manager Tracing

IDM provides a tracing tool (DMConfig.prp) and log file (DM-IDMDM.log) to assist with troubleshooting IDM problems that may occur. These files are included on the IDM Agent when it is installed on the RADIUS server. Note that the Decision Manager (DM) is an internal component of the IDM Agent.

The default configuration has the tracing options turned off because of the performance degradation when tracing is used.

To turn on tracing, edit the DMConfig.prp file on the RADIUS server. The default directory location is \Program Files\Hewlett-Packard\PNM\agent\logs.

Available logging options in DMConfig.prp are:

Log_dm_cache = true/false: True will log IDM configuration deployment events, including the configuration file data content. The default setting is false, IDM configuration deployment logging is turned off.

Log_radius_requests = true/false: True will log RADIUS requests and the IDM agent response to RADIUS. If the request is accepted then it also logs the access policy group, policy rule and access profile that is sent to RADIUS. The default setting is false, RADIUS requests are not logged.

Log_radius_acc_events = true/false: True will log session accounting events, such as session start and stop. The default setting is false, session events are not logged.

When logging is turned on, data is sent to the DM-IDMDM.log file. The default directory location is \Program Files\Hewlett-Packard\PNM\agent\logs.

Use this file for tracing purposes, to capture the following information:

- What RADIUS requests are received and the IDM agent response to the request, including the time (in milliseconds) it took the IDM agent to serve the RADIUS request.
- A list of accounting events (like session start/stop) being sent by RADIUS to the IDM agent, and whether or not the IDM agent could post them properly to the IDM server.
- Configuration deployments to the IDM Agent, along with the actual configuration image.

(This page is intentionally unused)

IDM Technical Reference

Device Support for IDM Functionality

Due to variations in hardware and software configuration of various ProCurve Devices, not all IDM [Access Profile] features are supported on all devices. The following table indicates IDM functionality supported by ProCurve Device type.

IDM Functions: / **Device Type:**	VLAN	QoS	Bandwidth
5300xl series	X	X	X
4100gl series	X		
3400cl series	X	X	X
2600 series, 2600PWR, 2800 series	X	X	
2500 Series	X		
420 Wireless Access Point	X		

For the 2600 series, release H.08.53 (or newer) of the device software is required for QoS support in IDM.

For the 2800 series, release I.08.55 (or newer) of the device software is required for QoS support in IDM.

The 9300 series and 6100 series are not "edge" switches thus are not included in the table.

ProCurve unmanaged switches do not support IDM, including: 2700 series, 2300 series, 2124, and 408.

Best Practices

Authentication Methods

The IDM application is designed to support RADIUS server implementation with 802.1x using supplicants, as well as Web-auth and MAC-auth. However to gain the full benefits of using IDM, HP advises that you implement RADIUS using an 802.1x supplicant.

If you use Web-auth or MAC-auth, you can still use IDM to provide authorization and access control, but the user session accounting will not work. This is because current version of Web-Auth and MAC-auth do not support session accounting features on the ProCurve devices. Specifically, the switches will not report session-stop events. If you are using Web-auth or MAC-auth, it is best to turn off session accounting. See “IDM Preferences” on page 2-14 for details. The drawback is that this will also disable the IDM usage reports.

Domain Names

If you are using Active Directory, and your standard Active Directory Domain Name is different than its pre-Windows 2000 Domain Name, then these two Domain Names may appear as different Realms to IDM. This will only be true if users log into IDM using different formats (e.g. "OLDDOMAIN\user" versus "user@NewDomain"). Under most circumstances, this will never be a problem.

It is best if the Active Directory Domain Name is the same as the pre-Windows 2000 format (e.g. use simple names without special characters). However, if this is not the case, you can mitigate the problem by having users log in using a standard format (either "DOMAIN\user" or user@domain, but not both).

Multiple RADIUS Server Implementation

If you are using multiple RADIUS servers, with users logging in through each, they should be discovered by IDM. However, if one of the servers is being used as a "back-up" system (not just for load-balancing), the back-up server may not appear correctly in IDM. This is because IDM is not "aware" of the server until a user logs into it.

You can use the manual configuration method to define the RADIUS server to IDM. “Defining RADIUS Servers” on page 3-25 for details. The server will then appear in the IDM tree, and event logs for the server are available.

