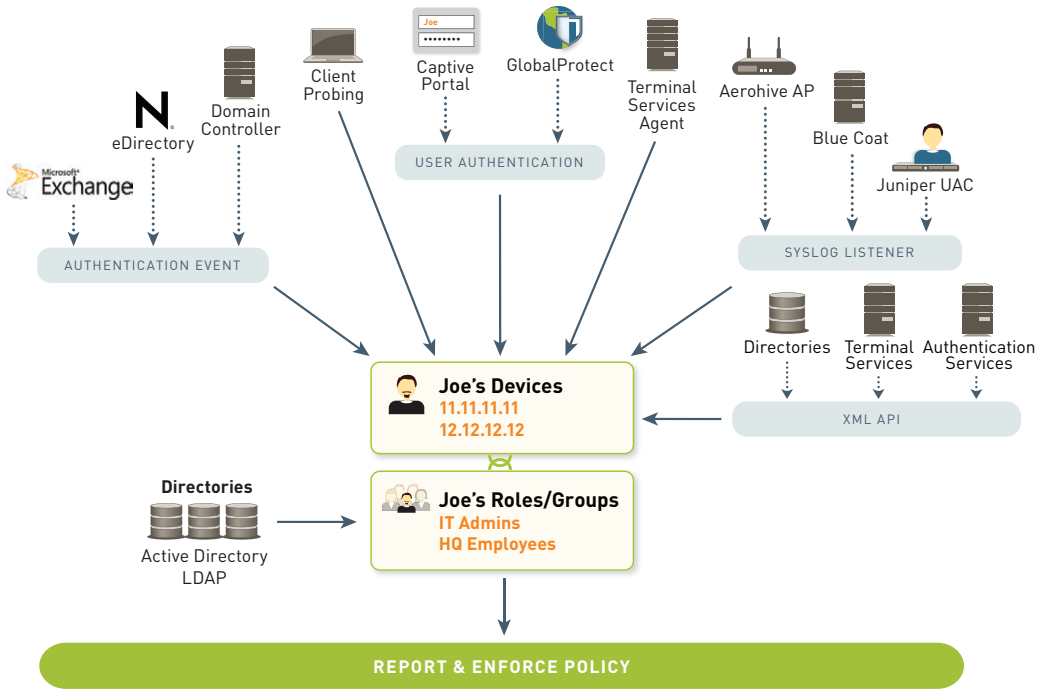
User-ID™



How User-ID works.

User-ID allows you to safely enable applications and content based on employee and group identity information stored in a wide range of user repositories.

- Extends user-based application enablement polices across Microsoft Windows, Mac OSX, Apple iOS and UNIX users.
- Analyzes application, threat and web surfing activity based on individual users and groups of users, as opposed to just IP addresses.
- Enables user information harvesting from enterprise directories (Microsoft Active Directory, eDirectory, Open LDAP) and terminal services offerings (Citrix, Microsoft Terminal Services).
- Integrates with Microsoft Exchange for user identification, provides a captive portal and an XML API enabling you to extend policies to Mac OSX, Apple iOS and UNIX users that typically reside outside of the Active Directory domain.

User-ID is a standard feature of our enterprise security platform that seamlessly integrates with a range of enterprise directories and terminal services, enabling you to gain visibility into usage patterns regardless of device type, determine security policies, generate reports and perform forensics based on users and groups—not just IP addresses. When used in conjunction with App-ID™ and Content-ID™, your security infrastructure is based on three pillars of your business—the application, the user and the associated content thereby strengthening your overall security posture.

Compounding the visibility problem in an increasingly mobile enterprise, where employees access the network from virtually anywhere around the world, internal wireless networks re-assign IP addresses as users move from zone to zone, and network users are not always company employees. The result is that the IP address is now an inadequate mechanism for monitoring and controlling user activity.

paloalto NETWORKS®

the network security company™

User-ID: Integrating User Information into Your Security Infrastructure

The user identity, as opposed to an IP address, is an integral component of your security infrastructure. Knowing which who is using each of the applications on your network; who may have transmitted a threat, or is transferring files can strengthen security policies and reduce incident response times. User-ID enables you to leverage user information stored in a wide range of repositories for the following uses:

- **Visibility:** Improved visibility into application usage based on user and group information can help you maintain a more accurate picture of network activity.
- **Policy control:** Tying user information to the security policy to safely enable applications or specific application functions while reducing the administrative effort associated with employee moves, adds and changes.
- **Logging, reporting, forensics:** In the event that a security incident occurs, forensics analysis and reporting can include user information, again, providing a more complete picture of the incident.

How User-ID Works

User-ID integrates our next-generation firewall functionality with a wide range of user repositories and terminal services environments. Depending on your network requirements, multiple techniques can be configured to map the user identity to an IP address. User mapping techniques include authentication events, user authentication, terminal services monitoring, client probing, directory services integration and a powerful XML API. Once the applications and users are identified, full visibility and control within Application Command Center (ACC), policy editing, logging and reporting is available.

Authentication events: User-ID can be configured to monitor authentication events for Microsoft Active Directory, Microsoft Exchange and Novell eDirectory environments. Monitoring of the authentication events on a network allows User-ID to associate a user with the IP address of the device the user logs in from to enforce policy on the firewall.

