

Palo Alto Networks User-ID Services

Unified Visitor Management



Technical Note

Copyright

© 2011 Aruba Networks, Inc. Aruba Networks trademarks include Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com
1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

1	Introduction	4
	Audience	4
	Document Overview.....	4
	Disclaimer	4
2	About Palo Alto Networks User-ID Services	5
	Overview	5
	Palo Alto Networks User-ID Services Architecture	6
3	Network Design	7
4	Configuring Palo Alto Networks User-ID Services	8
	Check Plugin Versions	8
	Accessing Palo Alto Networks User-ID Services	8
	Configuring the Palo Alto Networks User-ID Service	9
	Check Palo Alto Networks Version and Setup	10
	Configuring User-ID Agent Definition	11
	Enable Zone Based User Identification	12
	Configuring User-ID Agent Software	12
5	Verify Integration	15
	Create Test Account in Amigopod	15
	Login to Guest Wireless Network	15
	Verify Wireless Connection and IP Addressing	15
	Login via Captive Portal page.....	16
	Verify Successful RADIUS Authentication	16
	Verify Successful Wireless Authentication.....	16
	Monitor User-ID Agent.....	16
	Verify User Identity Availability.....	18
	Logout and Verify User Mapping Removed	19
6	Summary	20

1 Introduction

This technical note demonstrates how Palo Alto Networks customers can leverage Amigopod to provide User Identity tracking for both known corporate users (via Active Directory, eDirectory etc) and now Guest &/or Public Access users accessing the Internet through their Guest Access or Hotspot networks.

Audience

This document is intended for network administrators and system integrators deploying an Amigopod-based visitor management solution in conjunction with a Palo Alto Networks Next Generation firewall.

Basic familiarity with the Amigopod Visitor Management Appliance is assumed. For in-depth information about the features and functions of the Amigopod appliance, refer to the Amigopod Deployment Guide.

Some familiarity with the Palo Alto Networks firewall range is assumed, including knowledge of their User-ID technology, Virtual-Wire deployment mode and their web based User Interface.

Document Overview

The first section of this document describes how the Amigopod Visitor Management Appliance can be used to provide end-user identity visibility to many of the Palo Alto Networks Policy and Reporting features built on top of their core User-ID technology.

The next section contains a detailed configuration guide for administrators intending to deploy Palo Alto Networks User-ID Services on the Amigopod Visitor Management Appliance. Step-by-step instructions for configuring and validating a configuration are provided.

Disclaimer

The topics of network design, security architectures and visitor access are complex subjects, and no single document can hope to cover all of the possible combinations of network equipment, network design, deployment requirements, and device configurations, nor can all the possible security implications for a particular recommendation be covered.

Therefore, while you read this document, it is best to consider it as a guide to developing your own understanding of the network design topics covered, and as a basis for further investigation.

2 About Palo Alto Networks User-ID Services

Overview

Palo Alto Networks have developed a range of Next Generation firewalls that redefine the best practice for controlling and securing today's networks. Leveraging their core strengths of Application, User and Content Identification, Palo Alto Networks provides a unique approach to addressing the challenges surrounding Web 2.0 applications and peer to peer communications which dominate the concerns of IT Administrators.



Palo Alto Networks define their User-ID technology as offering the following benefits in a traditional enterprise environment:

User-ID seamlessly integrates Palo Alto Networks firewalls with Microsoft Active Directory (AD), 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.

Amigopod, with the introduction of the Palo Alto Networks User-ID Services plugin, can now extend this visibility to include non-corporate users typically associated with Enterprise Guest Access deployments, Hotels, Conference venues, Airports and other Hotspot style deployments.

Palo Alto Networks User-ID Services Architecture

Amigopod is typically deployed in conjunction with a Wired or Wireless Access Controller to provide a clean branded user experience, user session management and many other innovative enhancements to a traditional Guest or Public Access solution.

The additional of an upstream Palo Alto Networks firewall adds a wealth of security and traffic management features to these networks.

As discussed previously the Palo Alto Networks User-ID technology allows all sessions passing through (or visible via TAP interface) the firewall to be associated with the source Enterprise user's identity by integrating with Active Directory or Novell eDirectory, for example.

