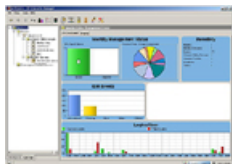


ProCurve Identity Driven Manager 2.3

ProCurve Identity Driven Manager (IDM), a plug-in to ProCurve Manager Plus, dynamically configures security and performance settings based on user, device, location, time, and device posture. IDM provides network administrators with the ability to centrally define and apply policy-based network access rights that allow the network to automatically adapt to the needs of users and devices as they connect, thereby enforcing network security while providing appropriate access to authorized network users and devices. IDM is a powerful tool that allows network administrators to efficiently manage the users and devices connecting to their network.



ProCurve Identity Driven
Manager 2.3 base
product--500-user license
(J9012A)

ProCurve Identity Driven Manager 2.3

Features and benefits

Additional information

• Ease of use:

- **Graphical user interface (GUI):** Identity Driven Manager provides a powerful GUI for defining network access policies and monitoring users on the network. Administrators can quickly see which users are currently on the network and easily drill down to know where and when they connected.

- **Auto-discovery of identity elements:** RADIUS servers with IDM agents, RADIUS realms, and users are automatically discovered and assigned to a default policy group for the administrator's attention.

- **Detailed reporting:** Identity Driven Manager provides reports of network access that can be automated to run at specified times or created on demand. Reports are useful for documenting network access by users and groups, as well as for investigating failed network access attempts in order to identify potential network attacks.

• Integration:

- **Integrates with Microsoft Network Access Protection:** Identity Driven Manager cooperates with Microsoft's Network Access Protection (NAP) in order to integrate the ProCurve Adaptive Network capabilities with endpoint validation from Microsoft NAP.

- **Integration with Active Directory:** Identity Driven Manager integrates with Active Directory to automatically map Active Directory group membership to IDM Access Policy Groups. Changes within Active Directory are automatically propagated to IDM and the new network access rights are enforced.

- **Import users from LDAP or XML file:** If current user data is not kept in Active Directory, Identity Driven Manager can read users and group membership from an LDAP directory or XML-formatted file.

- **Works with industry-standard RADIUS protocol:** Access policies are enforced based on RADIUS authentication, and Identity Driven Manager integrates with leading RADIUS authentication servers.

• Security:

- **Dynamic access rules based on time, location, and user system are formed by administrators and dynamically applied:** Access-policy groups have rules that are applied to each user in the group based on the time, location, and user system. These dynamic inputs are evaluated and the policies applied according to the user's profile, so the appropriate network access policies are applied at the right time and place.

- **Automatic VLAN assignment:** Users can be automatically assigned to the appropriate VLAN based on their identity, device, device status, location, and time of day.

- **Endpoint integrity verification:** When used with an endpoint integrity solution such as the ProCurve Network Access Controller 800 or Microsoft Network Access Protection (NAP), access policies can be set based on the posture of the endpoint connecting to the network, allowing non-compliant endpoints to be isolated until they comply with organization policies.

- **User-based access control lists (ACLs):** Users can be allowed or denied access to network resources (e.g., servers, printers) based on the destination IP address or a range of IP addresses, and/or to network services (e.g., Web pages, instant messaging, or FTP) based on well-known or user-defined TCP/UDP ports.

• Performance:

- **Traffic prioritization:** Traffic prioritization (QoS) can be automatically set for each connection based on user, device, location, and time of day, allowing appropriate prioritization of network traffic.

- **Rate limits:** Rate limits can be automatically applied to a session in order to limit the impact of lower-priority connections and reserve bandwidth for important business use.

• Resiliency and high availability:

- **The Identity Driven Manager agent can run independently and be deployed to redundant RADIUS servers:** The Identity Driven Manager agent can be deployed to each RADIUS server in the network. The agents are able to operate independently from the Identity Driven Manager server, allowing Identity Driven Manager to be deployed to multiple redundant RADIUS servers

ProCurve Identity Driven Manager 2.3

and providing authentication services for network devices.

