ProCurve
Identity Driven Manager

Software Release 2.0

User's Guide

Publication Number

5990-8851
November, 2005

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.

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.procurve.com

Contents

3 Using Identity Driven Manager

4 Troubleshooting IDM

A IDM Technical Reference

Index

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.

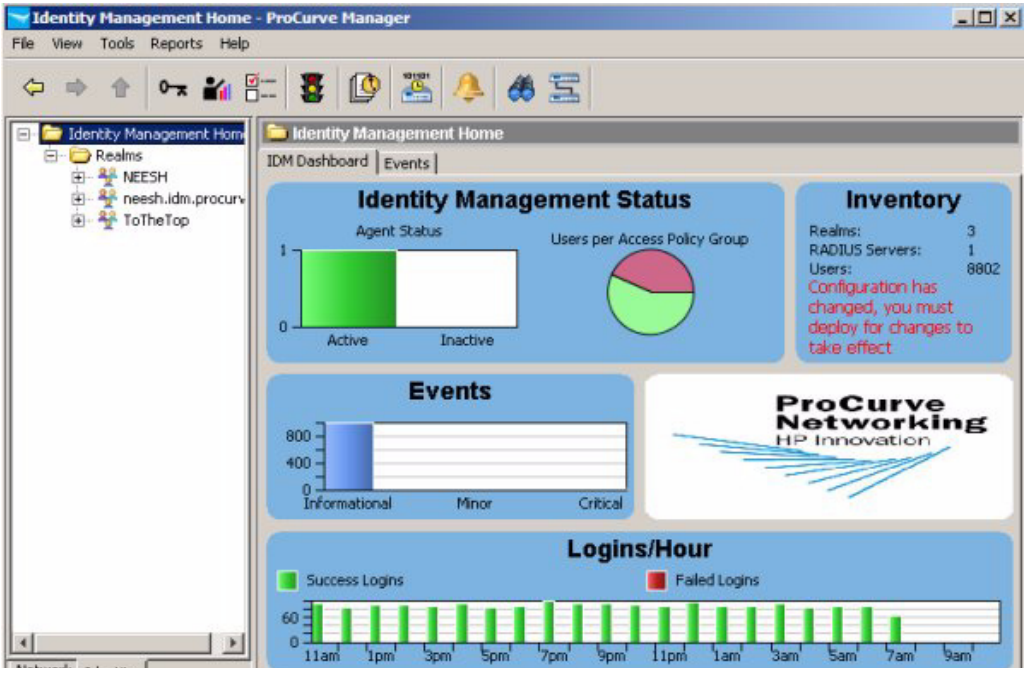


Figure 1-1. ProCurve Identity Driven Manager, Client Interface

Why IDM?

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

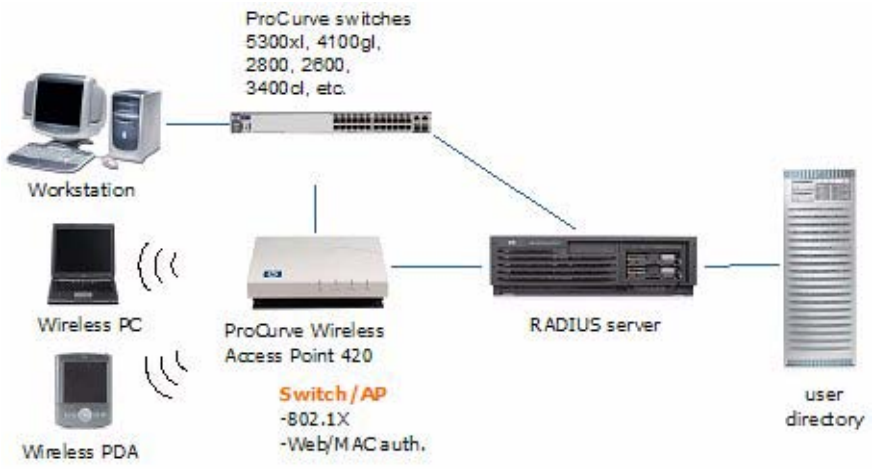


Figure 1-2. Current Access Control process

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, and what network resources the user can access 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.

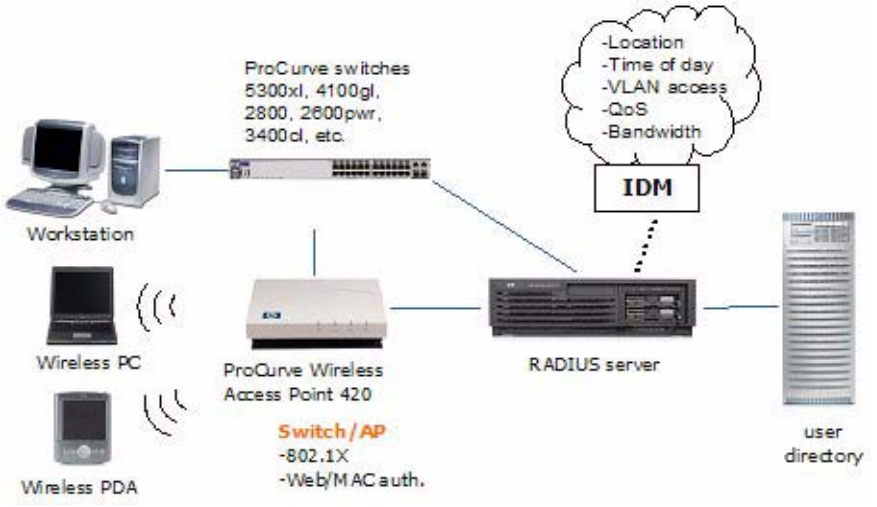


Figure 1-3. Access Control using IDM

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.

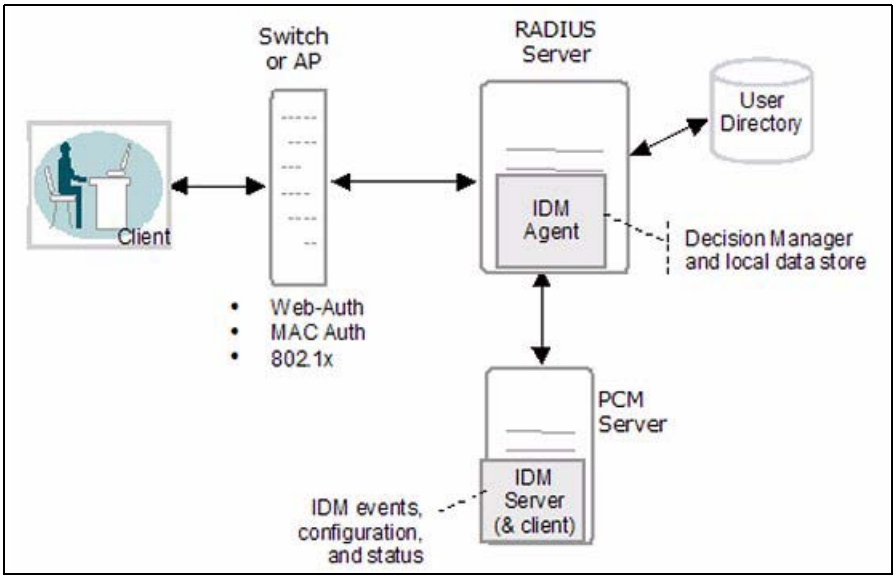


Figure 1-4. IDM Architecture

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, bandwidth, and network resource access 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, network resources, and access profiles.
- Creating access profiles that define the network resources and attributes (VLAN, QoS, bandwidth) assigned 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.

Endpoint Integrity Also referred to as "Host Integrity," this refers to the use of applications that check hosts attempting to connect to the network to ensure they meet requirements for configuration and security. Generally to make sure that virus checking and spyware applications are in place and up to date.

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, 2650-PWR, 2626-PWR, 2608-PWR, 6108)
  2500 Series (2512, 2524)
  ProCurve Wireless Access Points (420wl)
  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. (A total of 1 GB will be required for PCM+ and IDM.)
- Implementation of one of the following RADIUS services. The IDM agent will be installed on this system.
  - Microsoft's Internet Authentication Service, RADIUS authentication server on Windows 2003 Server (Enterprise or Standard Edition).
  - Funk's Steel Belted RADIUS (SBR).
- 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.

Upgrading from Previous Versions of PCM and IDM

The installation CD for PCM 2.1 contains the IDM 2.0 installation files. If you are running IDM 1.0 or 1.0.x, you must select the IDM option during the PCM 2.1 install process. This is required to support changes made in the underlying PCM and IDM databases.

If you have not purchased the IDM 2.0 license, your installation will include the IDM interface changes made for IDM 2.0, but all new functionality (FUNK SBR support, User Import/Export, Access Control, and Endpoint integrity support) will be disabled until you purchase and register an IDM 2.0 license.

If you want to test the IDM 2.0 functionality using the free 30-day trial provided on the PCM 2.1 CD, you need to install the software on a separate system that has no previous IDM version installed or in use.

When you upgrade to IDM 2.0, you need to manually install the IDM Agent upgrade on your RADIUS Server. Refer to “Installing the IDM Agent” on page 2-2 for detailed instructions.

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.

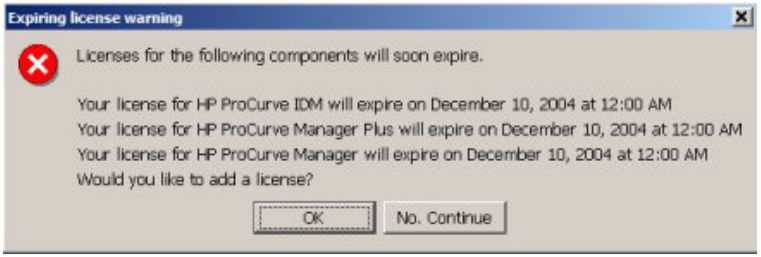


Figure 1-5. ProCurve Expiring License warning dialogue

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.*

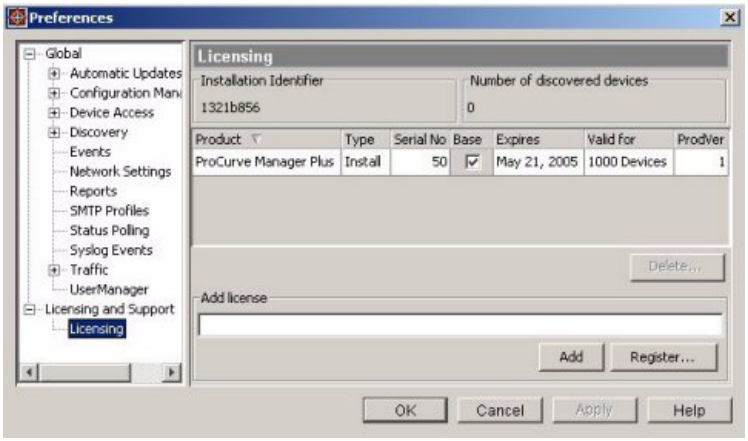


Figure 2. ProCurve License Administration dialogue

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 IDM software:

1. Contact your HP Sales Representative or HP Reseller to purchase the PCM+ and IDM software. You will receive a Registration ID for the purchased software—either on the Software CD case, or a separate registration card sent with the purchase information.
2. Go to the Licensing window in PCM [Preferences→Licensing and Support→ Licensing]. Write down the Installation Identifier for the software as it appears in the upper left corner of the window. You can also leave this window open and use the "copy and paste" functions to enter the Install ID in the My ProCurve software registration window.
3. Click the Register button to go to the PCM registration web site.
4. If this is an upgrade, log in with your My ProCurve ID and password.
   If you are a new user, click the "Register Here" button, and then enter the required information to create a user account, including user name, password, company name, and E-mail address.
5. In the Registration window:
   a. select the product to register from the Product Type pull-down menu.
   b. enter the Registration ID, found on the back of the software CD case, or on the registration card you received when you purchased the software.
   c. enter the Installation Identifier (from the Licensing window in PCM).
   d. Click the Generate License button.

The window is refreshed and the registration information, including your License key is displayed. The license key is also sent to you via e-mail.

e. To get the license key for the next software package, click Generate Another License and repeat the process in step 5, above.

6. When you receive the License key, go back to the Licensing window in PCM.

   Enter the License key number in the Add license field, then click Add.

   To avoid data entry errors, you can copy and paste the number from the e-mail or My ProCurve (My Software) Web page.

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

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.procurve.com.
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.procurve.com
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 1-9.

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 3-6)
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 3-11)
3. Define any "network resources" (systems and applications) that you want to specifically allow or restrict users from accessing.
4. 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 3-48)

5. Create the Access Profiles, to set the VLAN, QoS, rate-limits (bandwidth) attributes, and the network resources that are available, to users in an Access Policy Group. (See page 3-23)
6. 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 3-32)
7. Assign Users to the appropriate Access Policy Group. (See page 3-38)
8. Deploy the configuration policies to the IDM Agent on the RADIUS server. (See page 3-42)

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.

Authenticate	Authorize				Strategy Description
	VLAN	QoS	Rate-Limit	Network Resources	
					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	x	VLAN, QoS, and Rate-limit attributes, and accessibility of defined Network Resources for all users, based on Location, Time, and System

Table 2-1: 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.

The basic operational 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.

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

The IDM configuration tools are available at the top level. The definition of times, locations, network resources, and access profiles is independent of individual Realms or Groups. You can define multiple locations, times, and network resources, then create multiple access profiles to be applied to any Access Policy Group, in any Realm that exists within IDM.

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.

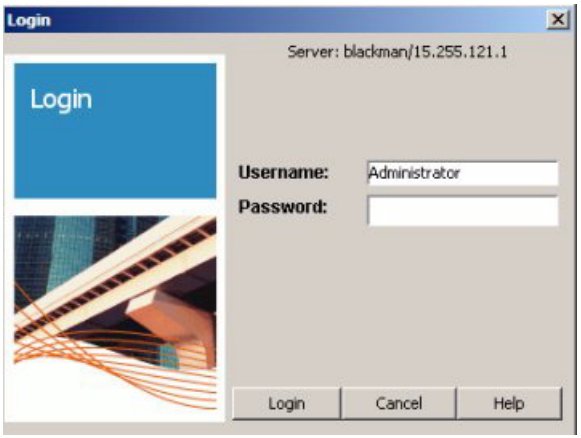


Figure 2-1. PCM Client Login dialogue.

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.

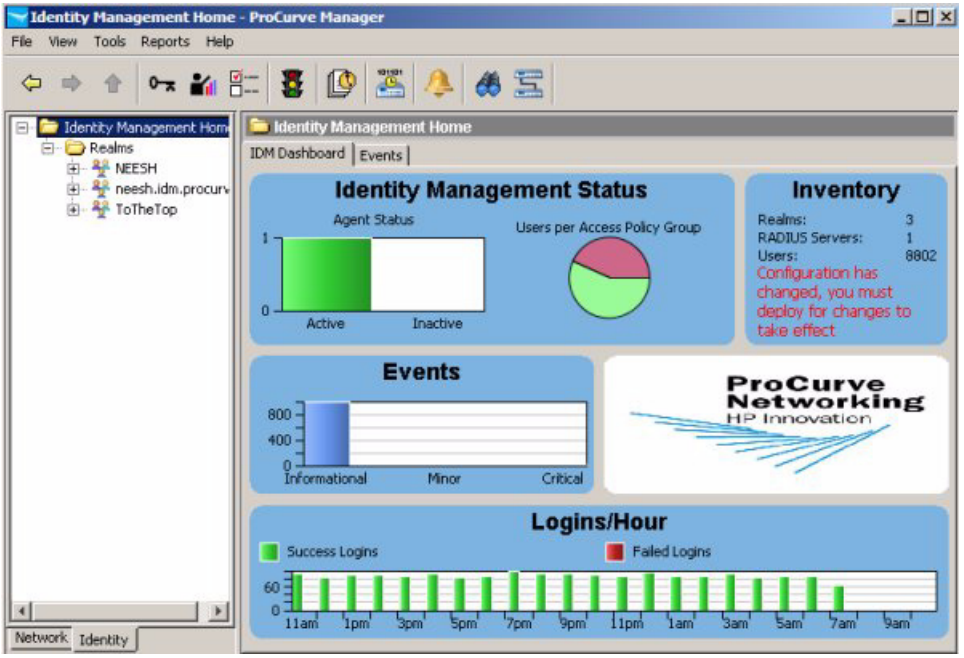


Figure 2-2. IDM Home Window

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 Identity Management Home window frame.

NOTE:

If the IDM 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 entry:
  "PCM remote client authentication failure: <*ip address*>"
- Check for IDM application events related to devices "supporting" or "not supporting" the configuration.
- 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.

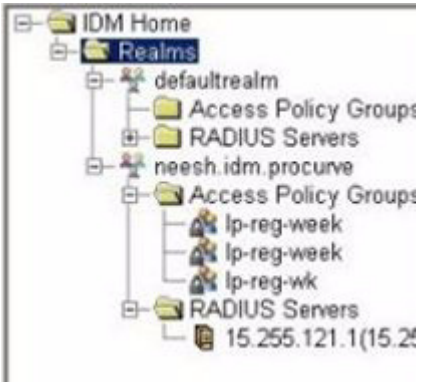
Inventory: The Inventory panel lists the current number of Realms, RADIUS Servers, Users, Access Policy Groups, Access Profiles, Locations, and Times that are defined in IDM.

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 per Hour panel is a scrolling 24-hour display that summarizes the total number of successful and failed IDM user logins at any given time during the past 24 hours. Information in this panel is updated every minute 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. Click the nodes to expand the list and change the display in the right window panel.



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.

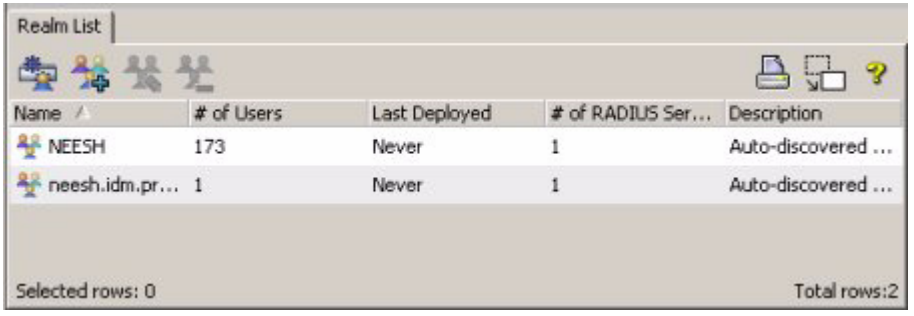


Figure 2-3. Realms List tab

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.

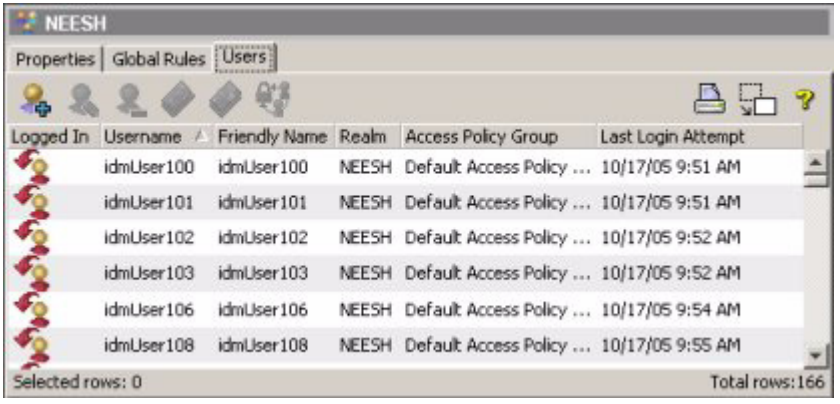


Figure 2-5. Realm Users tab

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 group's Properties.