Handling Unknown or Unauthorized users

If a user is authenticated in RADIUS, but is unknown to IDM, IDM will not override RADIUS authentication and default switch settings, unless you configure it to do so. Also, if IDM rejects the user, but you have set "unauth-vid", then the port will still be opened and the VLAN will be set to the unauth-vid. You can also create a "guest" profile in IDM to provide limited access for unknown users.

Allowing vs. Rejecting Access

When evaluating the rules for the Access Policy Group when a user logs in, IDM is looking to match all three of the parameters (Location, Time, System). If it does not get a match on all three, it will go to the next rule in the list. When a match on all three parameters is found, the Access Profile for that rule is applied.

There are two ways to look at the process of restricting user access using Access Profiles in Access Policy Group (APG) rules.

A. Create rules that allow access.

B. Create rules that reject access.

For example, to create an APG to allow access during the standard work week, you can create a Time that defines the work week, then create an Access Policy to be applied during that time. In this example, a Default policy was created. The APG to allow user access during the work week would then look like this:

Access Policy Group Name: Group A

Location	Time	System	Access Profile
ANY	Work week	ANY	Default

Users in the group will be allowed access as long as they are logging in during the times set for the Work week. At any other time, the user will be denied access, and an IDM event will be logged for the reason that no matching rules were found in the APG.

To create a rule that denies access on the weekend, while allowing access during the work week, you will need a Time to define the weekend. You will also need an Access Policy to define the access at all other times. In the Access Profile Group, you would enter two rules, similar to the following:

Access Policy Group Name:	Group B		
Location	Time	System	Access Profile
ANY	Weekends	ANY	REJECT
ANY	ANY	ANY	Default

In this instance, if the user attempts to login in during the times specified for the Weekends, they will be rejected, and an IDM event will be logged indicating that the APG had a specific Reject rule set to deny access.

If the user logs in at times not specified for the weekend, since the time in the first rule does not match, IDM moves to the second rule. Since all parameters match, the user is allowed on the network and the "Default" Access Profile settings are applied at the switch.

The other important piece in this process is the order of the rules. In the second example, if you change the order of the rules, users would be allowed access all the time.

The two examples above are quite simple. However, in instances where you want to be able to restrict user access to specific areas of the network at specific times, or restrict network resources to users at specific times and locations, the decision to use the "allow" vs. "reject" method and the ordering of the rules becomes more complex.

Rate-Limiting

The option for rate-limiting using the Bandwidth option in Access Profiles works like this:

- When the Access Profile is applied, IDM sends a rate-limit in Kbps to the switch.
- The switch takes the value passed from IDM and converts it to a rate percentage, based on the port link speed.

If the value passed to the switch by IDM is greater than the port link speed, the switch will ignore the parameter received from IDM. To avoid problems, avoid using low rate-limit policies on the switch, or make sure that the IDM rate-limits do not exceed the link speeds of ports in your network.

Types of User Events

The USER_FAILED_LOGIN event happens whenever RADIUS sends IDM a message of an unsuccessful login. This can have various sources, which you can review in the Event Details. It can be either because IAS didn't let the user log in (bad username, password, etc.) or because IDM rejected the login.

The IDM reasons for denied access that are currently defined include:

```
//Port is missing or invalid port
public static int INVALID_PORT = 1;

//Switch information is missing or invalid switch ip address
public static int INVALID_SWITCH_IP = 2;

//User name is missing or invalid user name
public static int INVALID_USER_NAME = 3;

//Unknown Realm for DM
public static int REALM_NOT_FOUND = 4;

//Realm config data is not found in DM cache
public static int REALM_CACHE_NOT_FOUND = 5;

//Access policy group is not found for a user
public static int APG_NOT_FOUND = 6;

//An access policy group doesn't have any policy rules
public static int NO_RULES_IN_APG = 7;

//Time constraint is not satisfied
public static int TIME_DOES_NOT_PERMIT = 8;

//Location constraint is not satisfied
public static int LOCATION_DOES_NOT_PERMIT = 9;

//Unknown user to IDM DM
public static int UNKNOWN_USER = 10;

//No rules in APG can allow user to login to network
public static int NO_RULES_MATCH = 11;

//Reject profile encountered
public static int REJECT_PROFILE = 12;

//Unknown reason
public static int UNKNOWN_REASON = 20;
```

For additional information, refer to the MS IAS documentation to see what the possible values are for user logins that are rejected or failed by RADIUS

This page is intentionally unused

Index

S

T

U

W

Edition 1
Printed in Singapore December 2004
Part number: 5990-8851