- **Identity Driven Manager updates the server with transactional resilience:** The Identity Driven Manager agent uses a transaction process to update Identity Driven Manager server data. If the connection from the agent on the RADIUS server to the Identity Driven Manager server is broken, the agent will queue the data until the connection is restored and then transmit the data, as appropriate, back to the Identity Driven Manager database.

• **Device support:**

- **ProCurve intelligent edge switches:** 5400zl series, 5300xl series, 3500yl series, and 3400cl series

- **ProCurve traditional edge switches:** 6108, 4200vl series, 2900 series, 2800 series, 2610 series, 2600 and 2600-PWR series, and 2500 series

- **ProCurve wireless access points:** Access Point 530 and 420

- **ProCurve wireless edge services:** Wireless Edge Services zl and xl Modules

Industry-leading warranty

- 90-day media warranty, lifetime phone support

ProCurve Identity Driven Manager 2.3



ProCurve Identity Driven Manager 2.3 base product--500-user license (J9012A)

ProCurve Identity Driven Manager 2.3--add 2,000 users license (J9014A)

ProCurve Identity Driven Manager 2.3 base product (upgrade from 1.0) (J9013A)

Specifications

Please see ProCurve Manager Plus for system requirements.

This license adds support for an additional 2,000 users to the IDM base products of J9012A or J9013A.

Please see ProCurve Manager Plus for system requirements.

Recommended software

Browsers

Required platforms

Supported platforms

RADIUS server support

FreeRADIUS on SuSe Enterprise Linux (9.3 and 10.0)
FreeRADIUS on Red Hat Enterprise Linux (4.0 and 5.0)
Steel-Belted RADIUS on Windows (versions 5.3 and 5.4)
Microsoft Network Policy Server on Windows Server 2008 (32-bit)
Microsoft Internet Authentication Service (IAS) on Windows Server 2003 (32-bit)

FreeRADIUS on SuSe Enterprise Linux (9.3 and 10.0)
FreeRADIUS on Red Hat Enterprise Linux (4.0 and 5.0)
Steel-Belted RADIUS on Windows (versions 5.3 and 5.4)
Microsoft Network Policy Server on Windows Server 2008 (32-bit)
Microsoft Internet Authentication Service (IAS) on Windows Server 2003 (32-bit)

Features

Intuitive Explorer-style interface
OpenView NNM integration
Application of policies by user identity
- Auto VLAN assignment
- Auto set quality of service by user
- Auto set bandwidth assignment by user
Rule-based access rights deployment
Dynamic rights assignment based on:
- Time
- Location
- User system
Auto-discovery of:
- RADIUS servers
- Realms
- Users

Intuitive Explorer-style interface
OpenView NNM integration
Application of policies by user identity
- Auto VLAN assignment
- Auto set quality of service by user
- Auto set bandwidth assignment by user
Rule-based access rights deployment
Dynamic rights assignment based on:
- Time
- Location
- User system
Auto-discovery of:
- RADIUS servers
- Realms
- Users

Intuitive Explorer-style interface
OpenView NNM integration
Application of policies by user identity
- Auto VLAN assignment
- Auto set quality of service by user
- Auto set bandwidth assignment by user
Rule-based access rights deployment
Dynamic rights assignment based on:
- Time
- Location
- User system
Auto-discovery of:
- RADIUS servers
- Realms
- Users

Notes

Identity Driven Manager requires the ProCurve Manager Plus platform.
The base product for Identity Driven Manager allows for managing up to 500 users. Customers may add users in quantities of 2,000 by purchasing J9014A.

Requires the Identity Driven Manager base product (J9012).

This upgrade provides Identity Driven Manager 2.0, which allows for managing up to 500 users. Customers may add users in quantities of 2,000 by purchasing J9014A.

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.



7/30/2008
To learn more, visit www.procurve.com
Information is subject to change without notice