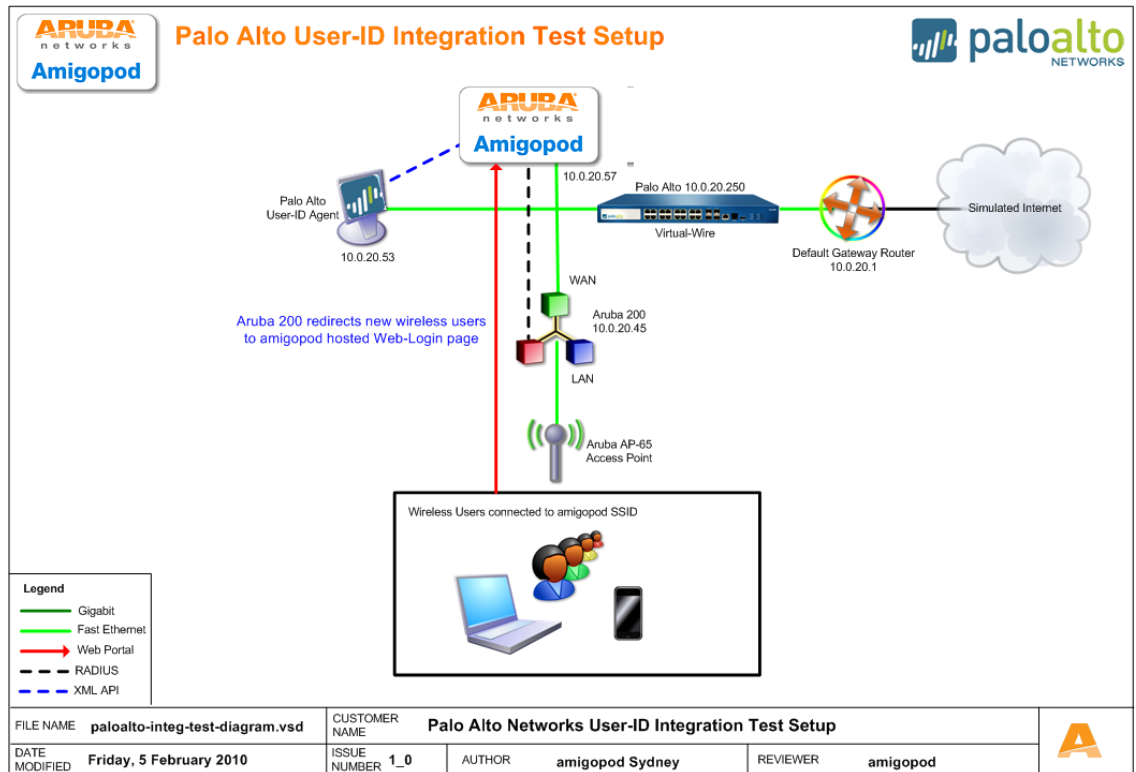
Typical Wired and Wireless Access Controllers have basic firewalling and traffic management features whilst granular application control, content filtering, anti-virus etc is passed onto purpose built platforms in the network DMZ.

The challenge arises on these devices that they have no visibility of the users associated with the traffic they are processing and therefore are unable to make policy decisions based on user identity or collect audit and forensic reports where the end user responsible for "interesting" traffic is identified.

With the introduction of the Palo Alto Networks firewall performing these functions, this lack of user visibility is removed through the tight integration with Amigopod's user authentication process.

3 Network Design

The following diagram shows a sample network architecture where a typical Guest Access network is delivered by an Aruba Networks wireless solution. The Aruba controller that performs authentication and access control tasks for the wireless users has been complemented by the integration of both the Amigopod and Palo Alto Networks technology. It should be noted that the integration with Palo Alto Networks technology is possible using other Amigopod supported NAS devices such as wireless/wired controllers from other enterprise manufacturers.



An integral part of Palo Alto Networks current User-ID solution is the User-ID Agent, which is installed on a Windows host machine on the network. For the Microsoft Active Directory integration the User-ID agent is installed on a domain workstation or server and uses a domain account that has access to the Active Directory tree.

For the Amigopod integration, the User-ID agent can be installed on any network connected Windows host that has IP access to both the Palo Alto Networks firewall and the Amigopod Visitor Management Appliance.

As can be seen in the above diagram, the User-ID agent deployed in the sample network design has been allocated an IP Address of **10.0.20.53** and communicates with both the Amigopod and the Palo Alto Networks firewall across the local network.

Once the Palo Alto Networks is configured to support the User-ID service as detailed in the next section, an outbound connection will be made to the IP Address of the Windows host running the User-ID Agent. It is essential that any host based firewalling implemented on this Windows device be modified to permit this style of traffic from both the firewall and Amigopod API processes.