- **Microsoft Exchange Server:** User-ID can be configured to constantly monitor the Microsoft Exchange logon events produced by clients accessing their email. Using this technique, even MAC OS X, Apple iOS, Linux/UNIX client systems that don't directly authenticate to Microsoft Active Directory can be discovered and identified.
- **Novell eDirectory:** User-ID can query and monitor logon information to identify users and group memberships via standard LDAP queries on the Novell eDirectory servers.
- **Microsoft Active Directory:** User-ID constantly monitors domain controller event logs to identify users when they log onto the domain. When a user logs onto the Windows domain, a new authentication event is recorded on the corresponding Windows Domain Controller. By remotely monitoring the authentication events on Windows Domain Controllers, User-ID can recognize those authentication events to identify users on the network for creation and enforcement of policy.

User authentication: This technique allows you to configure a challenge-response authentication sequence to collect user and IP address information.

- **Captive portal:** In cases where administrators need to establish rules under which users are required to authenticate to the firewall prior to accessing the internet, a captive portal can be deployed. Captive portal is used in cases where the user cannot be identified using other mechanisms. In addition to an explicit username and password prompt, captive portal can also be configured to send an NTLM authentication request to the web browser in order to make the authentication process transparent to the user.
- **GlobalProtect™:** Remote users logging into the network with GlobalProtect will provide user and host information to the firewall that in turn, can be used for policy control.

Client probing and terminal services: This technique allows you to configure User-ID to monitor Windows clients or hosts to collect the identity and map it to the IP address. In environments were the user identity is obfuscated by Citrix XenApp or Microsoft terminal Services, the User-ID Terminal Services Agent can be deployed to determine which applications users are accessing.

- Client probing: If a user cannot be identified via monitoring authentication events, User-ID actively probes Microsoft Windows clients on the network for information on the currently logged on user. Using this mechanism, laptop users who often switch from wired to wireless networks can be reliably identified.
- **Host probing:** User-ID can also be configured to probe Microsoft Windows servers for active network sessions of a user. As soon as a user accesses a network share on the server, User-ID identifies the origin IP address and maps it to the user name provided to establish the session.
- **Terminal services:** Users sharing IP addresses working on Microsoft Windows Terminal Services or Citrix can be identified. Completely transparent to the user, every user session is assigned a certain port range on the server, which allows the firewall to associate network connections with users and groups sharing one host on the network.

Syslog Listener: In environments with existing network services that authenticate users, such as wireless controllers, 802.1x devices, Apple Open Directory servers, or other Network Access Control (NAC) mechanisms, the firewall can now listen for syslog messages from those services so that the User-ID agent (either the Windows agent or the agentless user mapping feature on the firewall) can extract the authentication events from the logs. Syslog filters that you define allow User-ID to parse the messages and extract the IP addresses and usernames of users who successfully authenticated to the external service and add the information to the IP address to username mappings it maintains. Currently the syslog listener natively supports BlueCoat Proxy, Citrix Access Gateway, Aerohive AP, Cisco ASA, Juniper SA Net Connect, and the Juniper Infranet Controller.

- XML API: In cases where the syslog listener is not applicable, the User-ID XML API allows you to integrate user information into your security policies from other user directories, terminal services and authentication mechanisms

Directory integration: To allow customers to specify security policies based on user groups and resolve the group members automatically, User-ID integrates with nearly every directory server using a standards based protocol and a flexible configuration. Once configured, the firewall automatically retrieves user and user group information and keeps the information updated to automatically adjust to changes in the user base or within your organization.

- **Directory integration:** Microsoft Active Directory: In any other LDAP based directory service, the firewall can retrieve user and group information via standard LDAP from most LDAP based directory servers. The association of users to computers can be achieved through other means, for example Captive Portal or XML API.

Visibility into a User's Application Activity

The power of User-ID becomes evident when a strange or unfamiliar application is found on your network by App-ID. Using either ACC or the log viewer, your security team can discern what the application is, who the user is, the bandwidth and session consumption, along with the source and destination of the application traffic as well as any associated threats.

Visibility into the application activity at a user level, not just an IP address level, allows you to more effectively enable the applications traversing the network. You can align application usage with the business unit requirements and if appropriate, can chose to inform the user that they are in violation of corporate policy, or take a more direct approach of blocking the user's application usage outright.

User-based Policy Control

User-based policy controls can be assembled based on the application, which category and subcategory it belongs in, its underlying technology or what the application characteristics are. Policies can be used to safely enable applications based on users or groups, in either an outbound or an inbound direction. Examples of user-based policies might include:

- Enable only the IT department to use tools such as SSH, telnet, and FTP on their standard ports.
- Allow the Help Desk Services group to use Yahoo Messenger.
- Allow Facebook for all users, yet allow only marketing to use Facebook-posting and block the use of Facebook-apps for all users.

User-based Analysis, Reporting and Forensics

Informative reports on user activities can be generated using any one of the pre-defined reports or by creating a custom report. Custom reports can be quickly created from scratch or by modifying a pre-defined report. Any of the reports—predefined or custom—can be exported to either CSV or PDF, or emailed on a scheduled basis to an interested manager or an HR group.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com