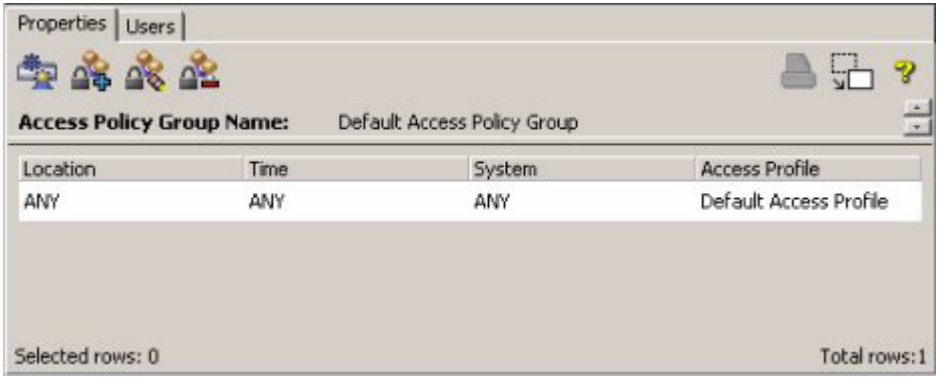


Figure 2-7. Access Policy Group Properties tab

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.

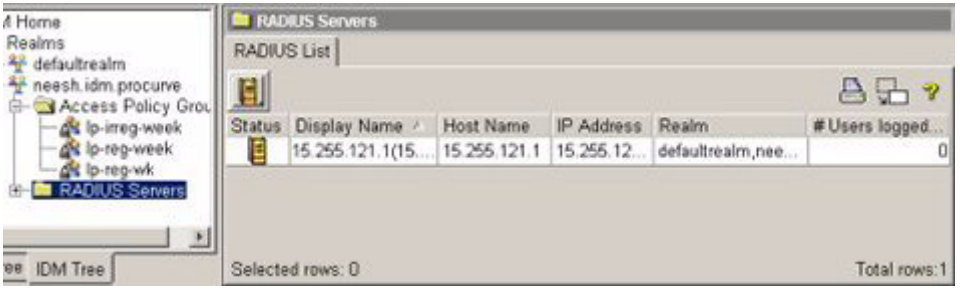


Figure 2-8. RADIUS List tab

NOTE:

If the RADIUS server is not in the IDM tree, check in the PCM Events for the following message: "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 window displays.

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

Whether or not you configure and apply access and authorization parameters using IDM, you can use IDM to monitor user sessions on the network and generate usage reports. You can use the monitoring features along with the IDM Reports to track usage patterns, user session statistics, bandwidth usage, top users, and so on. The User session information can also be used to track current user sessions and modify the User's access to network resources if needed.

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.

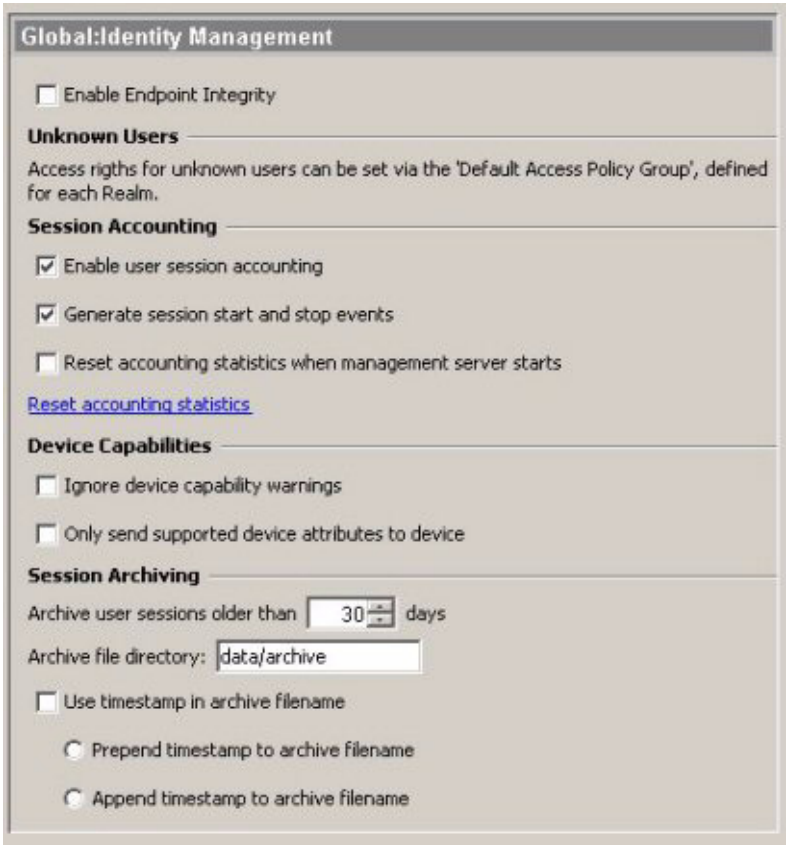
You can enable or disable IDM monitoring using the IDM Preferences. Using the IDM Preferences, you can also configure IDM to work with existing "Endpoint Integrity" applications used to determine the compliance of the authenticating clients to rules and requirements (for firewalls, anti-virus, etc.) that have been set up in the domain.

NOTE: If you are using Web-Auth or MAC-Auth for user authentication, user session statistics are unavailable from the switch and cannot be collected, unless you are using a version of firmware on the switch that supports accounting for Web-Auth and MAC-Auth sessions. Currently, only the latest versions of the 5300 support this; check the ProCurve web site for updates.

IDM Preferences

The IDM Preferences window is used to set up global attributes for session accounting and archiving, as well as enabling the Endpoint Integrity option.

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



Click on the option check boxes to select (check) or deselect (blank) the option.

1. To enable Endpoint integrity, check the **Enable Endpoint Integrity** checkbox. This will enable the Endpoint Integrity option in the Access Rules definitions, and you can configure an Access Rule with one of the Endpoint Integrity options (Pass, Fail or ANY). When you enable Endpoint Integrity and set the attribute in a Global Access Rule or Access Policy Group rule,

the IDM agent will look for the RADIUS attribute in the supplicant's authentication request and act accordingly, applying the defined access rule based on the endpoint integrity system response.

2. To collect information about user logins and logouts, check the **Enable User session accounting** checkbox. This box must be checked if you want to collect data for user logins and bandwidth usage, which is used for the Bandwidth and User reports.

3. To generate user session start and stop events and display them in the IDM Events list, check the **Generate Session Start and Stop Events** box. This option does not affect accounting or collection of session history and statistical information. Turning this option off will reduce the load on your IDM server and the GUI by eliminating two-thirds of the events created for every user login and logout.

4. To reset all session accounting information whenever the server is restarted, check the **Reset accounting statistics when the management server** starts box. When this option is selected, IDM closes any open sessions and resets the RADIUS Server totals to zero when the server restarts.

   If the status of users—logged on or off—seems incorrect, it is possible that the session accounting is out of sync. Use the **Reset accounting statistics** option to correct the problem. This immediately closes any open sessions (this has no effect on the user, only on the IDM accounting), and resets user login counts on the RADIUS server to zero.

   Existing accounting records are not removed by the Reset procedures, the only effect is that currently open sessions are closed.

5. To ignore capability override warnings generated by switches that don't support certain capabilities (e.g., VLAN, QoS, Bandwidth, and ACL overrides), check the I**gnore device capability warnings** checkbox.

6. To send only those attributes supported by the device, check the **Only send supported device attributes to device** checkbox.

7. If you wish to archive accounting records older than a specified time period, uncheck the **Disable session archiving** box, and set the desired archival time period in the **Archive user sessions older than** *x* **days** field.

8. To archive the user session archive file in a location other than the default IDM data archive directory, type the desired path in the Archive file directory field. The default path is:

   C:\Program Files\Hewlett-Packard\PNM\server\idm\data

9. If you do not want to add a timestamp to the archive filename, uncheck the **Use timestamp in archive filename** option.

   If a timestamp is not used in the archive filename, the existing archive file is overwritten each time user sessions are archived.

   a. To insert a timestamp in the front of the archive filename, check the **Prepend timestamp to archive filename** option.

   b. To add a timestamp to the end of the archive filename, check the **Append timestamp to archive filename** option.

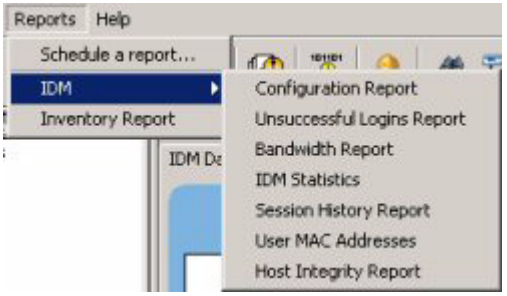
10. Click **Ok** to save your changes and exit the window.

    Click Apply to save your changes and leave the Preferences window open.

    Click Cancel to close the window without saving changes.

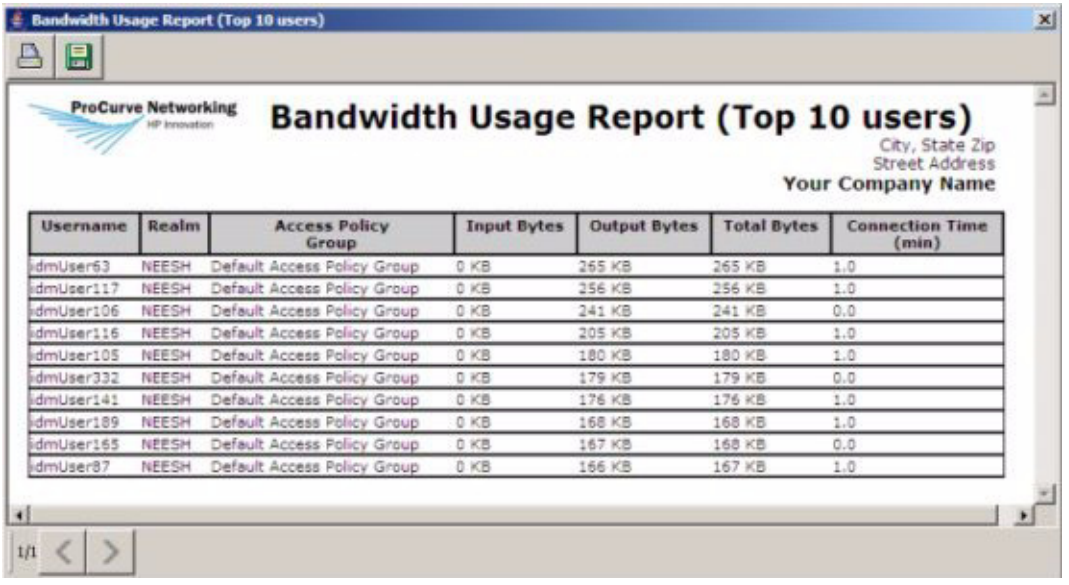
Using IDM Reports

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



The Report wizard screens and report parameters vary, depending on the type of report selected.

When you select a report using the IDM Reports sub-menu, the Report wizard is launched. Use the wizard to set filter options, and selectable data elements. When you click **Finish**, the report is generated and the output displays on the IDM Client, similar to the following example:



Username	Realm	Access Policy Group	Input Bytes	Output Bytes	Total Bytes	Connection Time (min)
idmUser63	NEESH	Default Access Policy Group	0 KB	265 KB	265 KB	1.0
idmUser117	NEESH	Default Access Policy Group	0 KB	256 KB	256 KB	1.0
idmUser106	NEESH	Default Access Policy Group	0 KB	241 KB	241 KB	0.0
idmUser116	NEESH	Default Access Policy Group	0 KB	205 KB	205 KB	1.0
idmUser105	NEESH	Default Access Policy Group	0 KB	180 KB	180 KB	1.0
idmUser332	NEESH	Default Access Policy Group	0 KB	179 KB	179 KB	0.0
idmUser141	NEESH	Default Access Policy Group	0 KB	176 KB	176 KB	1.0
idmUser189	NEESH	Default Access Policy Group	0 KB	168 KB	168 KB	1.0
idmUser165	NEESH	Default Access Policy Group	0 KB	167 KB	168 KB	0.0
idmUser87	NEESH	Default Access Policy Group	0 KB	166 KB	167 KB	1.0

You can save the report to a file, or print the report. To apply customized Report Header information for your company, use the Reports option in the global preferences. (Tools–> Preferences–> Global–> Reports)

The Schedule a report option in the Tools menu launches the Schedule Reports Policy Wizard, which lets you schedule reports to be created at recurring intervals.

Each of the available reports is summarized below, along with the report filter options, and configurable report parameters, if applicable.

Configuration Report: The Configuration Report provides information describing the configuration of the IDM systems, including: Realms, RADIUS servers, Access Profiles, and Users configured in IDM. Each category is listed on a separate page. You can filter out the User configurations in the report.

Unsuccessful Login Report: The Unsuccessful Login Report lists failed system logins, which can be filtered by date. The report includes the following information:

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.

Bandwidth Usage Report: The Bandwidth Usage Report lists bandwidth usage per User. the top 25 bandwidth users. You can filter the report to show results by top Users, dates, Realm, and Access Policy Group. This report is helpful in identifying candidates for throttling.

Note: You must have the Enable user session accounting option selected in the IDM Preferences in order to collect Bandwidth and other user session data for reports

The following information is provided for each user included in the Bandwidth Usage report:

Username	Username used to login
Realm	Realm (Access Policy Group and RADIUS server) to which the user is assigned
Access Policy Group	Access Policy Group governing a user's login to the RADIUS server
Input Bytes **Output Bytes** **Total Bytes**	The number of bytes (KB) processed during the User's session, indicating the bandwidth usage for that user.
Connection Time	Length of time the user was connected (in minutes) for the session.

IDM Statistics: The IDM Statistics report provides information on the number of logins, input bytes and output bytes, by day and hour. You can filter the report by configuring it for any one, or combination of: Realm, Access Policy Group, and Location.

Session History: The Session History Report provides details on user sessions. You can filter the report by configuring it for any one, or combination of: dates, Realm, Access Policy Group, and Location. You can also filter the report to show the top results by bandwidth only.

Once the initial report dates and filters are set, you can also configure what columns you want to include in the report. The available column headings include:

RADIUS Server IP	Location
MAC Address	Device
Device Port	VLAN
QOS	Endpoint Integrity State
BW (Bandwidth)	

User MAC Addresses: The User MAC Addresses provides a listing of MAC Addresses in use, and allowed for use by Access Policy Group and User. You can filter the report to get data for any one, or combination of Realm and Access Policy Group.

Endpoint Integrity State: The Endpoint Integrity State report collects data on the Endpoint Integrity State for users along with the date, and Access Profile used. This report lets you see which User's systems are compliant with your host integrity solution. You can filter the report by date, and by one or more of the following "**State**" types: Failed, Passed, and Unknown.

User Report: The User Report lists information for recent sessions in which the user participated, similar to the Session History report.

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.

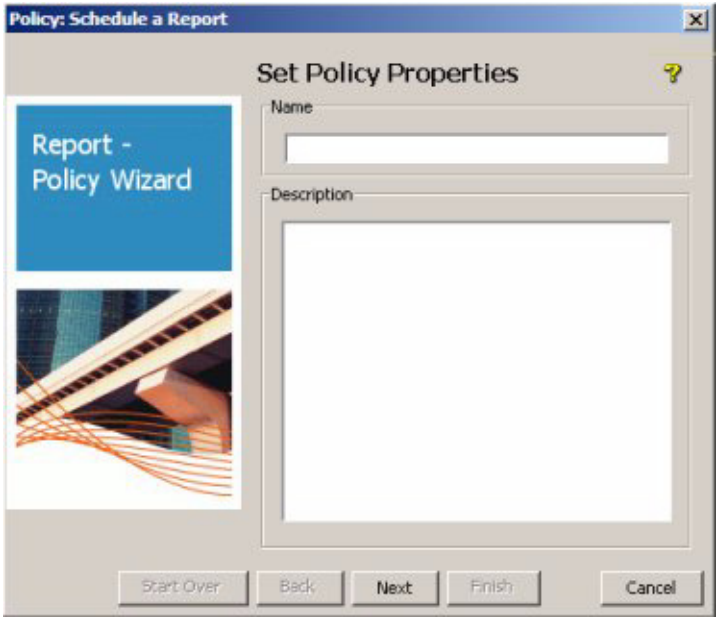
Scheduling a Report

To schedule a report:

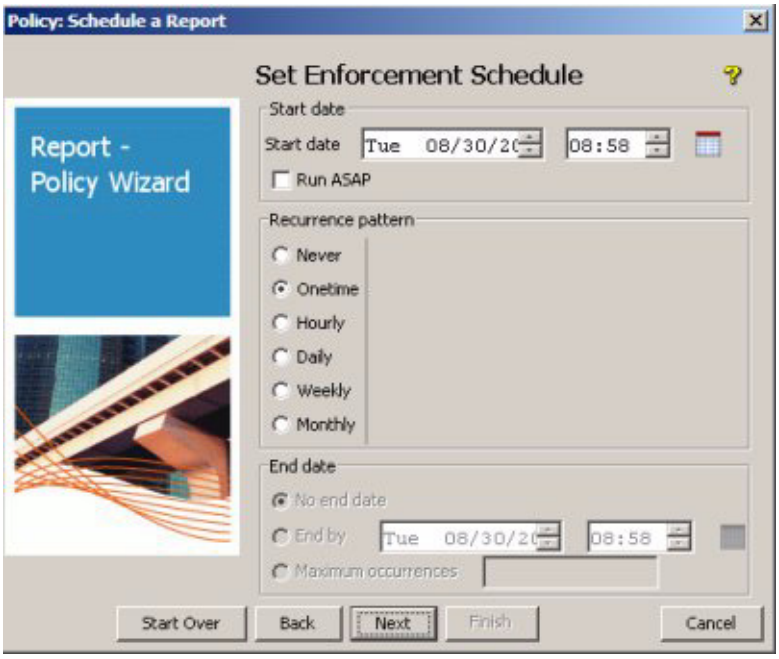
1. From the global toolbar select Reports–>Schedule a Report... option to launch the Report Scheduling Wizard.

   The Report Scheduling wizard works in the same manner as a policy (see "Creating a Policy" in Chapter 10 of the *ProCurve Manager Network Administrator's Guide*), guiding you through the following steps:

2. Enter a **Name** and **Description** for the report in the Set Policy Properties window



3. Click **Next** to continue to the Set Enforcement Schedule window.
4. Set the Enforcement Schedule for running the report. You can create a recurring schedule (daily, weekly, monthly) for running the report

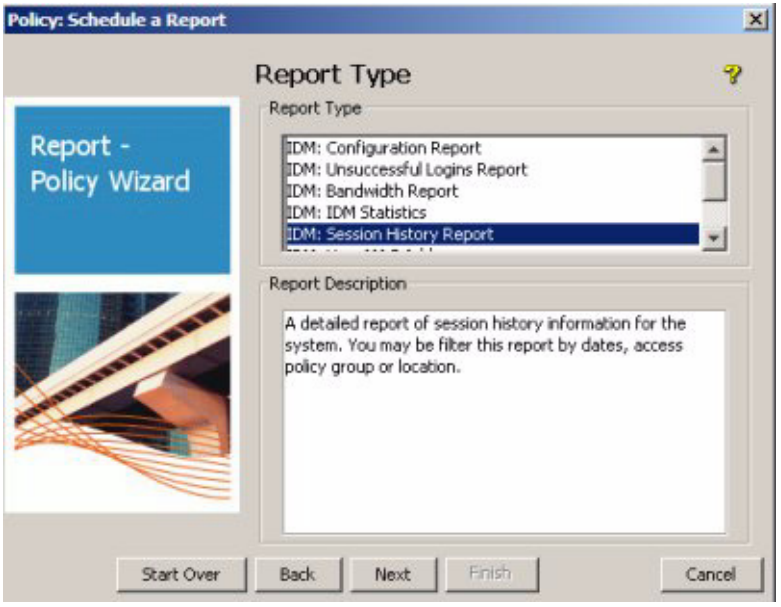


a. Enter the **Start date** and time.

b. Click one of the radio buttons to select the **Recurrence Pattern.**

c. Click to select the **End date** option. Enter the End by date and time, and Maximum occurrences as needed.

d. Click **Next** to continue to the Report Type window.