4 Configuring Palo Alto Networks User-ID Services

Check Plugin Versions

Pushing user identity information to a Palo Alto Networks firewall requires the following Amigopod plugin versions:

- Amigopod Kernel 2.1.7 or later
- RADIUS Services Plugin 2.1.7 or later
- Guest Manager Plugin 2.1.6 or later
- Palo Alto Networks Networks Services 0.6.0 or later

To verify you have the correct plugin versions installed, navigate to **Administrator > Plugin Manager > Manage Plugins** and check the version number in the list.

Use the **Update Plugins** link to download and install updated plugins.

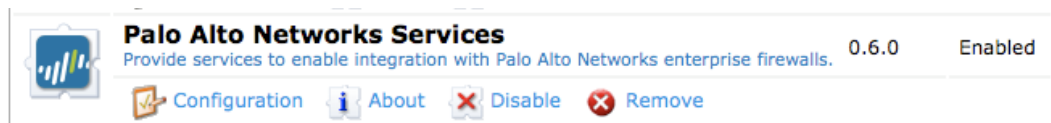
It is assumed that the configuration steps required to integrate the chosen Wired or Wireless Access Controller have been completed, tested and known to be working in isolation from any of these integration steps.

For more information on integrating Wired and Wireless Access Controllers with the Amigopod solution, please refer to our extensive database of detailed Integration Guides with the leading manufacturers.

Accessing Palo Alto Networks User-ID Services

Log in to the Amigopod Visitor Management Appliance's graphical user interface as an administrator.

Navigate to **Administrator > Plugin Manager > Manage Plugins** and you will find the installed Palo Alto Networks Services Plugin.

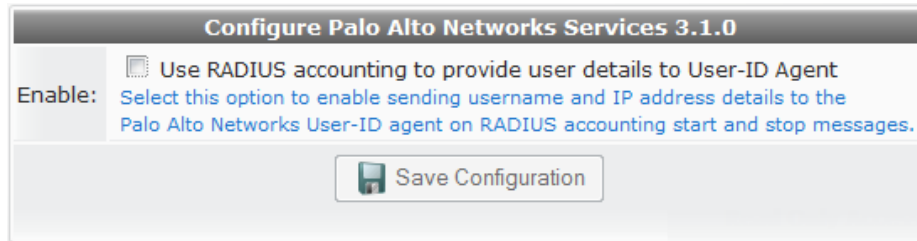


Ensure that the plugin is **Enabled** as shown above.

Configuring the Palo Alto Networks User-ID Service

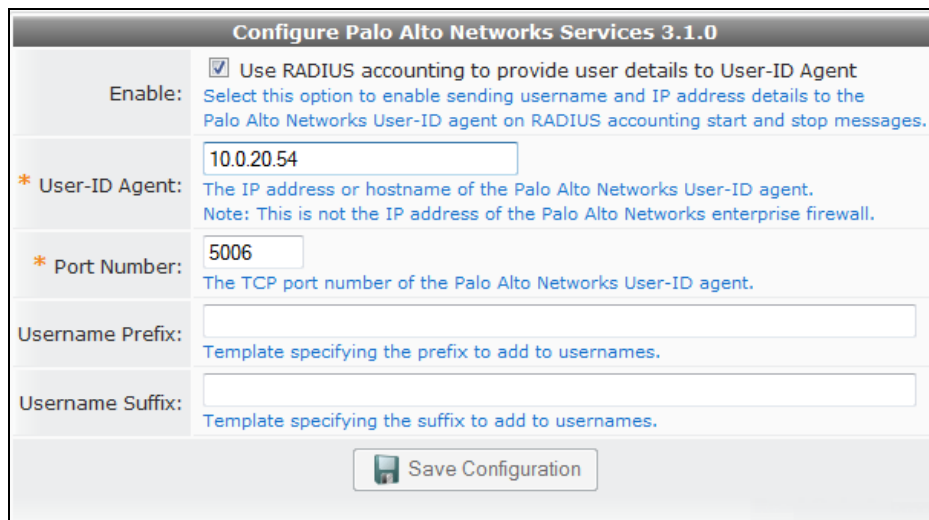
To configure the Palo Alto Networks plugin:

1. Click on the **Configuration** option of the Palo Alto Networks Plugin shown in the Manage Plugins list.



2. To start the XML API service, click the **Enable** checkbox to enable the plugin.

Amigopod leverages its advanced RADIUS authentication engine to allow the Palo Alto Networks XML API calls to be made every time there is a successful RADIUS login or logout. As the description implies, the API calls are triggered by the receipt of RADIUS accounting start and stop messages. It is essential the Wired or Wireless Access Controller must be configured correctly to support RADIUS accounting otherwise the Palo Alto Networks firewall will not be updated with the real time user identity information.



