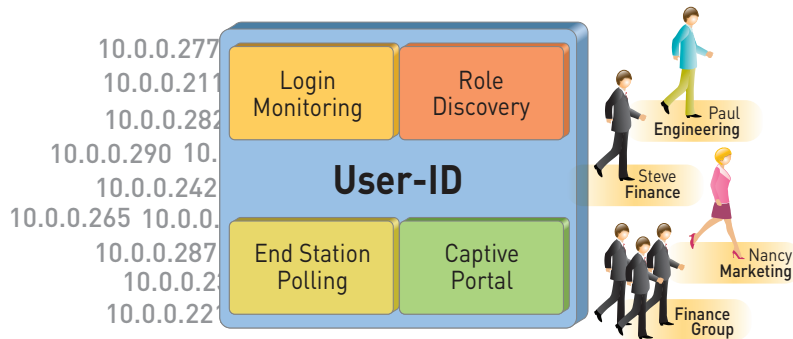


# User-ID



User-ID seamlessly integrates Palo Alto Networks firewalls with enterprise directory services including Active Directory, LDAP and eDirectory, enabling administrators to tie network activity to users and groups – not just IP addresses. When used in conjunction with App-ID and Content-ID technologies, IT organizations can leverage user and group information for visibility, policy creation, forensic investigation and reporting on application, threat, web surfing and data transfer activity.

User-ID helps address the challenge of using IP addresses to monitor and control the activity of specific network users – something that was once a fairly simple task, but has become difficult as enterprises moved to an Internet- and web-centric model.

Compounding the visibility problem is 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.

User-ID enables policy control over applications and content based on the employee and group identity through seamless integration with enterprise directory services including Active Directory, LDAP and eDirectory.

- Perform analysis on application, threat and web surfing activity based on individual users and groups of users, as opposed to just IP addresses.
- Identify Citrix and Microsoft Terminal Services users and apply policy controls over their respective application usage.
- Build policies to positively enable application usage for specific groups such as marketing, IT, and sales.

### Visibility and Control Over User Activity

User-ID seamlessly integrates Palo Alto Networks firewalls with enterprise directory services such as Active Directory, eDirectory, LDAP, and Citrix, enabling administrators to leverage user and group data for application visibility, policy creation, logging and reporting. The Palo Alto Networks User Identification Agent communicates with the domain controller, mapping the user information to the IP address that they are using at a given time. On a configurable basis, the User Identification Agent uses multiple techniques to verify and maintain the user to IP address relationship:

- **Login monitoring:** Login activity is monitored to correlate IP address to user and group info when a user logs in to the domain.
- **End station polling:** Each active PC is polled to verify IP address information to maintain accurate mapping when users move around the network without re-authenticating to the domain.
- **Captive portal:** Associates user and IP address in cases where hosts are not part of the domain via a web page-based authentication form.

In addition, the User Identification Agent maintains an up-to-date mapping of users to their assigned roles or groups. User-ID works with the existing infrastructure, eliminating any requirements to duplicate user and group information on a separate device and there is no need to install an agent on every PC.

### Identifying Citrix/Terminal Server Application Activity

In environments where user identity is obfuscated by a Citrix or Terminal Server deployment, a User-ID agent can be deployed to determine which applications Citrix users are accessing. If an enterprise directory service is in use, user and group information (not IP address) will be displayed. Once the applications and users are identified, full visibility and control within Application Command Center, policy editing, logging and reporting is available.

### Visibility into User's Application Activity

The power of User-ID becomes evident when an administrator finds a strange application on the network (revealed through App-ID™ technology), and with a click of a mouse, can quickly determine whether it is a single user or a larger group that is using the application. The administrator not only sees all the users of the individual application, but also the bandwidth and session consumption, the sources and destinations of the application traffic as well as any associated threats. Investigating the other applications that an individual user may be accessing is as easy as selecting their user name with a mouse click. The administrator can then see the different applications used, the bandwidth and sessions consumed, as well as threats.

Visibility into the application activity at a user level, not just an IP address level, is a required step in regaining control over the applications traversing the network. Administrators can align application usage with the business unit requirements

The image displays three overlapping screenshots of the Palo Alto Networks Application Command Center (ACC) interface. The top screenshot shows the main dashboard with a risk score of 3.9 and a table of applications. The middle screenshot shows detailed information for the 'facebook-base' application, including its description and category. The bottom screenshot shows a drill-down view for a specific user, 'pandemo/ginger.poppe', listing top applications and their session counts.