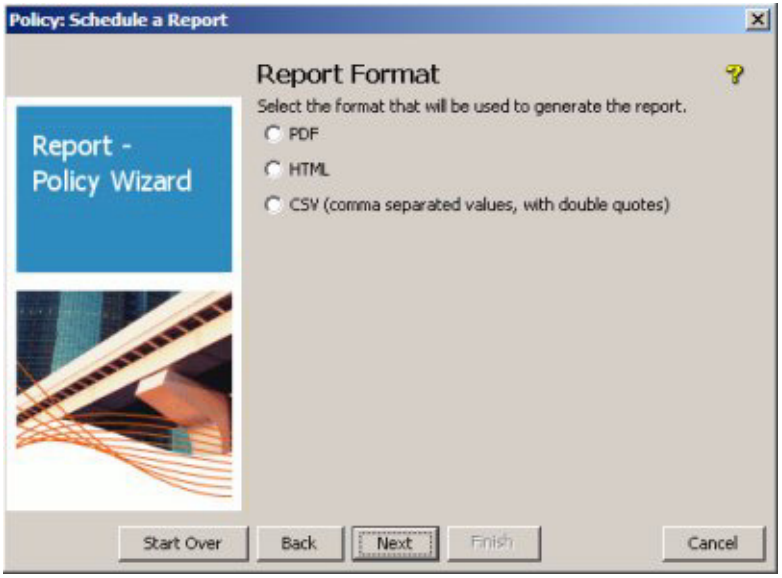


5. Click to select the Report Type from the list.
6. Click **Next** to continue to the Report Filter window.

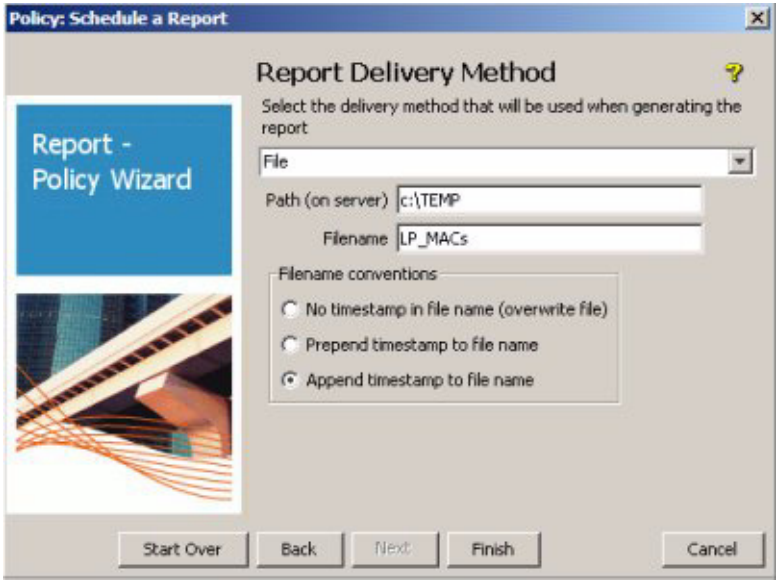
.

7. Depending on the report type, select the **Report Filters**, to configure what data is included in the report. For most reports you can filter by one or more or the following: Dates, Realms, Access Policy Group, Location, or Users
   a. Use the **All Dates** option to set the **Start Date** and **End Date** for data to be included in the report.
      The default report dates are 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.
   b. For some reports, such as IDM Session History, you also configure the data columns to be included in the report output.

8. Click **Next** to continue to the Report Format window.



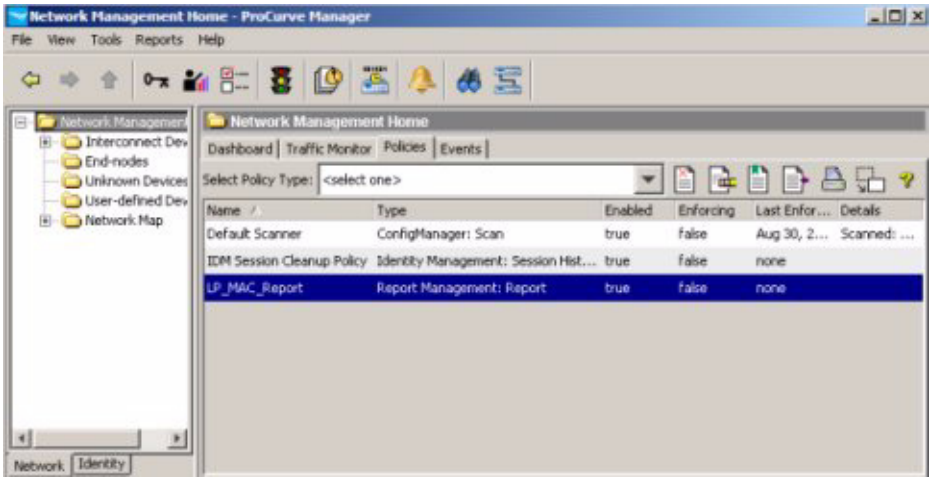
9. Click the radio button to select the Report Format for output: **PDF**, **HTML**, or **CSV** (comma separated values).
10. Click **Next** to continue to the Report Delivery Method window.



11. Select the Delivery method: FTP, File, or Email from the pull-down menu. Then set the parameters needed to define the delivery option (FTP server, filename and path etc.) The wizard displays data entry fields for the selected delivery method.

    In order to use the Email delivery option, you must add an SMTP Profile in the Preferences, as described under "Adding SMTP Profiles" on page 5-26 of the *ProCurve Manager Network Administrator's Guide*.

    Scheduled Reports appear in the PCM Policies list



To edit the report policy:

1. Select the report in the Policies list, then click the edit icon in the toolbar to launch the report wizard.
2. Edit the report parameters, and the report schedule as needed.

To delete the report policy:

1. Select the report in the Policies list, then click the delete icon in the toolbar.
2. Click **Yes** in the confirmation pop-up to remove the report policy.

NOTE: Report output is limited to 40 pages. Therefore, to create a report on many (1000+) items, you need to create separate reports to generate all the data.

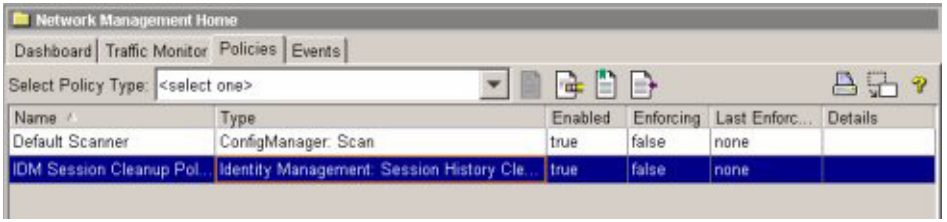
You can access User Reports by right-clicking on the user in the Users tab display in IDM, then select the report option.

IDM Session Cleanup Policy

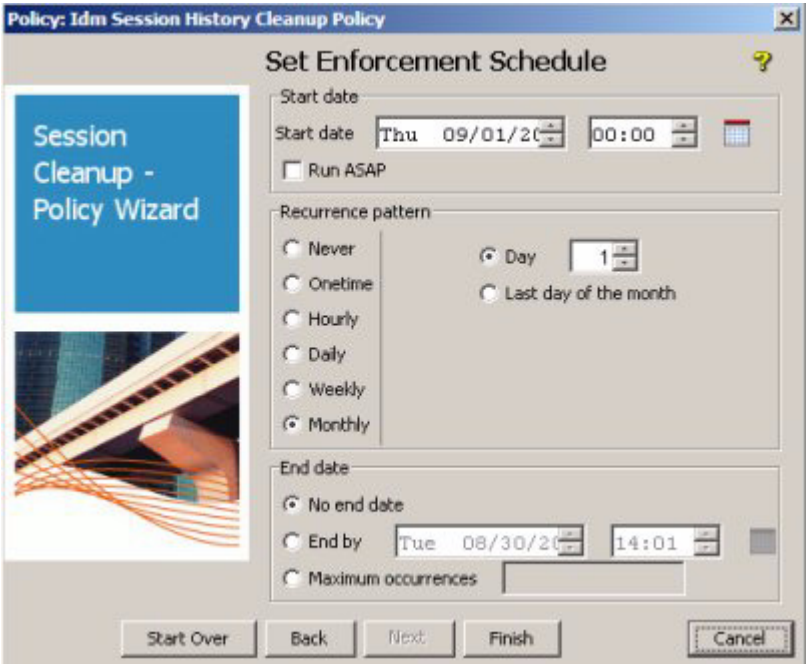
The IDM Session Cleanup Policy is included in the PCM+ policies by default when you install IDM. The report statistics IDM reports are cleared by the Session Statistics Cleanup policy (in PCM) on the first day of each month. You can edit the policy if you want to change the cleanup recurrence schedule.

To modify the IDM Session Cleanup Policy:

1. Click the Policies icon in the global (PCM and IDM) toolbar at the top of the window to display the list of Policies in PCM.



2. Select the IDM Session Cleanup Policy and click the modify icon in the toolbar to start the policy wizard.
3. Click **Next** to continue to the Set Enforcement Schedule window.



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:

Table 9-1. 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.

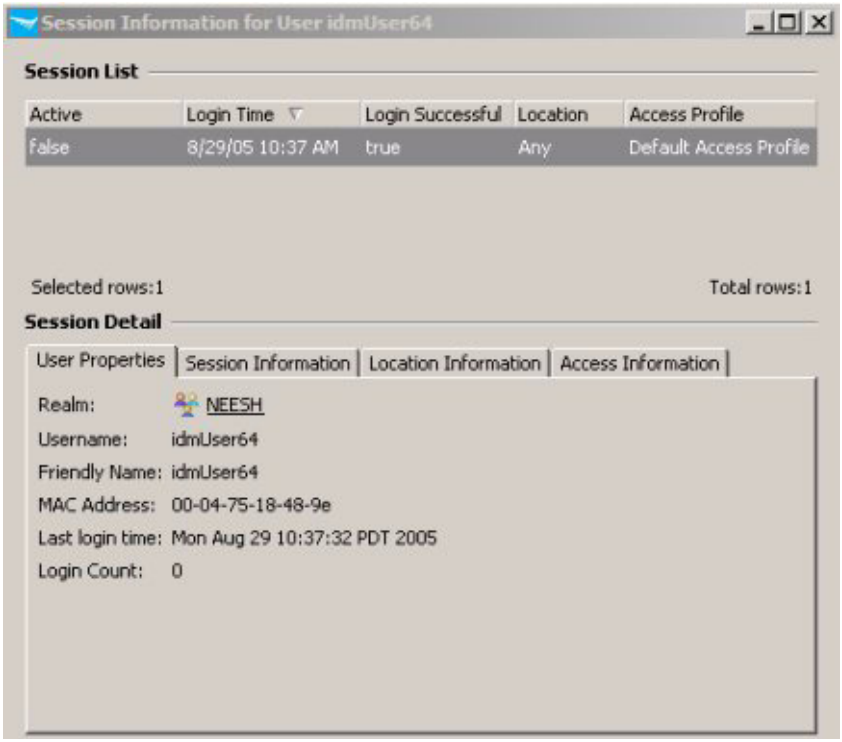
7. Click **Finish** to complete the process and exit the wizard.

User Session Information

You can use IDM to just monitor the network, and receive detailed information about user's access to the network. The User Session information provides statistics about exactly *how* the network is being used (when the user logged in and out, where a user logged in from, and how much bandwidth they consumed, for example). Based on the User Session information, you can adjust access rights for users, further restricting or providing additional network resources and access attributes as needed.

To review user session information,

1. Navigate to the Realm the user belongs to, and display the Users tab.
2. Click the Session Information tab in the Users tab toolbar to display the Session Information window.



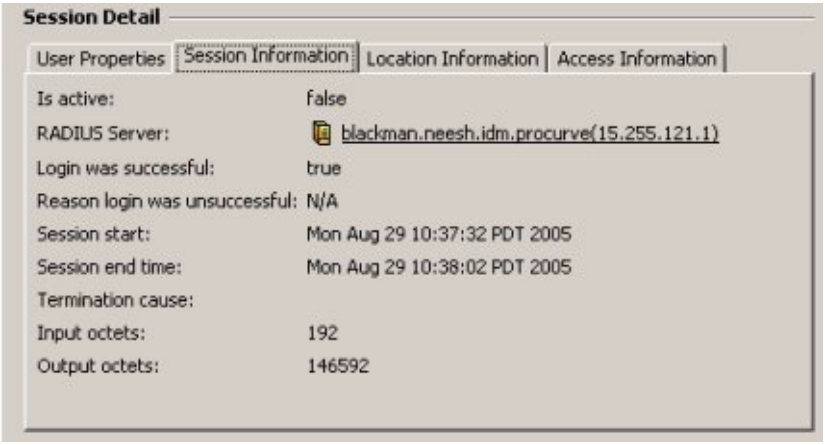
The Session List provides a listing of recent sessions, including the following information:

Active	True if the user is currently logged in for this session or False if the session has ended
Login Time	Date and time the user logged in
Login Successful	True if the user logged in successfully or False if login failed
Location	Name of the location where the user logged in
Access Profile	Access profile assigned to the access policy group governing the user's permissions during the session

The User Properties tab of the User Status window contains the following information:

Realm	Realm to which the user is currently assigned.
Username	Username used to login
Friendly Name	Name of the user to which the username is assigned
MAC Address	MAC address of the computer where the user logged in
Last login time	Date and time of the most recent user login
Login Count	Total number of times the user logged in during the report period.

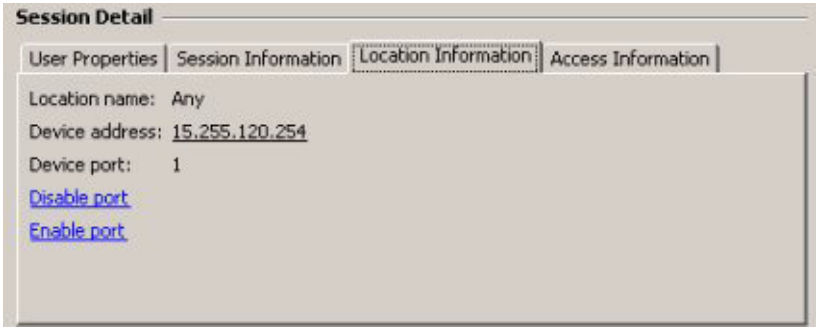
Click the Session Information tab to view additional user session information.



The Session Information tab of the User Status window contains the following information:

Is Active	True if the user is currently logged in for this session or False if the session has ended
RADIUS Server	IP address of the RADIUS server that authenticated the user
Login was successful	True if the user logged in successfully or False if login failed
Reason login was unsuccessful	If the login was unsuccessful, the reason the RADIUS server or IDM denied the login (e.g., access policy group not found for user or username/password incorrect)
Session start	Date and time the user logged in
Session end time	Date and time the user logged out or the session was ended
Termination cause	Reason the RADIUS server ended the session (e.g., user logout, connection interruption, or idle timer expiration)
Input octets	Bytes received by the user during the session
Output octets	Bytes sent by the user during the session

To track the user's login location information for the session, click the Location Information tab.

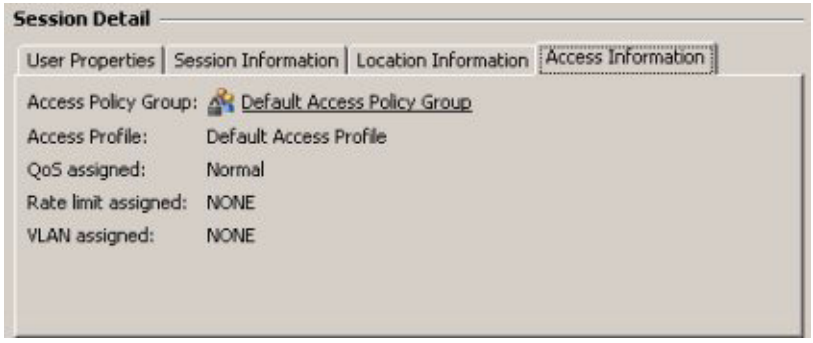


The Location Information tab of the User Status window contains the following information:

Location name	Name of the location where the user logged in
Device address	IP address of the device used to login
Device port	Port on the device used for the session

Click the **Disable port** or **Enable port** links to disable or re-enable the port used for the session. For example, if you want to prevent the user from logging in at a specific device or force the user to re-authenticate, you would use the Disable port function. If you need to re-enable the port so the user can resume the session, use the Enable port function.

Click the Access Information tab to display details about the access attributes applied to the user session.



The Access Information tab of the User Status window contains the following information:

Access Policy Group	Access policy group that governs user permissions for the session.
Access Profile	Access profile assigned to the access policy group.
QoS assigned	Quality of service or priority for outbound traffic. QoS ranges from lowest to highest.
Rate limit assigned	Maximum bandwidth allocated to user by the access profile.
VLAN assigned	The VLAN to which access is given. The DEFAULT_VLAN(1) is equivalent to allowing access on the entire network.
ACL	The access control rules that were applied to the user's session on the switch or access point.

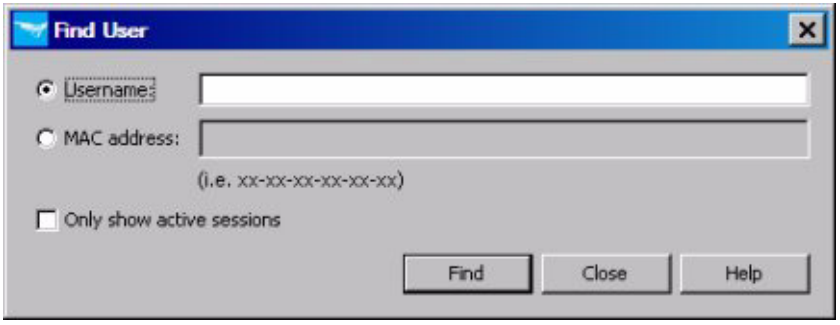
Finding a User

The Find User feature lets you search for and display information about a user by name or MAC address. The displayed information is similar to User Session Status information.

To find information for a user or MAC address:

1. In the IDM navigation tree, right-click the Realms or Access Policy Groups folder to which the user or computer is assigned. Select Find User from the right-click menu.

   This launches the Find User window.



2. In the **Username** field, type the complete user name of the user you want to find and display information (This field is not case-sensitive.),

   OR

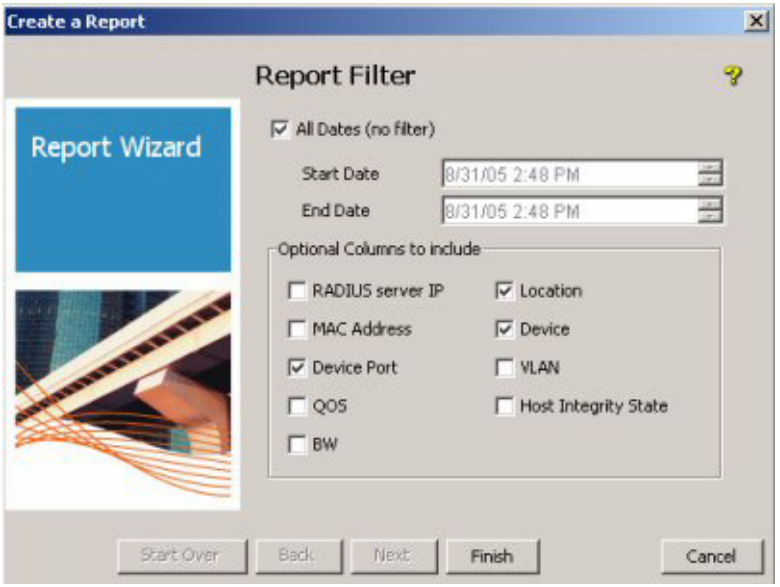
In the **MAC address** field, type the MAC address of the computer for which you want to find and display information. The MAC address can be separated by a vertical bar (|), hyphen, or colon or typed with no spaces.