3. Configure the following settings:
 - **User-ID Agent:** The IP Address of the User-ID Agent installed on the Windows host must be configured at this step. The Palo Alto Networks firewall does not accept direct API calls and all communications must flow through the User-ID Agent so it is critical that this IP Address is of the Agent and not the firewall itself.
 - **Port Number:** The default port number that the Palo Alto Networks User-ID Agent listens to for inbound XML API calls is 5006. This is user configurable on both the Amigopod and User-ID Agent.
 - **Username Prefix:** The Palo Alto Networks plugin versions 0.7.0 and later allow you to optionally specify a prefix to add to usernames, e.g., GUEST\

- **Username Suffix:** The Palo Alto Networks plugin versions 0.7.0 and later allow you to optionally specify a suffix to add to usernames, e.g.,
`#{ $user.sponsor_name }`
4. Click **Save Configuration** to save your settings. The configuration of the plugin is complete.

Check Palo Alto Networks Version and Setup

Palo Alto Networks firewalls and Agent Software are required to be running the following software releases in order to support the XML API for the User-ID integration:

- Firewall Software Version 3.1.0 or later
- User-ID Agent Software Version 3.1.0 or later

In the test environment referenced in this document, the Palo Alto Networks firewall was deployed in a simple **VWire** or virtual wire deployment mode as shown below.

Interfaces										
Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN/ Virtual Wire	Security Zone	Features	
ethernet1/1	VWire					Untagged	default-vwire	untrust		
ethernet1/2	VWire					Untagged	default-vwire	trust		

In a virtual wire deployment, the firewall is installed transparently on a network segment by binding two ports together. You can install the firewall in any network environment with no configuration of adjacent network devices required. If necessary, a virtual wire can block or allow traffic based on the virtual LAN (VLAN) tag values. By default, the virtual wire “default-vwire” binds together Ethernet ports 1 and 2 and allows all untagged traffic.

This configuration will not suit all deployments and it is not a mandatory requirement for the integration with Amigopod. The actual design and deployment of the Palo Alto Networks firewall is outside of the scope of this document and the reader is encouraged to consult the Palo Alto Networks documentation and/or their Palo Alto Networks Networks reseller or representative.

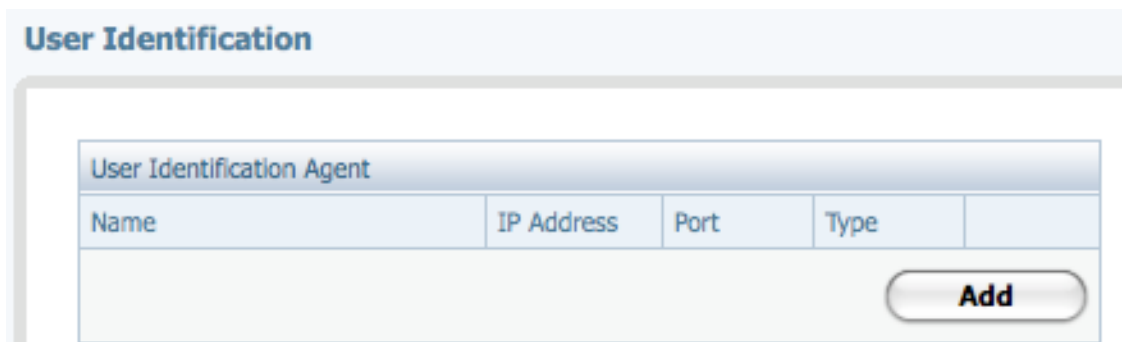
A very simplistic **Policy** configuration has been adopted for the test environment that is forwarding bi-directional traffic between the **Trust** and **UnTrust** zones.

Security Rules											
	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	rule1	trust	untrust	any	any	any	any	any			
2	rule2	untrust	trust	any	any	any	any	any			

Again this configuration will certainly not suit all deployments but Palo Alto Networks policy definitions are considered to be out of scope for this document.