**Application Command Center (ACC) Dashboard**

Risk	Application	Sessions
1	web-browsing	178,327
2	dns	72,676
3	bittorrent	41,789
4	ssl	31,276
5	unknown-udp	9,889
6	secureus	7,424
7	blackboard	6,721
8	facebook-base	5,004

**URL Filtering**

Category	Sessions
1 educational-institutions	42,158
2 web-advertisements	24,233
3 parked-domains	18,795
4 business-and-economy	17,113
5 personal-sites-and-blogs	11,981

**Threat Prevention**

Severity	Threat	ID
1 MEDIUM	FTP: login brute force attempt	40001
2 INFORMATIONAL	HTTP OPTIONS Method	30520
3 CRITICAL	Bot: Mariposa Command and Control	12652

**Application Information: facebook-base**

Name: facebook-base  
 Related: Facebook  
 Description: Facebook (branded as "facebook") is a social networking website launched on February 4, 2004. The free-access website is privately owned and operated by Facebook, Inc. Users can join networks organized by city, workplace, school, and region to connect and interact with other people. People can also add friends and send them messages, and update their personal profile to notify friends about themselves. The website's name refers to the paper Facebooks depicting members of a campus community that some American colleges and preparatory schools give to incoming students, faculty, and staff as a way to get to know other people on campus. Features include a Wall for posting messages and Photos for uploading digital photos. The website has more than 80 million active users worldwide. Facebook has met with some controversy over the past few years. It has been blocked in several countries including Syria and Iran. Privacy has also been an issue, and it has been compromised several times. It is also facing several lawsuits from a number of Zuckerberg's former classmates, who claim that Facebook had stolen their source code and other intellectual property.  
 Category: collaboration

**Top Applications**

Risk	Application	Sessions	Bytes
1	web-browsing	725	11,419,787
2	dns	252	86,028
3	msn	198	1,025,004
4	facebook-base	136	2,285,256
5	myspace-base	42	244,674
6	flash	31	639,699
7	myspace-in	8	134,398
8	myspace-video	4	2,218,964
9	facebook-chat	2	55,838
10	ssl	2	9,912

**Source User: pandemo/ginger.poppe**

Risk	Application	Sessions	Bytes
1	facebook-base	5,005	44,912,456

**Top Sources**

Source address	Source Host Name	Source User
1 10.154.12.89	engr89.net12.bigeduo.local	pandemo/ginger.p

### Visibility into a User's Application Activity

Quickly drill down into unusual application activity to determine who is using the application. Additional drill down shows other applications for individual users.

Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile
1 Allow Yahoo!M--Helpdesk	trust	untrust	any	helpservicesgroup	any	yahoo-im	any	✓	none
2 Allow MS-RDP--Server Ops	trust	untrust	any	server operators	any	ms-rdp	application-default	✓	none
3 Block P2P	trust	untrust	any	any	any	p2p file sharing	any	✗	none
4 Allow BitTorrent	trust	untrust	any	akendall	any	bittorrent	any	✓	none

### Policies Based on Users and Groups

Assign policies that dictate the users and groups that are allowed to use different applications.

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

The increased visibility into the application usage that is generated by App-ID means the security team can quickly analyze the role and risk of applications, who is using them, then easily translate that information into user-based application control policies. The ability to control applications based on users and groups, as opposed to IP addresses is a key differentiator for Palo Alto Networks. 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 control application access for specific 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 the standard port.
- Allow the Help Desk Services group to use Yahoo Messenger.
- Block the use of all file sharing applications that use P2P technology except for A. Kendall, who is allowed to use BitTorrent for file transfer purposes.

### User Identity in Logging and Reporting

Access to the user and group information for visibility and control over application and threat activity is pervasive throughout the Palo Alto Networks next generation firewalls. Application Command Center provides an initial view into user activity with the log viewer providing more fine-grained forensic analysis. Administrators can easily create log filters by clicking on a cell value, which can be expanded by combining additional log fields and adding multiple criteria using the expression builder. Any log results can be exported for additional analysis. Policy controls can be exerted over all users, a single user or a group of users based on the information stored within a directory service.

Informative reports on user activities can be generated using any one of the many 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.



**Palo Alto Networks**  
 232 E. Java Drive  
 Sunnyvale, CA. 94089  
 Sales 866.320.4788  
 408.738.7700  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

Copyright ©2010, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN-OS 3.1, March 2010.