3. Click the **Only show active sessions** checkbox to get only the information on active sessions for the user.
4. Click **Find** to display information for the specified user or computer.
5. Click **Close** to exit the window.

User Reports

To review information for multiple sessions, run the User Report.

1. Select a username in the Users tab of the Access Policy Group or RADIUS Server window.
2.  Click the User Report icon in the toolbar. This launches the Report Wizard, Report Filter window.



3. Click the check boxes to select the data columns.
4. Click **Finish** to run the report.

The report is displayed in a separate window on the IDM Client.

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 four 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 access provided to the network once the user is authenticated, including:

- VLAN—what VLANs the user can access.
- QoS—"Quality of Service," from lowest to highest.
- Rate-limits—bandwidth that is available for the user.
- Network Resources—resources the user can access, by IP address and/or protocol. These resources must be defined, similarly to the Locations and Times used in the access rules.

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 one 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, based on the system they use to access the network, you need to modify the User profile to include the MAC address for each system from which the user is allowed to login.
4. Define the Network Resources that users will have access to, or will be denied from using, if applicable.
5. Create the Access Profiles to set the VLAN, QoS, rate-limits (Bandwidth), and network resources that are applied to users in Access Policy Groups.
6. Create the Access Policy Groups, with rules containing the Location, Time, System, and Access Profile that will be applied to users when they login.
7. 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 Identity Management

All of the elements described for configuring user access in IDM are available in the Identity Management Configuration window.

To launch the Identity Management Configuration window:

1. Right-click on the Identity Management navigation tree, and select the **Configure Identity Management...** option from the menu, or

2. Click the Configure Identity Management icon in the Realms window toolbar.

The Identity Management Configuration default display is the Access Profiles pane with the Default Access Profile.

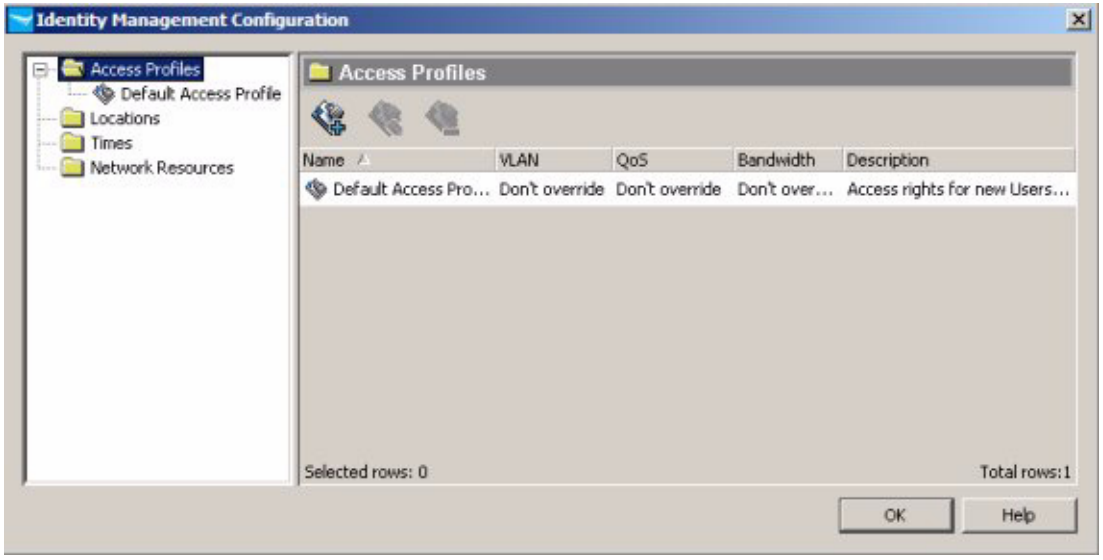


Figure 3-1. Identity Management Configuration, default display

Click the node in the navigation tree to display the defined configuration parameters and add or edit new configuration parameters, as described in the following sections.

Configuring Locations

Locations in IDM identify the switch and/or ports on the switch and wireless access points where users connect to the network. 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 configure a location:

1. Click the Locations node in the Identity Management Configuration navigation tree to display the Locations panel.

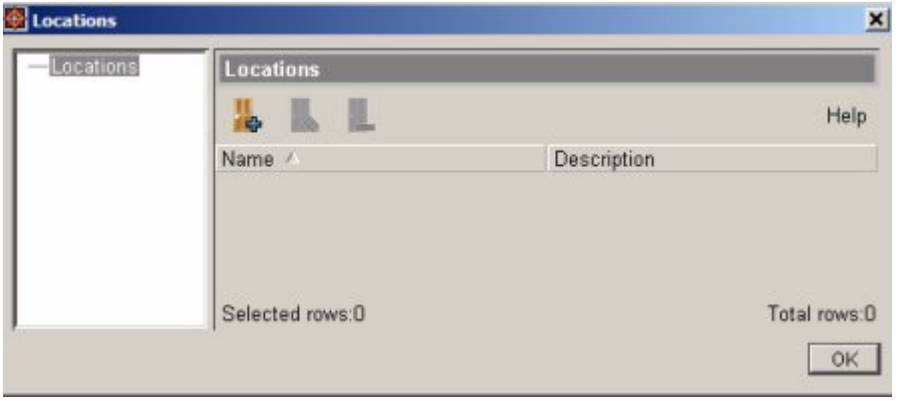
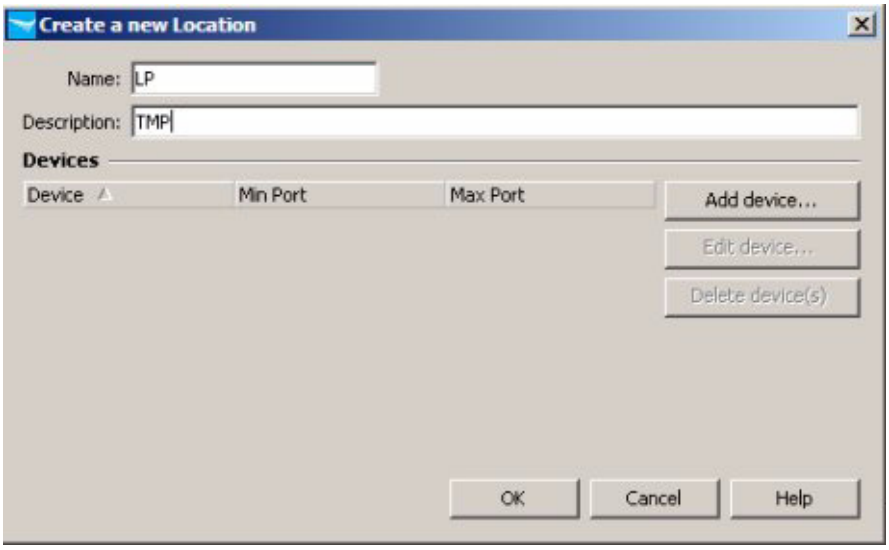


Figure 3-2. Locations panel

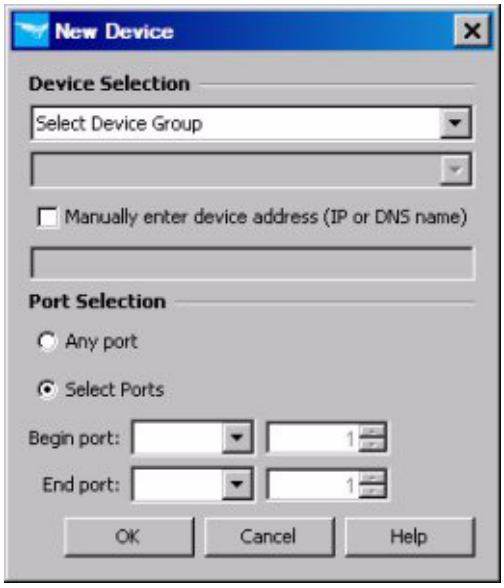
Adding a New Location

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 **Add device...** to open the New Device window, and define the devices and/or port combinations that will be included in the location.



5. Enter the Device to be added using the **Device Selection** pull-downs, or select the **Manually enter device address** option.

   Using the Device Selection option:

   a. Select a device group using the pull-down menu. This will enable the Select Device pull-down menu in the next field.

   b. Select a device from the pull-down list of available devices. The list is populated with the IP address or DNS name for all (PCM managed) devices in the selected group.

   Using the Manually enter device address option:

   a. Click the check box to enable the data entry field below it.

   b. Type in the IP address or DNS name of the device to be added.

6. Use the **Port Selection** to define the ports on the device that will be associated with the location.

   - Click to select **Any port** on the switch, or
   - Click **Select ports**, then use the pull down lists to select the **Begin** and **End** ports on the device that will be associated with the new location.

     If you manually entered the device address, the Begin port and End port pull-down menus are disabled, and you must manually enter the ports.

7. Click **Ok** to save the New Device settings to the Location, and close the window.

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 and if the device uses industry standard RADIUS protocols, the settings should work; however, HP does not provide support for IDM configurations with non-ProCurve devices.

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 Locations node in the Identity Management Configuration navigation tree to display the Locations panel, with the list of defined locations.
2. Double-click on a location in the navigation tree, or in the Locations list to open the (modify) location panel.

   You can also select the location in the list, then click the Edit Location icon in the toolbar to display the Location in edit mode
3. Edit the location **Name** and **Description** as needed.
4. To edit the device configuration for the location
   - To Modify the device settings, select the device in the list, then click **Edit 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 Location panel.
   - To add another device, click **Add Device**.
   - To delete a device, select the device in the list, then click **Delete Device**.
5. Click **OK** to save the location changes and close the 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 Locations node in the Identity Management Configuration navigation tree to display the Locations panel, 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.

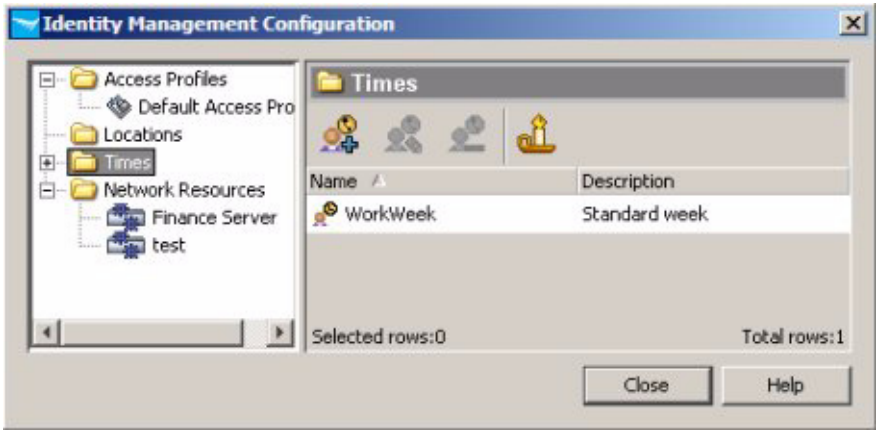
NOTE: If you modify or delete a Location, check to make sure that the changes do not adversely affect users in Access Policy Groups where the Location is used.

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.

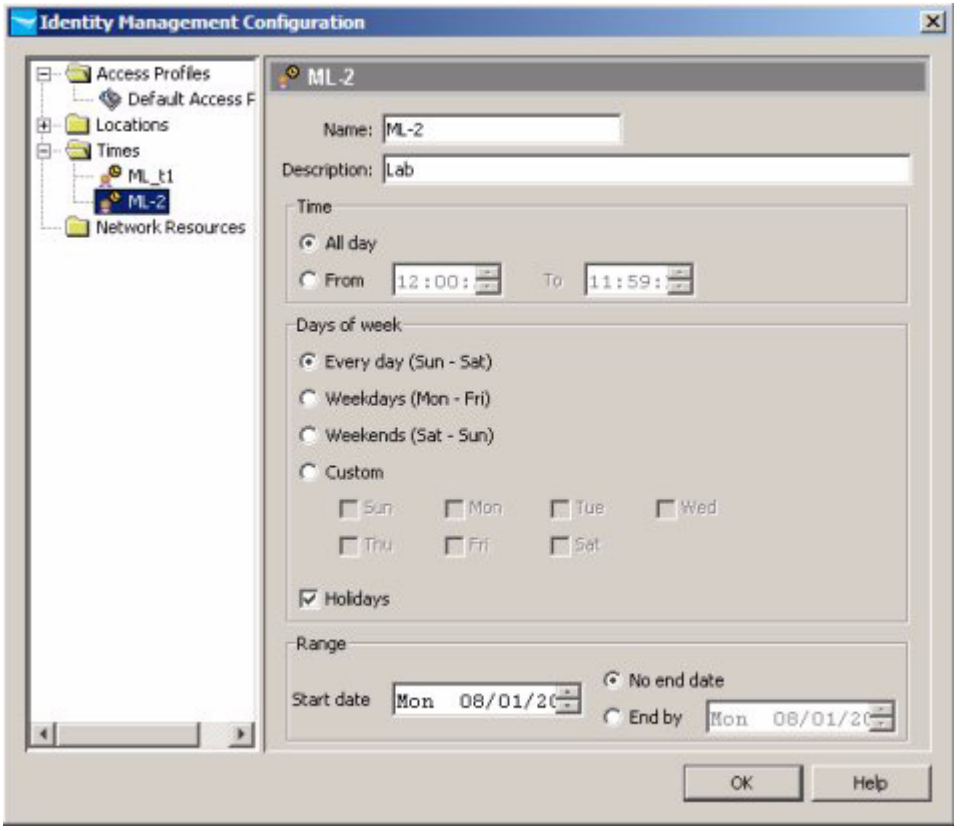
To configure a Time:

1. Click the Times node in the Identity Management Configuration navigation tree to display the Times panel.



The Times window lists the name and description of defined times. Double-click the time in the list, or select the time in the navigation tree 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.

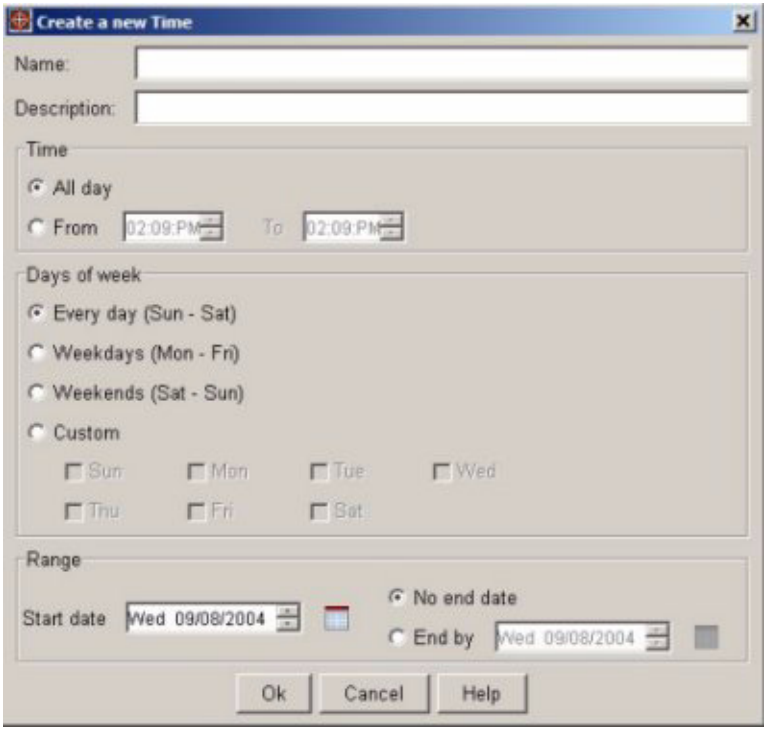


Creating a New Time

To configure a Time:

1. Click the Times node in the Identity Management Configuration navigation tree to display the Times panel.

2. Click the Add 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**.

Table 3-1. IDM Time parameters

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

Modifying a Time

1. Click the Times node in the Identity Management Configuration navigation tree to display the Times panel.
2. Click on a Time in the navigation tree to display the Time details in edit mode, similar to the Create a new Time panel.

You can also select the Time in the list then click the Modify Time icon in the toolbar to display the modify panel.

3. Modify the time parameters, as described in Table 3-1 on page 3-12.
4. 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 Times node in the Identity Management Configuration navigation tree to display the Times panel with the list of defined Times.
2. Click on a Time in the list to select it.

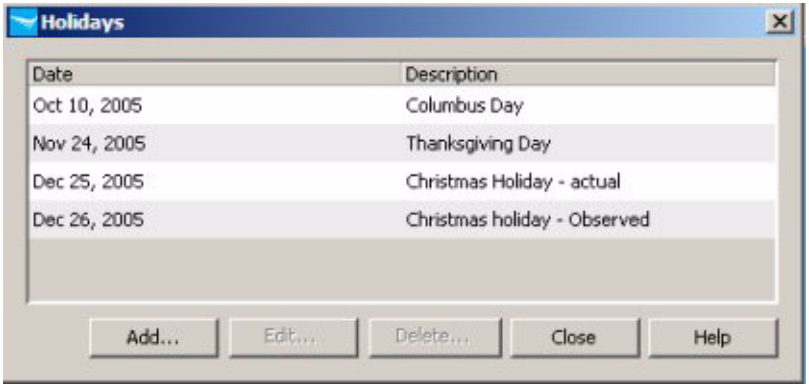
3. Click on the Delete Time icon in the toolbar to remove the location.

   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.

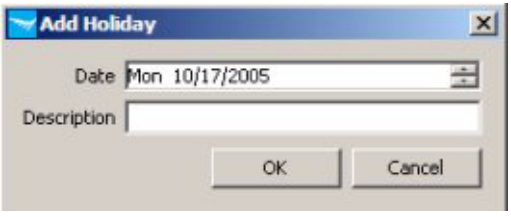
Defining Holidays

To add holidays for use when defining Times in IDM:

1. Click the Times node in the Identity Management Configuration navigation tree to display the Times panel.
2.  Click the Holidays icon in the toolbar to launch the Holidays window.



3. Click **Add.** to launch the Add Holidays window.



4. The **Date** field defaults to the current date. You can use the field buttons to increase or decrease the date. You can also type in a new date.
5. In the **Description** field, enter the text that will identify the holiday in the Holidays list.
6. Click **OK** to save the holiday and close the window.

The new holiday appears in the Holidays list.

To edit a Holiday, select it in the Holidays list, then click **Edit...** This launches the Edit Holiday window, similar to the Add Holiday window.

To delete a Holiday, select it in the Holidays list, then click **Delete...** Click **Yes** in the confirmation pop-up to complete the process.

Configuring Network Resources

The Network Resources in IDM are used to permit or deny traffic to and from specified sources and destination. This is done by configuring an IP-based filter based on either:

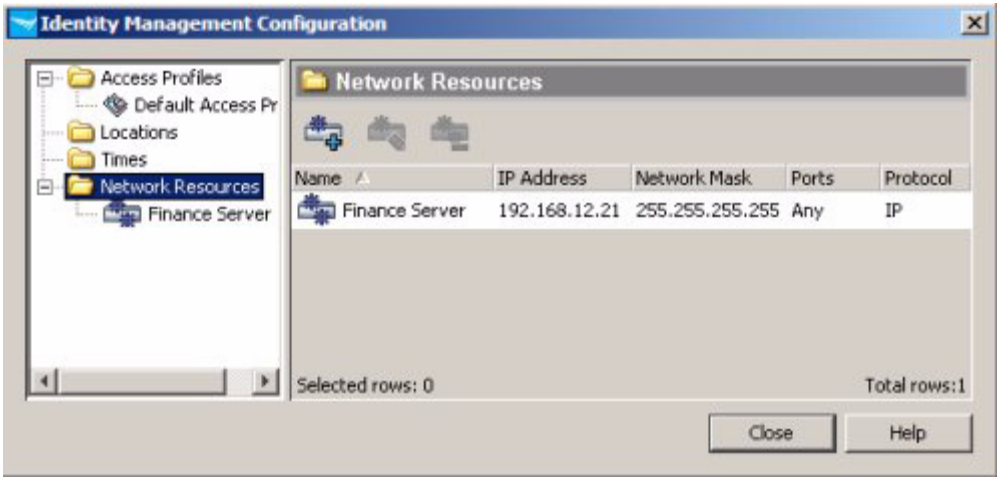
- The IP address (individual address or subnet address) of the source or destination, or
- The protocol (IP, ICMP, VRRP, etc.)
- The TCP or UDP port (i.e., based on protocol and application, such as Telnet or HTTP)

For example, you can create a Network Resource to restrict "guest accounts" so that they only have access to the external Internet, and no access to internal resources. Or you can define a resource that allows HR employees to access the payroll systems, and denies access to all other employees.

Network Resource features can be used only for switches that support IDM-based ACLs. As of this writing, this includes only the 5300 with version E.10.02 and greater; check the ProCurve web site (www.procurve.com) for more information.

To configure a Network Resource:

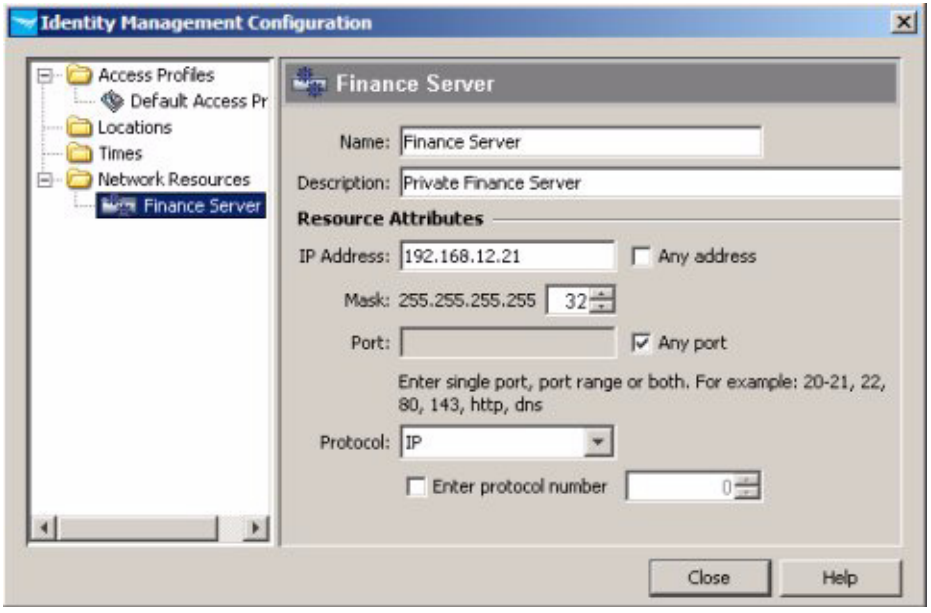
1. Click the Network Resources node in the Identity Management Configuration navigation tree to display the Network Resources panel.



The Network Resources window lists the name and parameters for defined resources, including:

Name	Name used to identify the resource
IP Address	IP Address for the switch associated with the resource ("any" if the resource is being filtered by protocol).
Network Mask	The subnet mask for the IP Address.
Ports	Device port(s) associated with the resource or Any if the resource is being filtered by protocol. Ports can be selected by number, or friendly port name. Refer to the section on "Using Friendly (Optional) Port Names" in the *Management and Configuration Guide* for your switch for details.
Protocol	The Protocol (UDP, TCP, or IP) used to filter access to the resource.

Double-click the Network Resource in the list, or select it in the navigation tree on the left to display individual Network Resource configuration details.



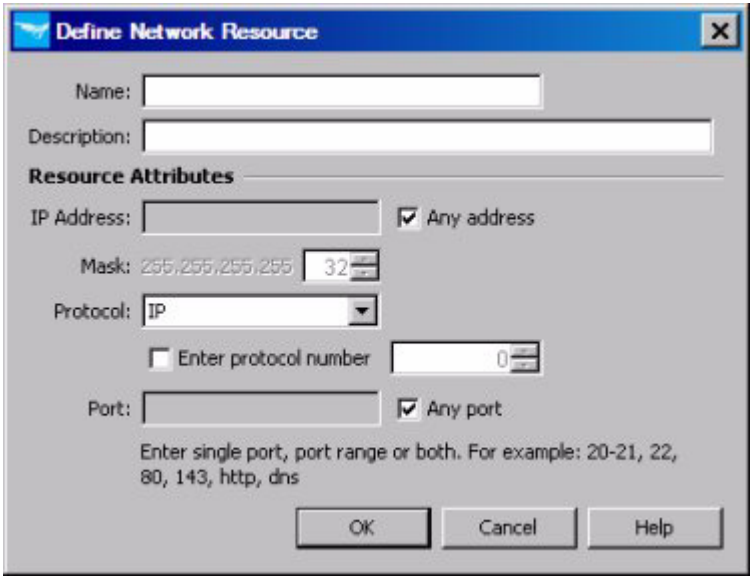
Note that when you open the window, it is in "Edit" mode. You can modify the entries in the display fields, and the changes are automatically saved when you click **Close**. For details on the field entries, refer to the definitions under “Adding a Network Resource” on the next page.

Adding a Network Resource

To define a Network Resource:

1. Click the Network Resources node in the Identity Management Configuration navigation tree to display the Network Resources panel.

2. Click the Add Network Resource toolbar icon to display the Define Network Resource window.



3. Define the properties for the network resource.

Name	Name used to identify the network resource
Description	Brief description of the network resource (optional)
Resource Attributes:	
IP Address:	To filter by device address, uncheck the **Any Address** checkbox and type the IP address for the switch associated with the resource in the IP Address field. Use the **Any address** option if you will be filtering by Protocol and application port only, and not by specific device or port.
Mask:	The subnet mask for the IP Address (if used). Use the up/down buttons [▲, ▼] to set the mask number.

Table 3-2. IDM Network Resource parameters

Protocol:	Select UDP, TCP, or IP to identify the protocol used to filter access to the resource. Protocol can be used alone or with an IP address and port parameters to define the network resource access. To use a custom protocol number for a network resource, check the **Enter protocol number** checkbox and type the protocol number (0-137)
Port:	**Any port** is selected by default, which means all ports associated to the IP address are included in the network resource definition. To specify a port for the network resource, click the **Any port** checkbox to de-select it and enable the **Port** field. Enter the port number, or friendly port name* used for the resource.

Table 3-2. IDM Network Resource parameters

* Valid Friendly port names supported in IDM include: ftp, syslog, ldap, http, imap4, imap3, nntp, pop2, pop3, smtp, ssl, telnet, bootpc, bootps, ssh, dhcp, ntp, radius, rip, snmpsnmp-trap, tftp.

Note:

If you are setting a resource to represent an application port such as "dhcp" or "smtp" or "http", you must make sure that you set the correct protocol, either TCP or UDP. If you do not set the correct protocol, the rule will not operate as intended at the switch or access point.

4. Click **Ok** to save the Network Resource definition and close the window.

   All entries are saved immediately upon entry. This allows you to configure several IDM features without closing and reopening the Configure Identity Management window

   Click Cancel to close the window without saving your changes.

To Edit a Network Resource:

1. Click the Network Resources node in the Identity Management Configuration navigation tree to display the Network Resources panel.

2. Click in the list to select the network resource to edit, then click the Edit Network Resource toolbar icon to display the Define Network Resource window.
3. Edit the properties as needed. Refer to “Adding a Network Resource” on the previous page for definitions.
4. Click **Ok** to save the Network Resource definition and close the window.

To Delete a Network Resource:

1. Click the Network Resources node in the Identity Management Configuration navigation tree to display the Network Resources panel.

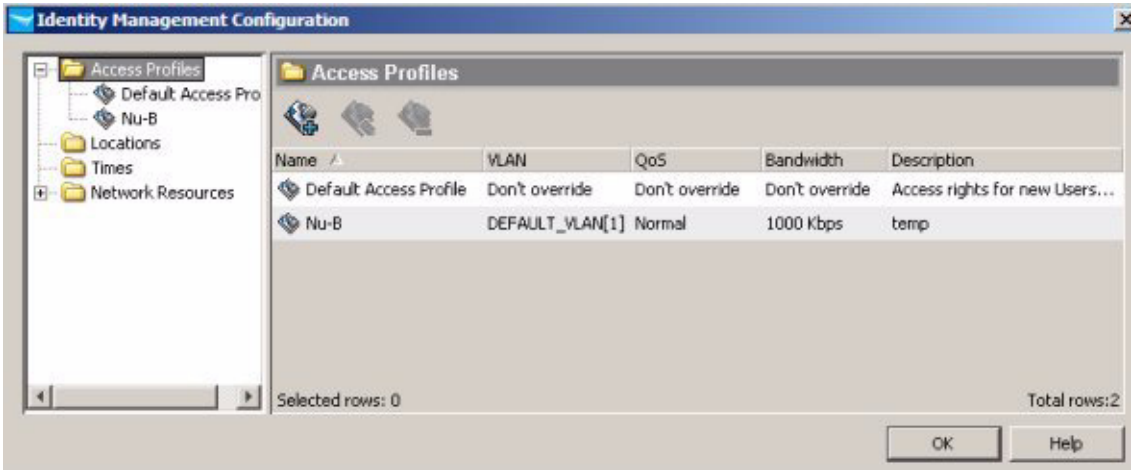
2. Click in the list to select the network resource to edit, then click the Delete Network Resource toolbar icon.
3. Click **Yes** in the confirmation pop-up to complete the process.

The selected network resource is removed from the Network Resources list display.

Configuring Access Profiles

IDM uses an Access Profile to set the VLAN, QoS, Bandwidth (rate-limits) and Network Resource access rules 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 or wireless access point settings to provide the proper network access and resources for the user.

To begin, click the Access Profiles node in the Identity Management Configuration navigation tree to display the Access Profiles window.



The Access Profiles window lists defined Access Profiles, including:

Name	Name used to identify the profile
VLAN	VLAN to which users are assigned when they log in
QoS	The "Quality of Service" setting
Bandwidth	The rate limits for outbound traffic
Description	Brief description of the profile

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

Click the Access Profile node in the navigation tree, or double-click on a profile in the list to display the details of the selected profile.

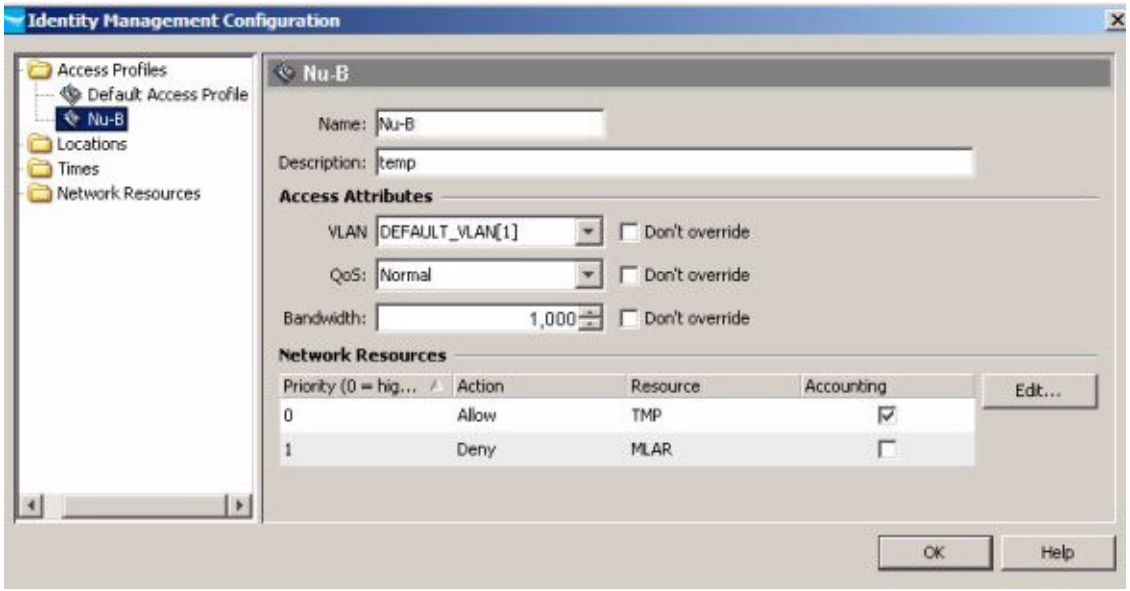


Figure 3-3.

The Name, Description, and Access Attributes are the same as defined in the Access Profiles list.

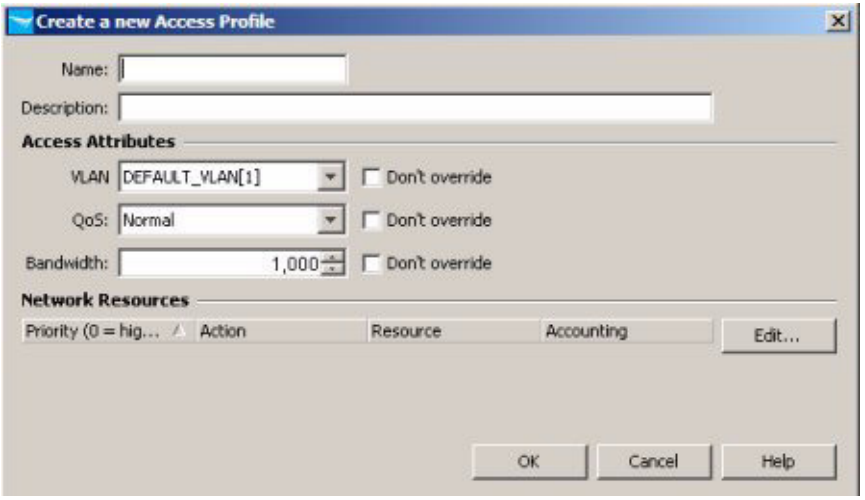
The Network Resources section lists the Network Resources included in the profile:

Priority	The order in which the network resource rules are evaluated; the first one to match each incoming packet is applied
Action	Indicates if access to the Network Resource is allowed or denied.
Resource	The defined network resource name.
Accounting	Tells the switch to keep a count of the number of hits using this rule.

Creating a New Access Profile

1. Click the Access Profiles node in the Identity Management Configuration navigation tree to display the Access Profiles window.

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



3. Define the attributes for the Access Profile:

Name	Name used to identify the Access Profile
Description	Brief description of the Access Profile
VLAN	Type in the VLAN or select one from the pull-down menu, which lists VLANs configured in PCM. The DEFAULT_VLAN(1) allows access across all segments 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" given to outbound traffic under this profile. Select the setting from the pull-down menu.
Bandwidth	The rate-limits applied for this profile. Use the up-down arrows to increase or decrease the Bandwidth setting. The default setting is 1000 Kbps (1 Mbps) NOTE: This is translated to a percentage of bandwidth at the switch.
Don't Override	Select this option for any of the Access Attribute parameters to use the current settings at the switch when the user logs in.

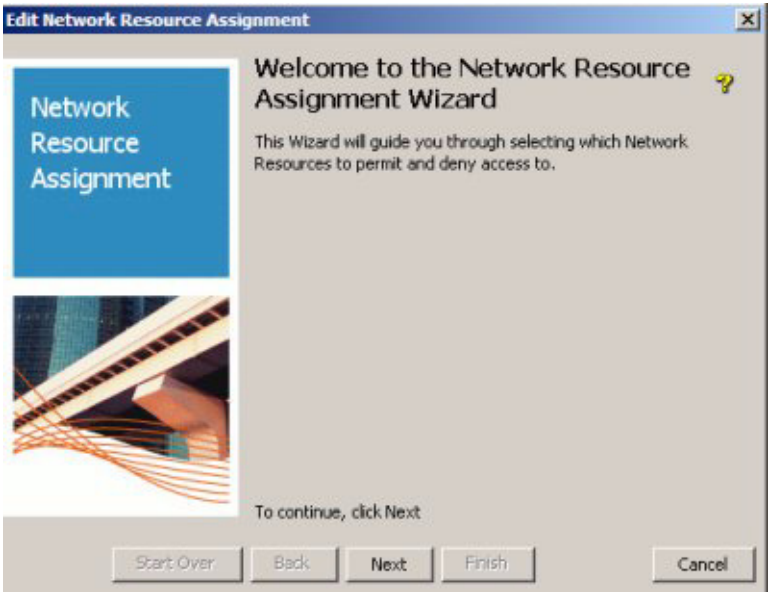
Table 3-1: Access Attributes

NOTE:

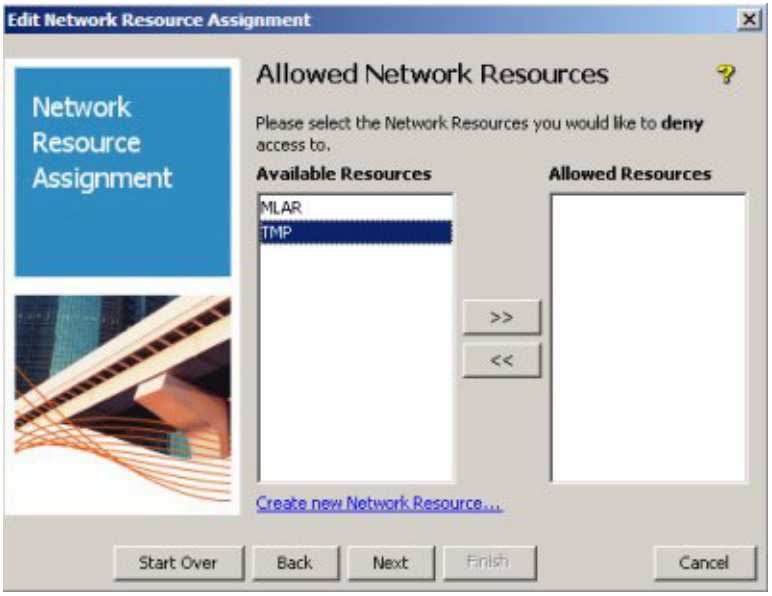
If you are assigning any VLAN other than the default VLAN, ensure that the VLAN is configured correctly on the all switches to which this access profile will be applied before defining the access profile.

The VLAN that gets set for a user will override the statically configured VLAN, as well as the auth-vid which may have been configured for that port. Note also that if an unauth-vid is set and the user is rejected by IDM for any reason, the port is opened and the VLAN is set to the unauth-vid.

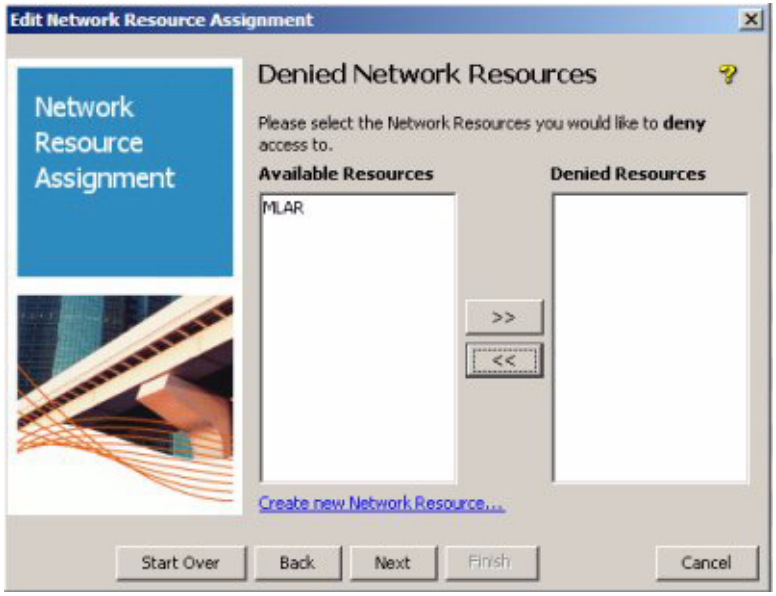
4. To assign the Network Resources, click **Edit...** This launches the Network Resource Assignment Wizard.



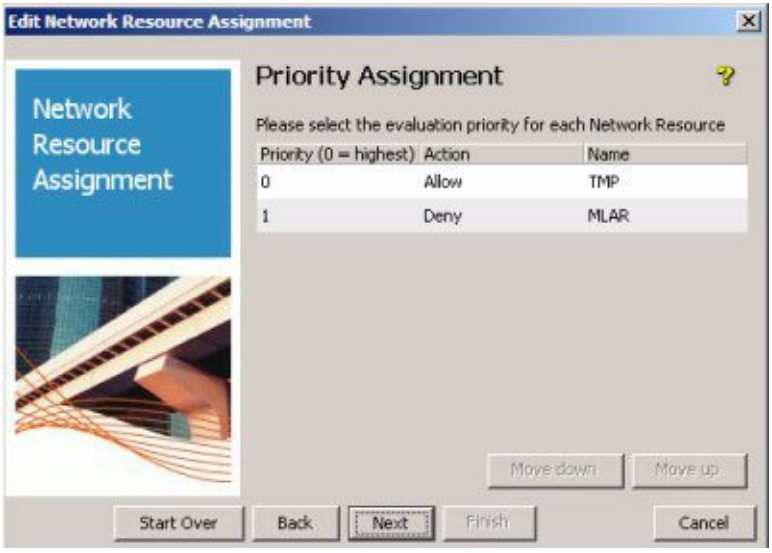
5. Click **Next** to continue to the Allowed Network Resources window.



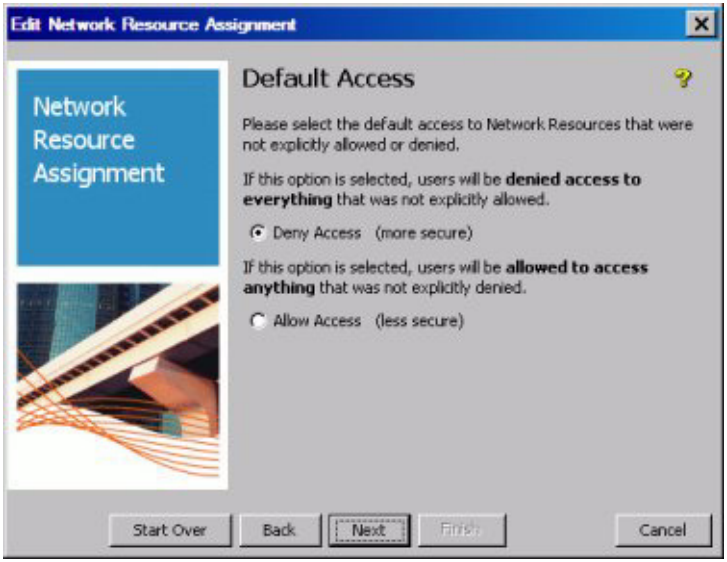
6. To permit access to Network Resources:
   a. Select the Resource in the Available Resources list. Use shift-click to select multiple resources.
   b. Move the Available Resource(s) to the Allowed Resources list (click **>>**)
   c. Click **Next** to continue to the Denied Resources window.



7. To deny access to Network Resources:
   a. Select the Resource in the Available Resources list. Use shift-click to select multiple resources.
   b. Move the Available Resource(s) to the Denied Resources list (click **>>**)
   c. Click **Next** to continue to the Priority Assignment window.

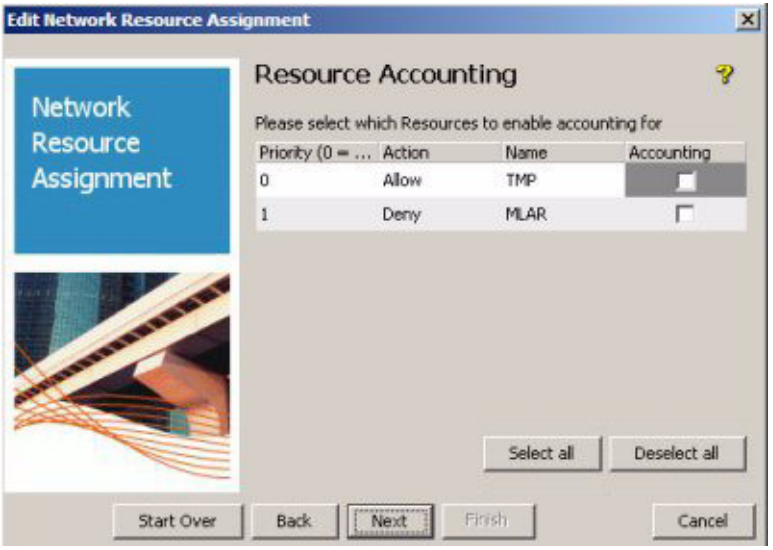


8. Set the priority (order of evaluation) for the Network Resources. To change the priority, click the Resource in the list, then click **Move down** or **Move up**. The first rule to match is the one that will be applied.
9. Click **Next** to continue to the Default Access window.

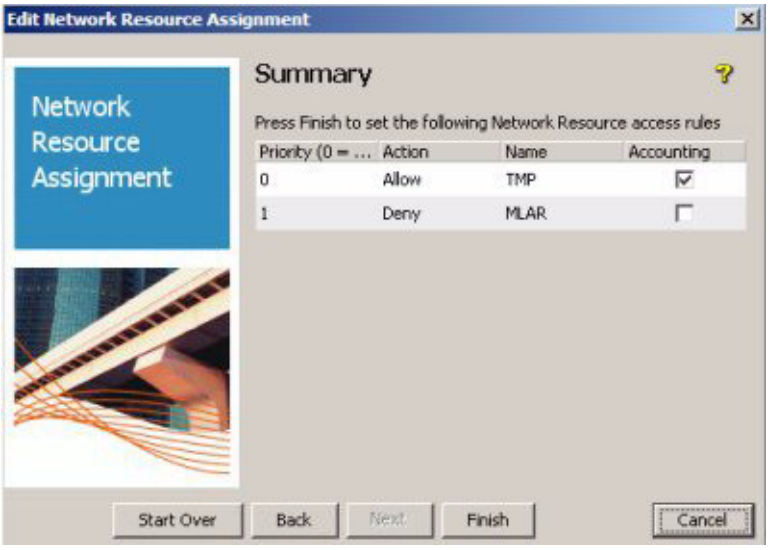


10. Select the option to tell IDM what to do if there are no matches found in the network resource access rules.

11. Click **Next** to continue to the Resource Accounting window.



12. Click the check box to enable the **Accounting** function (optional). This enables tracking of hits on this resource on the switch or access point. Use CLI on the switch to review the hits.
13. Click **Next** to continue to the Summary window.



14. Click **Finish** to save the Network Resource Assignments to the Access Profile and close the wizard.

    Click Back to return to a previous window to change the assignment, or

    Click Cancel to close the wizard without saving the changes.

    Click Start Over to return to the start of the Network Assignment Wizard.

Modifying an Access Profile

To modify an existing Access Profile:

1. Click the Access Profiles node in the Identity Management Configuration navigation tree 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 for creating a new profile. Click the Edit... button to change the Network Resource Assignments using the wizard.
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 Access Profiles node in the Identity Management Configuration navigation tree 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: Before you modify or delete an Access Profile, make sure that your changes will not adversely affect users in Access Policy Groups where the profile is used.

Defining Access Policy Groups

An Access Policy Group (APG) contains rules that define the VLAN, rate-limit (bandwidth), quality of service, and network resource access rules for users in the group, based on the time, location, and system from which the user logs in. You can also create rules to work in conjunction with third-party endpoint integrity (Host Integrity) applications to verify that systems attempting to connect to the network meet security requirements.

Each rule in an Access Policy includes the following parameters:

- Location - identifies the switch and/or switch ports where users connect to the network. Location can identify physical wiring connections or VLANs configured to segment the network
- Time
- System
- Enpoint Integrity
- Access Profile

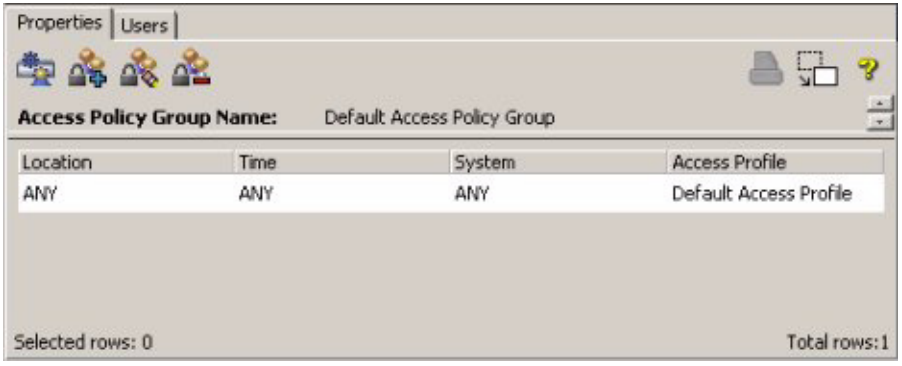
Multiple access policy groups can be added to a realm, and multiple access profiles, locations, and times can be referenced and configured in an access policy group

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 or access point to accept or reject the user, and modifies the RADIUS reply to provide the appropriate network access to the 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, expand the Realms node to display the Access Policy Group node in the IDM tree. Click to display the Access Policy Groups tab.

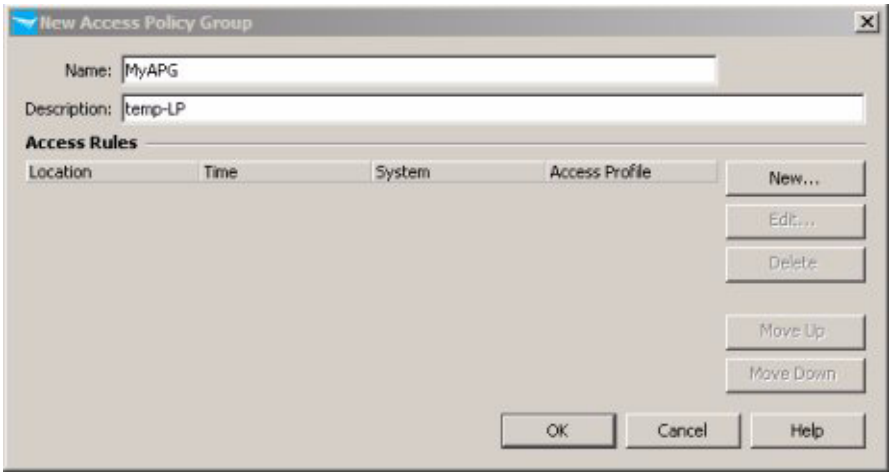
You can expand the Access Policy Group (APG) node in the tree, and click the individual APG node to display the policy Properties tab.



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 Add 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...** to display the New Access Rule dialogue.

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

Location	Lists the Locations you created by name, and the "ANY" option. If you select ANY and the access profile for the rule points to a VLAN, ensure that the VLAN is configured on every switch to which users in this access policy group will be connecting
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 3-48 for detail.

Access Profile	Lists the Access Profiles you created by name, the Default Access Profile, and a REJECT option. Select REJECT if the rule will prohibit a user from logging in.

6. Repeat the process for each rule you want to apply to the APG.
7. The Access rules are evaluated in the order (priority) they are listed in the Access Rules table. Use **Move Up** or **Move Down** buttons to arrange the rules in the order you want them to be evaluated. IDM checks each rule in the list until a match on all input parameters is found, then applies the corresponding access profile to the user.

   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

Using IDM with Endpoint Integrity Systems

You can create access profiles in IDM to work in conjunction with endpoint integrity (host integrity) applications to verify that systems attempting to connect to the network meet security requirements. To use the Endpoint Integrity support options you need to select the Endpoint Integrity option in the IDM Preferences window (Tools->Preferences->Identity Management).

With the Endpoint Integrity preference set, the Endpoint Integrity option will appear in the Access Rules windows.

- Select **PASS** to apply the access rule in cases where the system the user is logged in on passes the endpoint integrity check.
- Select **FAIL** to apply the access rule in cases where the system the user is logged in on fails the endpoint integrity check.
- Select **ANY** to apply the access rule regardless of the status passed from the endpoint integrity system.

For example, if you want to restrict access to a specific (remediation) VLAN when the endpoint integrity check fails, create a Location that specifies the remediation VLAN, then create an access rule that will put the user on that Location if the Host Integrity value is FAIL.

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

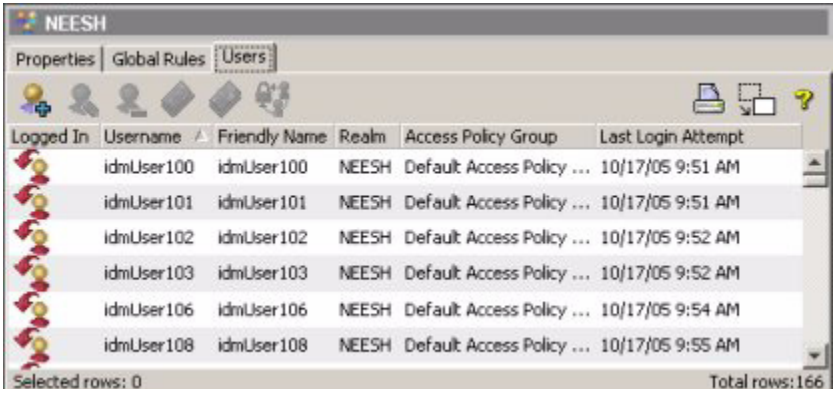
1. Click the Access Policy Group node in the IDM tree to display the Access Policy Groups tab.
2. Click on an Access Policy Group Name to select it.
3.  Click the Delete Policy Group icon in the toolbar to delete the Access Policy Group.

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 list of users.



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.
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. Expand the Realms node, then click the individual Realm to display the Users tab, or expand the realm to display access policy groups. Click the Users tab in the individual Realm or Access Policy Group window.

2. Select the users in the list, then click the Add Users to APG icon in the toolbar to display the Select Access Policy Group window.

3. In the **Assign selected Users to Access Policy Group**: field, use the pull-down menu to select the access policy group to which you want to assign the user(s).

   If you select the Default Access Policy Group from the assignment pull-down menu, users can log into RADIUS servers, but they are not governed by access policy group rules. IDM will still collect and display event information for users in the Default APG, as long as they are authenticated by the RADIUS server.

4. 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. Select the users in the list, then click the Add Users to APG icon in the toolbar to display the Select Access Policy Group window.

3. Select a different option from the **Assign selected Users to Access Policy Group** pull-down menu.

4. Click **Ok** in the confirmation pop-up, then click **OK** in the Select Access Policy Group window to save your changes and close the window.

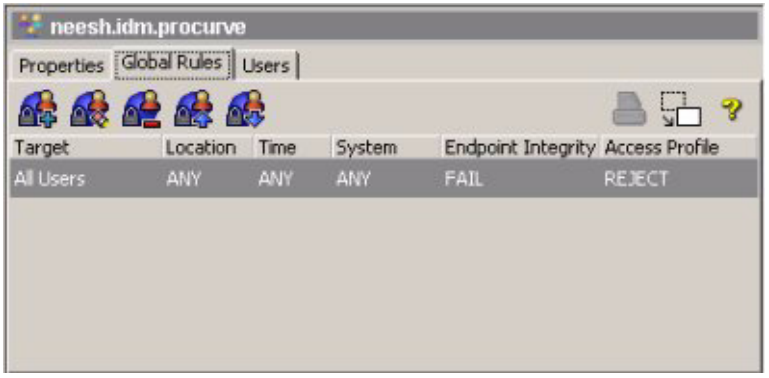
   The new APG assignments are displayed in the Users list.

Using Global Rules

Global Rules can be used to provide an "exception process" to the normal processing of access rules via Access Policy Groups. IDM will check for Global Rules and apply them to the designated users before processing any access rules found in Access Policy Groups. For example, you can use a Global Rule to deny access to the network during a specific time period, such as a site shutdown or during periods when network maintenance is being done.

Global Rules are typically used to apply to all users in a realm. They can also be defined to apply to a single user or access policy group. Global Rules should not take the place of existing rules defined within the Access Policy Groups; they are intended for special use cases.

To display global rules, click on the Realm in the IDM navigation tree, then click the Global Rules tab in the Realm display.



The Global Rules tab provides the following information for defined global rules:

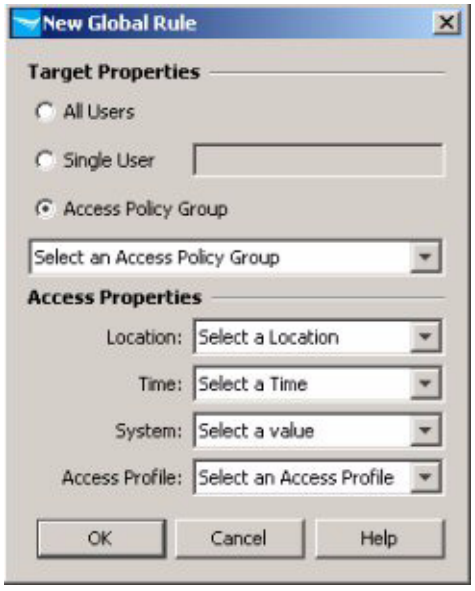
Target	User(s) or access policy group to which the rule applies
Location	Location where the rule is used
Time	Time that the rule is used
System	System where the rule is used
Endpoint Integrity	Indicates the endpoint integrity status used by the rule. This appears only if the Endpoint Integrity option is set in IDM (Global) Preferences.
Access Profile	Access profile governing user permissions during the session

Creating a Global Rule is similar to creating Access Rules for an Access Profile Group.

To create a global rule:

1. In the navigation tree, click on the realm that will use the global rule, then click the Global Rules tab in the Realm's display.

2. Click the Add Global Rule button to display the New Global Rule window.



1. Select the **Target Properties**
   - To use the global rule for all users in the realm, select the All Users
   - To use the global rule for a specific user, select Single User and type in the user name.
   - To use the global rule for an access policy group, click Access Policy Group, and select the group from the drop-down menu.

Note:

If you want to create a global rule for multiple users or multiple groups, you do this by creating multiple rules, each referencing a single user, or group.

2. Set the **Access Properties** for the Global Rule. This is similar to the process used to define Access Policy Rules when you create an Access Policy Group (see page 3-32)

a. Select the **Location** where the global rule will be applied, or "ANY".
b. Select the **Time** when the global rule will be used, or "ANY".
c. Select the **System** where the global rule will be used, or "ANY"
d. In the **Access Profile** field, select the access profile where the global rule will be used.
e. If **Endpoint integrity** is enabled, select the option that indicates when the rule will be applied, relative to the endpoint integrity status (Pass, Fail, or Any)

3. Click **Ok** to save your changes and close the New Global Rule window
4. The new global rule appears in the Global Rules list.

5. Similar to access rules, the global rules are evaluated in the order they are listed in the Global Rules table. Use the Move Up or Move Down button in the toolbar 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.

Changing Global Rules

To edit Global Rules:

1. Navigate to the Global Rules window.
2. Select the rule you want to modify in the Rules list.

3. Click the Edit Global Rule icon to display the Edit Global Rules window.
4. Change the desired values, as explained for New Global Rule (on the previous page).
5. Click **Ok** to save the changes and close the Edit Global Rules window.

To delete a Global Rule:

1. Navigate to the Global Rules window.
2. Select the rule you want to delete in the Rules list.

3. Click the Delete Global Rule icon in the toolbar.
4. Click Yes in the confirmation pop-up to complete the process.

The rule is removed from the Global Rules list.

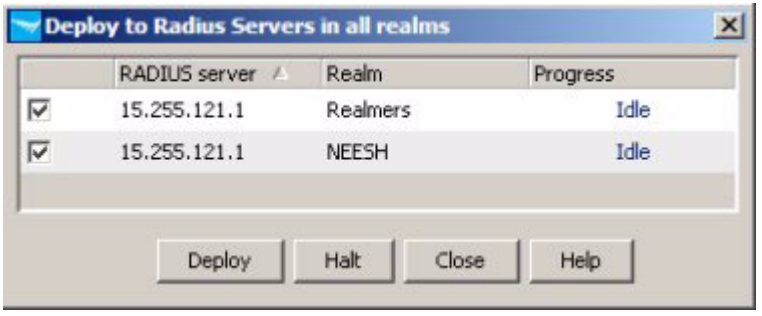
Deploying Configurations to the Agent

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, but have not yet deployed the changes, 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. Deployment overwrites and replaces the current configuration for that realm, on that RADIUS server.

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 Servers 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

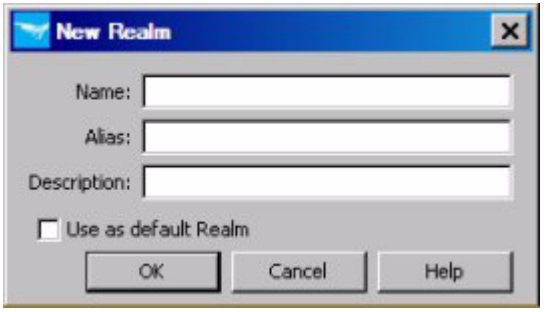
It is simplest to let the IDM Agent run and collect information about Realms, including RADIUS servers and users in the Realm from the RADIUS server, but you can also manually define information about the Realm, RADIUS servers, and users in the IDM GUI.

Defining New Realms

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

To define a realm:

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



2. Enter the information for the Realm:
   - Type the **Name** used to identify the realm.
   - In the **Alias** field, type an alternate name that can be used for the realm. For example a fully qualified realm Name can be idm.main.procurve and the Alias can be IDM. This is most useful when using IDM with Active Directory; and you should make sure that the IDM realm alias matches the Active Directory "NETBIOS" name.
   - Type a brief **Description** of the realm to help identify the realm.
   - 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 Realms list, and the IDM Tree.

Modifying and Deleting Realms

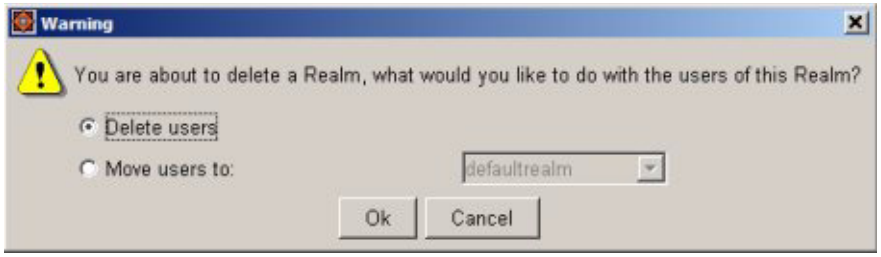
To modify an existing Realm:

1. Select the Realm in the Realms 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:
   - The Name used to identify the realm.
   - The realm Description.
   - 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 changes and close the window.

The Realm modifications appears in the Realm List and Realm Properties tab.

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.



When you delete a realm, the users and Access Policy Groups belonging to the realm are also deleted. Click one of the radio buttons to indicate what to do with users in the realm:

Delete users: Delete all users currently belonging to this 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)

Click **Ok** to complete the realm delete process.

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 a 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 server window. (similar to the New RADIUS server 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.

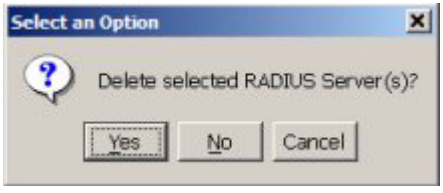
The edited RADIUS Server information appears in the RADIUS List, and the Properties tab for the server.

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.

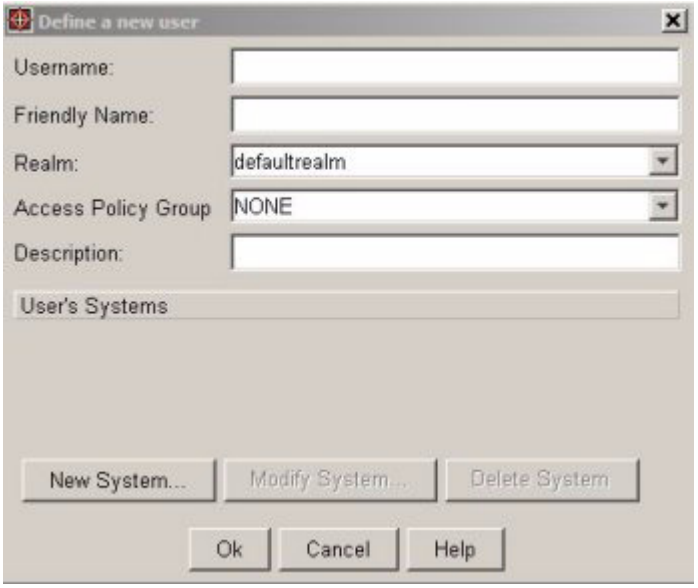
Adding New Users

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. You can also use the IDM User Import feature in the Tools menu.

Adding users in IDM: Manual Process

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 Define a new user window.



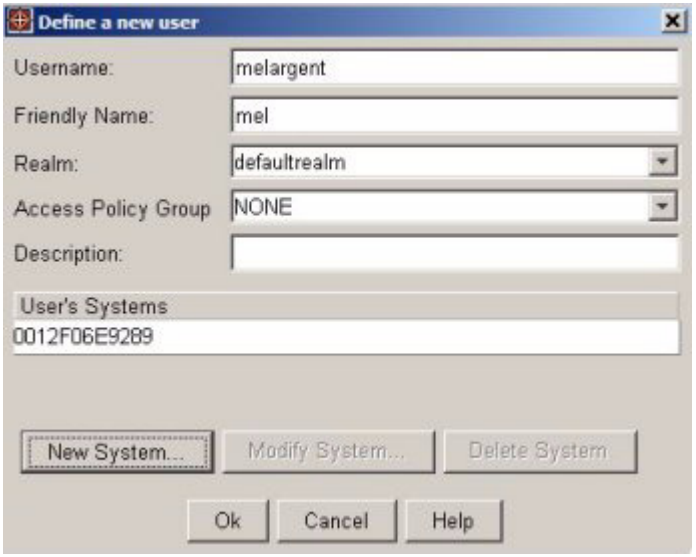
2. Enter the information for the User
   - **Username**: The user's login name (required).
   - **Friendly Name**: Friendly name for the user.
   - **Realm**: Select the Realm the user "belongs" to, if different from the default realm.
   - **Access Policy Group**: Select the Access Policy Group to which 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 3-42 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 Define a new user window) displays.
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 3-42 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.

Using the User Import Wizard

The IDM User Import Wizard lets you add users to IDM from another source, such as an Active directory or LDAP server. The IDM Import Wizard also synchronizes the IDM user database with the import source directory, and allows you to delete users from the IDM user database that are not found in the import source directory. IDM does this by copying the list of users from the directory to an XML file, comparing users in the XML file to users in the IDM user database, and listing the differences for you to add or remove the mismatched users in the IDM user database.

Importing an existing company directory or user database has the following benefits:

- Easier initial setup, because all users in the company directory can be automatically added to the IDM directory.
- If the company directory contains group assignments, users can be automatically assigned to the appropriate policy group (based on membership in the company directory).
- When a user is removed from the company directory, they are automatically removed from the IDM user database. In addition, when a user's group membership is changed in the company directory, their network access policy group is automatically changed accordingly.
- Automating user import and synchronization leaves less room for error and reduces tedious work.

The basic import procedure is listed below, though the specific windows you see will vary based on the import data source.

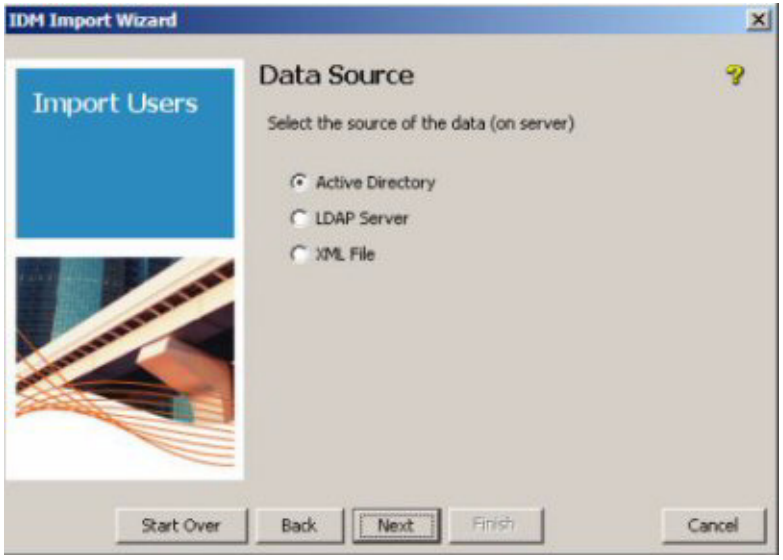
1. Select the Source Type (Active directory, LDAP server, or XML file)
2. Define the source parameters.
   a. for Active directory, select the Group Scope to import.
   b. for LDAP server, supply the server details, username, and password.
   c. for XML, supply the filename (including the directory path). This file must exist on the IDM Server system.
3. IDM extracts the user information from the data source, based on the defined parameters.
4. Select the Users, and groups (if applicable) to be added to IDM.
5. Select any Users to be removed from IDM.
6. Commit the changes to IDM.

Importing Users from Active Directory

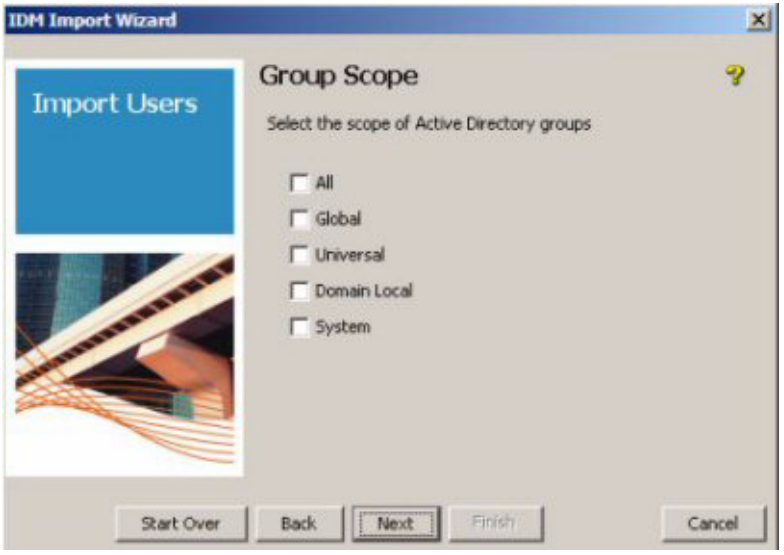
To import user information into IDM from an Active Directory:

1. Select IDM User Import option from the Tools drop-down list in the global toolbar. This launches the IDM User Import Wizard.

2. Click **Next** to continue to the Data Source selection window.



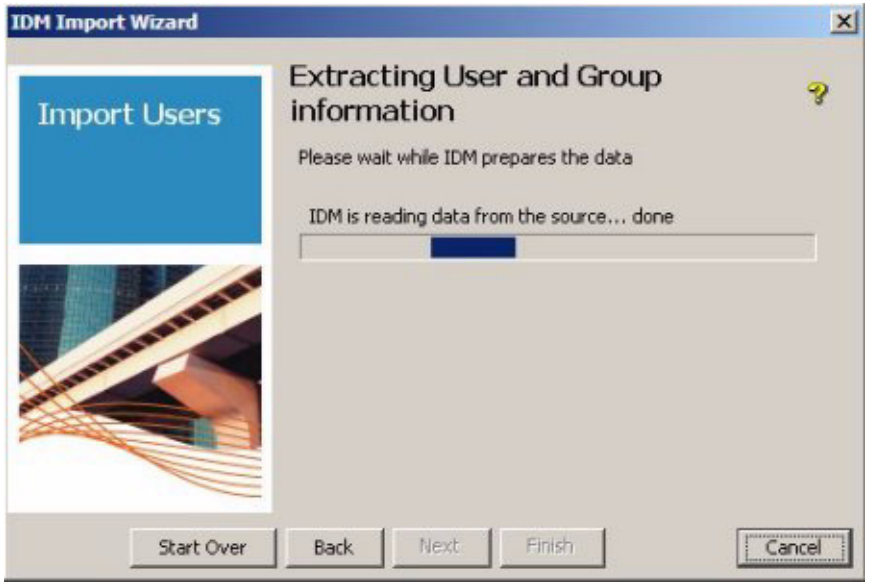
3. Click the radio button to select the **Active Directory** data source.
4. Click **Next** to continue to the Group Scope window.



5. Select the scope of Active Directory groups that you want to import user data from.

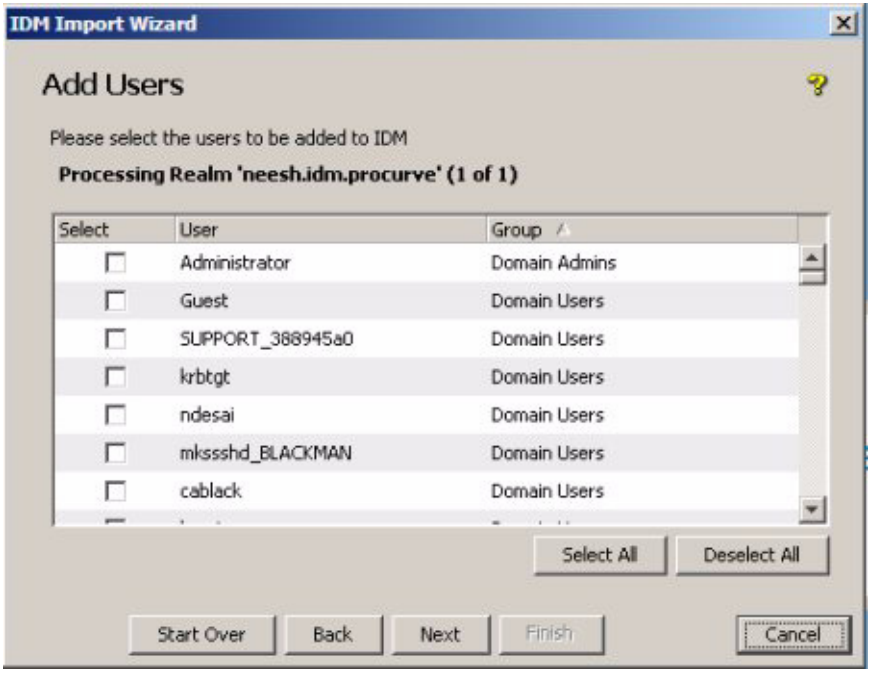
Group	Description
All	Import users from all Active Directory groups
Global	Import users from the Global Active Directory group. This will also get user data from any custom defined group in your Active directory.
Universal	Import users from the Universal Active Directory group
Domain Local	Import users from the Domain Local Active Directory group
System	Import users from the System Active Directory group

6. Click **Next** to continue to the Extracting User and Group information window.



7. When the display indicates the data extraction is done, click **Next** to continue to the Import Groups window.

8. Click the Select checkbox to choose the groups you want to import from the Active Directory to IDM. If there is no checkbox, the group already exists in IDM and does not need to be selected.
9. Click **Next** to continue to the Add Users window.



10. Click the Select checkbox to choose the users you want to import from the Active Directory to IDM.

    The current Import data is compared to the existing user list in IDM. If no new (additional) users are found in the import data, the user list is empty.

    If any user exists in more than one Active Directory group, you will be prompted to select the group the user will belong to in IDM.

    a. **Select the group** from the drop down list.

       If you have a large number of users that belong to multiple groups, click the checkbox to **Assign all users to selected group**. This will assign all the users to the selected group in a single step, and you will not need to repeat the group selection for each user.

b. Click **Next** to continue. Repeat the process for each user.

c. Click **Finish** to save the Group Selections and exit the pop-up.

d. Click **Back** to change the previous selection.

11. Click **Next** to continue to the Remove Users window.

    The Import data is compared to the existing user list in IDM. Any users that exist in IDM, that are not found in the Import data, are listed. Select any users you want to delete from IDM. This window operates similarly to the Add Users window.

12. Click **Next** to continue to the Users and Groups Commitment window.

13. Click **Go** to save the selected group and user data (adds and deletes) to IDM.

14. When the commit data function is done, click **Next** to continue to the Import Complete window.

A summary of the IDM Import displays.

15. Click **Finish** to exit the wizard.

Importing Users from an LDAP Server

The IDM Import Wizard includes support for using Windows 2003 LDAP service to import users from an MS Active directory. You can also import user data from other LDAP V3 (version 3) servers, (e.g., Netscape® LDAP server).

To import user information into to IDM from an LDAP Server:

1. Select the IDM User Import option from the Tools drop-down list in the global toolbar to launch the IDM User Import Wizard.
2. Click **Next** to continue to the Data Source selection window.
3. Click the radio button to select the **LDAP Server** data source.
4. Click **Next** to continue to the LDAP Authentication window.

a. To use the SSL authentication method, check the **Use SSL** checkbox.

Note:

To use SSL, ensure that your LDAP server supports SSL. The X509 certificate for your LDAP server must be installed in your Java trust store, and the PCM server must be restarted after installing the certificate. Contact your (LDAP) Administrator to get the certificate. The trust store is available under the installation directory of PCM. For example, if PCM is installed under Program files\Hewlett-Packard, type:

```
C:> cd c:\Program files\Hewlett-Packard\PNM\jre\
lib\security

C:> ..\..\bin\keytool -import -file <ldapcertfile> -
alias myldapcert -keystore cacerts -keypass <certifi-
cate password> -trustcacerts -storepass <keystore
password>
```

The default keystore password is changeit.

b. Select the LDAP **Authentication type** to be used with the imported user data:

Authentication	Description
Simple	Simple authentication, which is not very secure, sends the LDAP server the fully qualified DN of the client (user) and the client's clear-text password.
Digest-MD5	In Digest MD5, the server generates a challenge and the client responds with a shared secret (password).
Kerberos-V5	Based on Internet standard security, Kerberos V5 authentication is used with either a password or a smart card for interactive logon.
External-TLS	External authentication uses authentication services provided by lower level network services such as TLS.
Anonymous	No authentication is required by LDAP server.

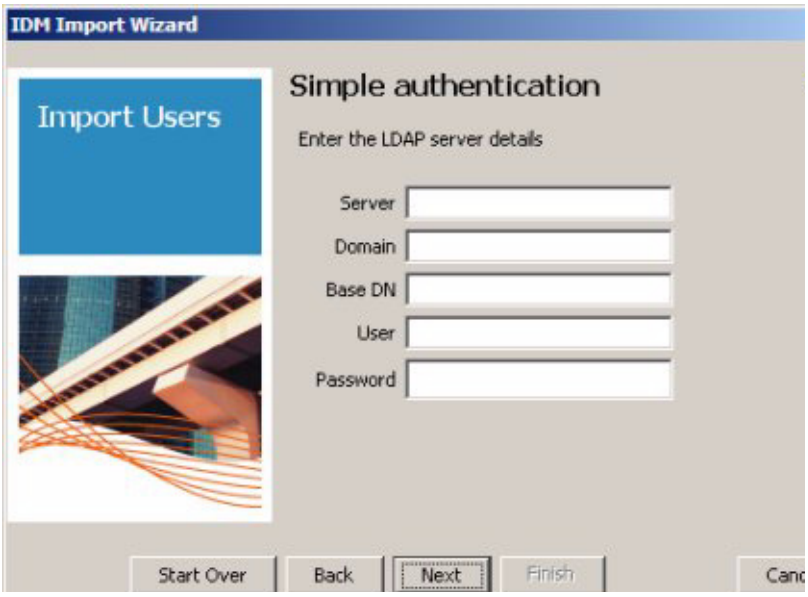
c. Click **Next** to continue to the Authentication details window:

The Authentication details will vary based on the Authentication type selected; however, all LDAP Authentication methods require the following information:

- Server – The IP Address or DNS name (fully qualified domain name) of the LDAP server.
  The IP address can be used for Simple, Anonymous, and Kerberos-V5 authentication in non-SSL mode.
- Domain – The domain name that will be used to create the Realm in IDM.
- Base DN – The Base Distinguished Name. This is the node in the directory where the search for users will begin. For example, for the domain "hp.com" the Base DN entry would be: `dc=hp,dc=com`

For Simple Authentication

Simple authentication, which is not very secure, sends the LDAP server the fully qualified DN of the client (user) and the client's clear-text password. Values for these fields can be obtained from the LDAP server administrator.



To set up Simple authentication:

1. In the **Server** field, type the IP address or DNS name of the LDAP server
2. In the **Domain** field, type the domain name. (It will be used to create a realm in IDM.)
3. Optionally, in the **Base DN** field, type the Base Distinguished Name. IDM will search only for users and groups from this node of a directory tree.
4. In the **User** field, type the user's DN used to access the LDAP server.
5. In the **Password** field, type the password associated with the user.
6. Click **Next** to continue to the Extract Users and Groups window.

Using Digest-MD5 Authentication

The SASL Digest MD5 authentication window is used to define the LDAP data source for Digest-MD5. In Digest-MD5, the server generates a challenge and the client responds with a shared secret (password). Values for these fields can be obtained from the LDAP server administrator.

To set up Digest MD5 authentication:

1. In the **Server** field, type the DNS name of the LDAP server.
2. In the **Domain** field, type the domain name. It is used to create a realm in IDM.
3. Optionally, in the **Base DN** field, type the Base Distinguished Name. IDM will search only for users and groups from this node of a directory tree.
4. In the **User** field, type the user DN used to access the LDAP server.
5. In the **Password** field, type the password associated with the user.
6. Click **Next** to continue to the Extract Users and Groups window.

Using Kerberos-V5 Authentication

The SASL Kerberos V5 authentication window is used to define the LDAP data source for Kerberos. Kerberos V5 authentication requires that your LDAP server is setup with a KDC (Key Distribution Center). Please contact your LDAP server administrator for details.

To set up Kerberos V5 authentication:

1. In the **Server** field, type the IP address or DNS name of the LDAP server.
2. In the **Domain** field, type the domain name. It will be used to create a realm in IDM.
3. Optionally, in the **Base DN** field, type the Base Distinguished Name. IDM will search only for users and groups from this node of a directory tree.
4. In the **User** field, type the user name used to access the LDAP server.
5. In the **Password** field, type the password associated with the user.
6. In the **Config file** field, type the complete path and filename of the configuration file that identifies the domain of the KDC.
7. Click **Next** to continue to the Extract Users and Groups window.

Using External Authentication

The SASL External authentication window is used to define the external LDAP data source. External authentication uses an X509 certificate for user authentication. The LDAP X509 User Certificate must be installed in a keystore on the IDM server, and the LDAP server's certificate must be stored in the trust store under your JRE installation on the IDM server. See page 3-64 for details on importing LDAP X509 User certificates for use with IDM.

To set up External authentication:

1. In the **Server** field, type the DNS name of the LDAP server.
2. In the **Domain** field, type the domain name. It is used to create a realm in IDM.
3. Optionally, in the **Base DN** field, type the Base Distinguished Name. IDM will search only for users and groups from this node of a directory tree.
4. In the **Keystore** field, type the keystore file name.

   For JKS, the Keystore is the location on the IDM server where you installed the keystore. (for example: `c:\idmuser\mykeystore`)
   For PKCS12, enter the PKCS certificate in the Keystore field,.
5. In the **Password** field, type the password.

   For JKS, enter the password of the keystore on the IDM Server.
   For PKCS12, enter the PKCS12 key in the Password field
6. Select the **Type**: either **jks,** or **pkcs12**.

7. Click **Next** to continue to the Extract Users and Groups window.

Importing LDAP X509 User Certificates into a Keystore:

If you are using a JKS Keystore, the X509 User Certificate must be installed in a keystore on the IDM server. You can get the X509 User Certificate from your LDAP Administrator.

For example, if the X509 User Certificate is "`myldapcert.cer`" and the alias is "`mycert",` use the following command to import the certificate in a keystore in `c:\idmuser\mykeystore` on your IDM server:

```
C:\idmuser> keytool –import –file myldapcert.cer –alias
mycert –trustcacerts –keystore .\mykeystore
```

If you are using a PKCS12 keystore, ask your LDAP Administrator to provide you PKCS12 certificate along with the key. Enter the PKCS certificate in the Keystore field, and enter the PKCS12 key in the Password field.

Using Anonymous Authentication

The LDAP Anonymous Authentication window is used to define the LDAP data source. Values for these fields can be obtained from the LDAP server administrator.

To set up an LDAP server with anonymous authentication:

1. In the **Server** field, type the IP address of the LDAP server.
2. In the **Domain** field, type the domain name.
3. Optionally, in the **Base DN** field, type the Distinguished Name. IDM will search only for users and groups from this node of a directory tree.
4. Click **Next** to continue to the Extract Users and Groups window.

The remainder of the process for importing users from LDAP Servers is the same as described for importing users from Active Directories.

- Select the Groups and Users to Import to IDM.
- Select Users to remove from IDM (if applicable)
- Commit the selected groups and users (adds and deletes) to IDM.

Editing IDM Configuration for LDAP Import

The IDM server includes several configuration files that contain information used to import User information from LDAP files. The default configuration settings will work if you are using MS Active Directory as the LDAP Server directory. If you are using any other LDAP directory source (for example Novell Edirectory) you will need to modify the LDAP Directory settings in:

~Program Files\Hewlett-Packard\PNM\server\config\IDMImportServerComp.scp

Following is an example of the DMImportServerComp.scp file for reference. Comments are indicated by "//".

```
LDAP_SERVER_CONFIG {
    PORT=389 //Port where LDAP server receives bind request.
    SSL_PORT=636 // Port where LDAP server receives SSL bind requests.
    BATCH_SIZE=50 // Internal to IDM.
    COUNT_LIMIT=0 // Internal to IDM.

    SASL_CONFIGURATION {
    // This section is for SSL configuration: Digest MD5, Kerberos V5 and External.
    QOP=auth-conf,auth-int,auth
        // Quality of protection. Valid values are 1 and more of "auth-conf", auth-
        int", "auth" separated by ",".
    ENCRYPTION_STRENGTH=high,medium,low
        // Strength of encryption. Valid values are 1 and more of "high", "medium",
        "low" separated by ",".
    MUTUAL_AUTHENTICATION=true
        // If both LDAP server and IDM server wants to authenticate each other.
    }

    KERBEROS_JAAS_CONFIG {
    // This section is for Kerberos authentication method.
    KERBEROS_AUTH_MODULE=IDMKerberos
    // Kerberos authentication module name. If this entry is changed, you must also
    change the module name in idm_kerberos_jass.conf file.
    KERBEROS_JAAS_CONFIG_FILE=config/
    idm_kerberos_jaas.conf   // configuration file for JAAS Kerberos
    configuration.
    }
 }
```

(Example continued on next page)

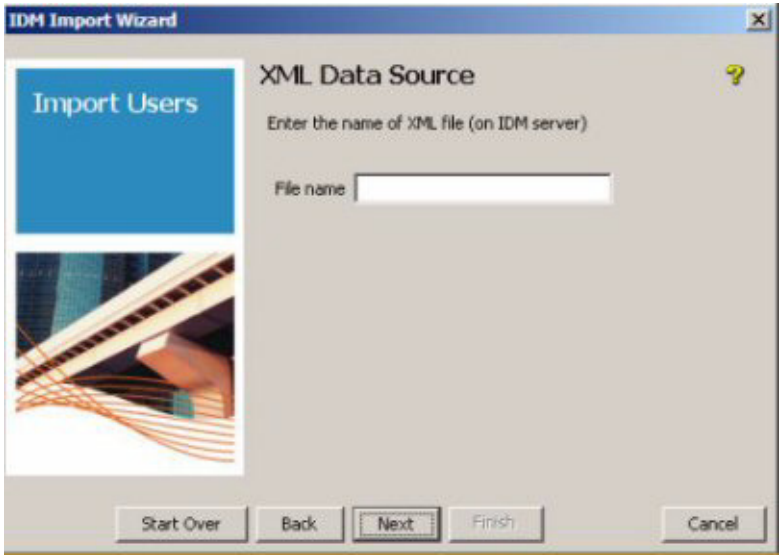
```
  LDAP_DIRECTORY_CONFIG {
// Configuration for LDAP directory. Following values are for Active Directory. Change
as needed per object class and attributes in LDAP directory being used.
    USER {  // User object
    OBJECT_CLASS=User  // User object class
    LOGON_NAME=sAMAccountName  // Login name attribute.
    COMMON_NAME=cn  // Common Name attribute
    DESCRIPTION=description  // User description attribute
    DISPLAY_NAME=displayName  // User display name attribute
    }
    GROUP {  // Group object
    OBJECT_CLASS=Group  // Object class for Group
    COMMON_NAME=cn  // common name attribute
    DESCRIPTION=description  // Group Description attribute
    MEMBER=member  // Group member attribute
    USER_MEMBER_ATTRIBUTE=cn // User attribute used to link member users
      from Group objects.
    }
}
```

You would modify the `LDAP_Server_Config` section only if your LDAP server is using other than the standard port (389). Similarly, if you select any of SASL or Kerberos authentication methods, edit the related sections of the `config` file as needed to match custom configurations.

Importing Users from XML files

If you select to import users from an XML File, the XML Data Source window displays.

The XML file containing user data must reside on the IDM server to use this option and contain information similar to the data shown in the "XML User Import File Example" on page 3-69.



To identify the XML file: 5.

1. In the **File name** field, type the complete path and name of the XML file.
2. Click **Next** to continue to the Extract Users and Groups window.

The remainder of the process for importing users from LDAP Servers is the same as described for importing users from Active Directories.

a. Select the Groups and Users to Import to IDM.
b. Select Users to remove from IDM (if applicable)
c. Commit the selected groups and users (adds and deletes) to IDM.

XML User Import File Example

XML files used to import user data to IDM should have the following format.

```
<?xml version='1.0' encoding='ISO-8859-7' ?>
    <DirData>
    <Domain name="domain name">
    <User name="username" description="user description"
displayName="user
     display name" />
    ...
    ...
    <Group name="group name" description="group description">
    <Member name="username"/>
    </Group>
    <Group name="other group" description="other group
description">
    </Group>
    </Domain>
    </DirData>
```

The description and displayName for the `User` element and the description for the `Group` element are optional.

Some `Group` elements may not have `Member` elements, for example the "`other group`" in the above example.

4

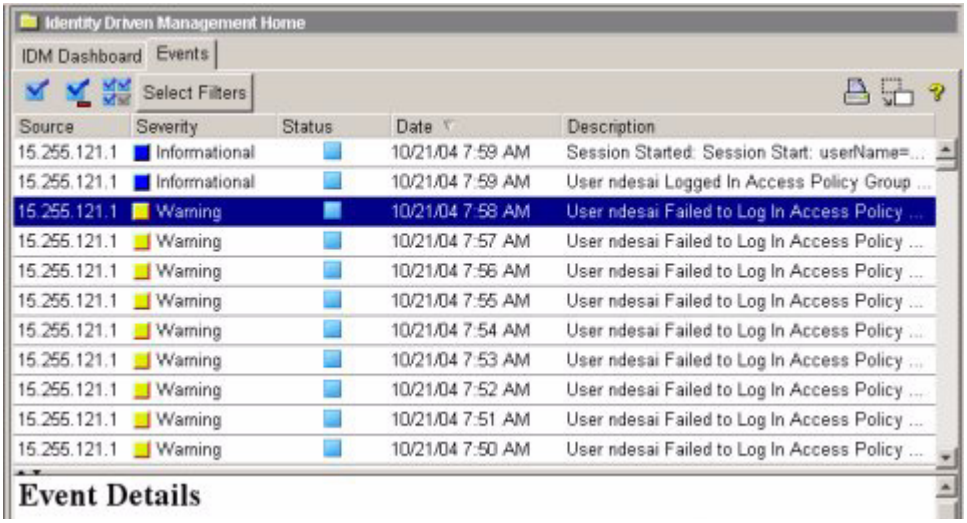
Troubleshooting IDM

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:

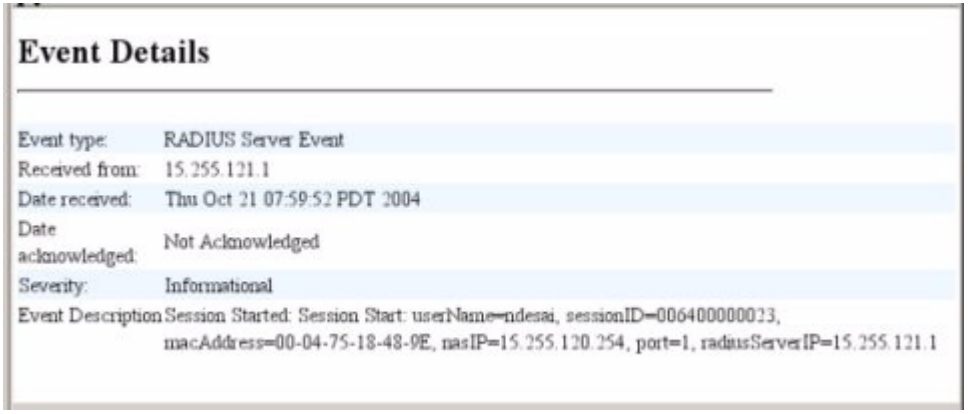
Column Heading	Description
Source	This column contains the name or IP address of the component or device that generated the event.
Severity	The Severity column shows the severity of each event. Events are categorized into five levels of severity.
Status	The Status column identifies whether the event 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.

The Event Log is trimmed at the level specified in the IDM Preferences window; by default there will be 1000 events in the event log.

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.

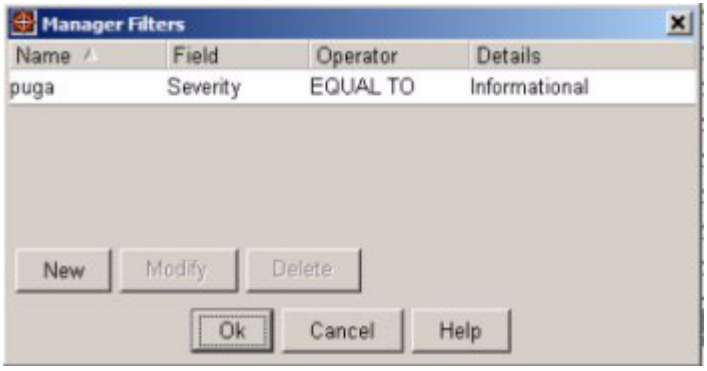
Deleting an event removes the event from the Events list and reduces the Event count in the IDM Dashboard window.

Using Event Filters

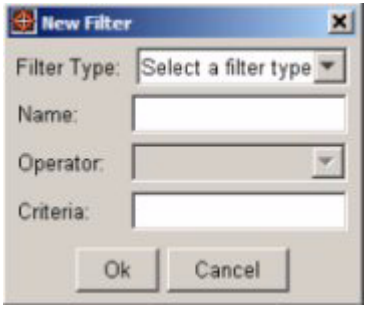
The events shown in the Events window can be filtered to show only specific types of events based on the device that generated the event, severity, date of occurrence, or description.

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".

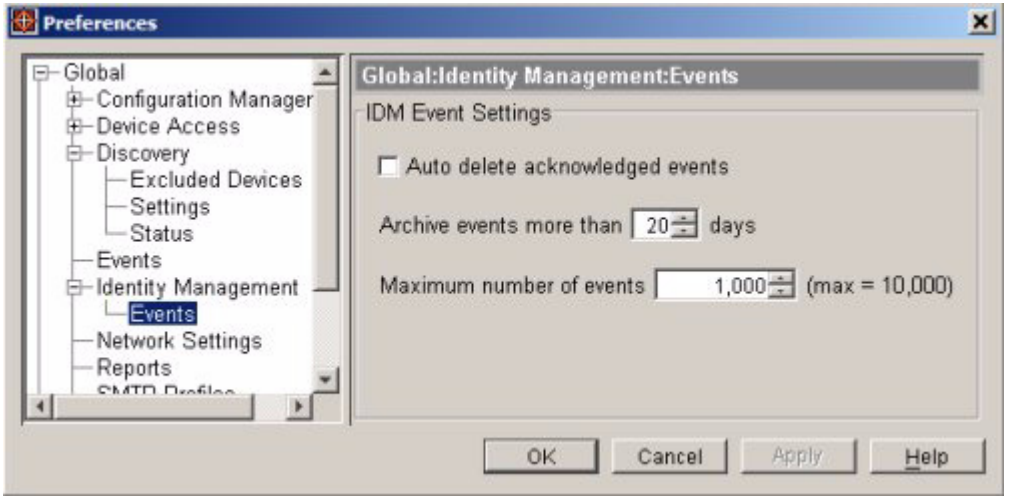
   The selected filter is deleted and the associated option is removed from the Select Filters drop-down menu on the Events tab.
5. Click **Ok** to exit the Manage Filters window.

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.



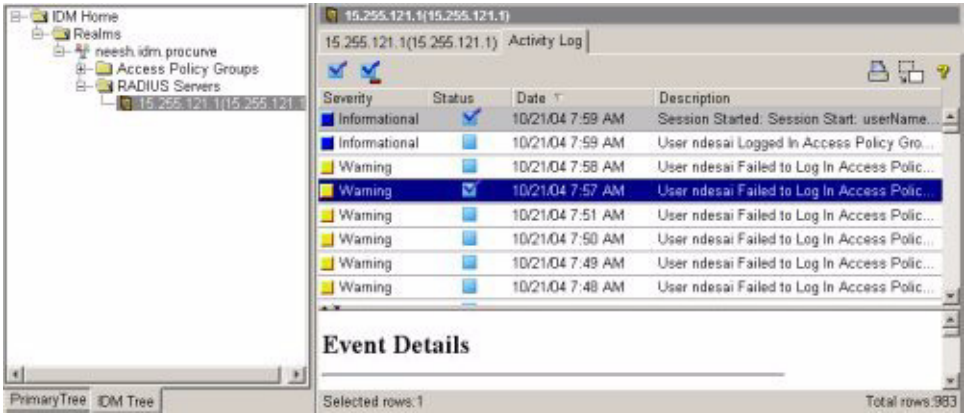
2. To delete IDM events once they are acknowledged, select the "Auto delete acknowledged events" checkbox.
3. In the Archive events more than "*x*" days field, click the up or down arrows or type the number of days to list events in the IDM Events window. Events are moved from the IDM Events window to 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, but the more severe events will be retained.
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.

Miscellaneous

For authenticating a MAC-Auth user using Funk Steel Belted RADIUS (SBR) with IDM, the password should be specified in lower-case (in the SBR User directory). If upper-case characters are used in the password, you may get the following error:

"MAC-Auth user gets rejected because of incorrect password".

The MAC-Auth user will be rejected by SBR and eventually by IDM2.0.

You can use the validate tool on SBR to verify if the MAC-Auth user password is in lower-case. If it is not, enter the MAC-Auth user password (MAC Address itself), in lower case.

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 at the time this manual was printed.

IDM Functions: / **Device Type:**	VLAN	QoS	Bandwidth	Network Resources
5300xl series	X	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.

Please check the ProCurve Web site (www.procurve.com) for the latest information on supported features and devices.

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 2-15 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 3-45 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

K

L

M

N

P

Q

R

S

T

U

W

X