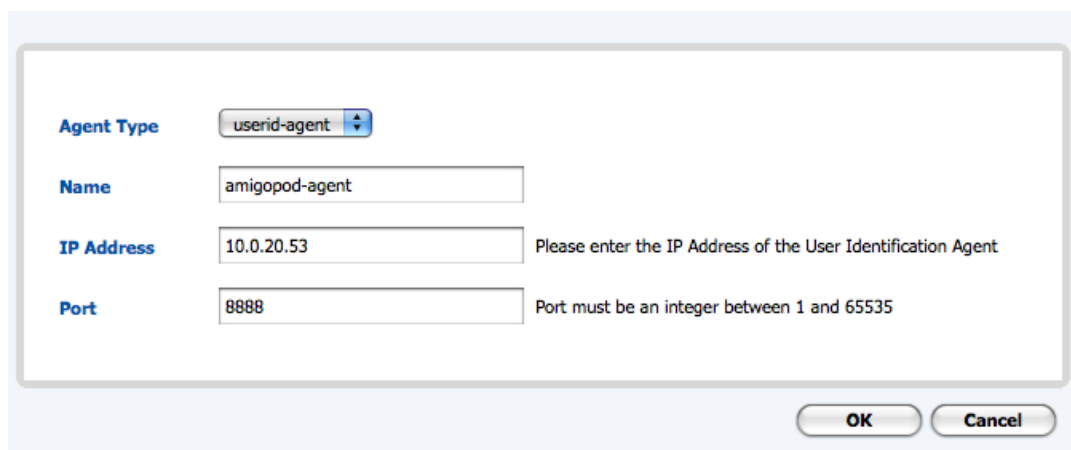
Configuring User-ID Agent Definition

From the **Device > User Identification** screen click **Add** under the **User Identification Agent** section shown below:



The screenshot shows the 'User Identification' configuration page. At the top, there is a header 'User Identification Agent'. Below it is a table with the following columns: Name, IP Address, Port, and Type. The table is currently empty. To the right of the table is an 'Add' button.

From the resulting screen enter the IP Address details of the Windows Host you have installed the Palo Alto Networks User-ID Agent software. In our test environment the Windows host has an IP Address of **10.0.20.53**.



The screenshot shows a configuration dialog box for the User Identification Agent. It contains the following fields and values:

- Agent Type:** A dropdown menu with 'userid-agent' selected.
- Name:** A text input field containing 'amigopod-agent'.
- IP Address:** A text input field containing '10.0.20.53'. To the right of the field is the text: 'Please enter the IP Address of the User Identification Agent'.
- Port:** A text input field containing '8888'. To the right of the field is the text: 'Port must be an integer between 1 and 65535'.

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

A port must also be defined for communications between the Palo Alto Networks firewall and the User-ID Agent software on the Windows host. Ensure to make note of your chosen port number as this configuration will need to be matched on the User-ID Agent configuration in the subsequent section.

Also this port will need to be permitted through any Access Control Lists or Firewall rules that may exist elsewhere on the network between these two devices or potentially on the host based firewall running on the Windows host.

Enable Zone Based User Identification

An additional step is required to enable the User Identification process on the Palo Alto Networks firewall is based on the configuration of the **Zones** that any interesting traffic with pass through.

In our test environment all traffic is passing between the **Trust** and **UnTrust** zones so it is these zones whose configuration will need modification.

From the **Network > Zones** menu option, select each Zone in question and ensure the **Enable User Identification** option shown below is checked.

The screenshot shows the configuration page for a Zone named 'trust'. The 'Zone' field is set to 'trust', the 'Type' is 'Virtual Wire', and the 'Interfaces' list includes 'ethernet1/2'. The 'Zone Protection Profile' and 'Log Setting' are both set to 'None'. The 'Enable User Identification' checkbox is checked. The 'User Identification ACL' section is visible, showing 'Include List' and 'Exclude List' fields. The 'Include List' field is empty, and the 'Exclude List' field is also empty. Below each list is a text input field and an 'Add' button. The text below the input fields reads: 'Select an address or address group or type in your own address (must be of the form IP Address (ex. 192.168.1.20) or IP Address/Mask (ex. 192.168.1.0/32))'. At the bottom right of the configuration page are 'OK' and 'Cancel' buttons.

Once you have edited each relevant **Zone** in your deployment, the summary table should look similar to this with the **User Identification** feature clearly enabled on each **Zone**.

At this point the configuration of the Palo Alto Networks firewall is complete. For the changes to take affect you must ensure the Commit button is clicked to save the changes.

Zones						
	Name	Type	Interfaces / Virtual Systems	Protection Profile	Log Setting	Enable User Identification
<input type="checkbox"/>	trust	virtual-wire	ethernet1/2			✓
<input type="checkbox"/>	untrust	virtual-wire	ethernet1/1			✓

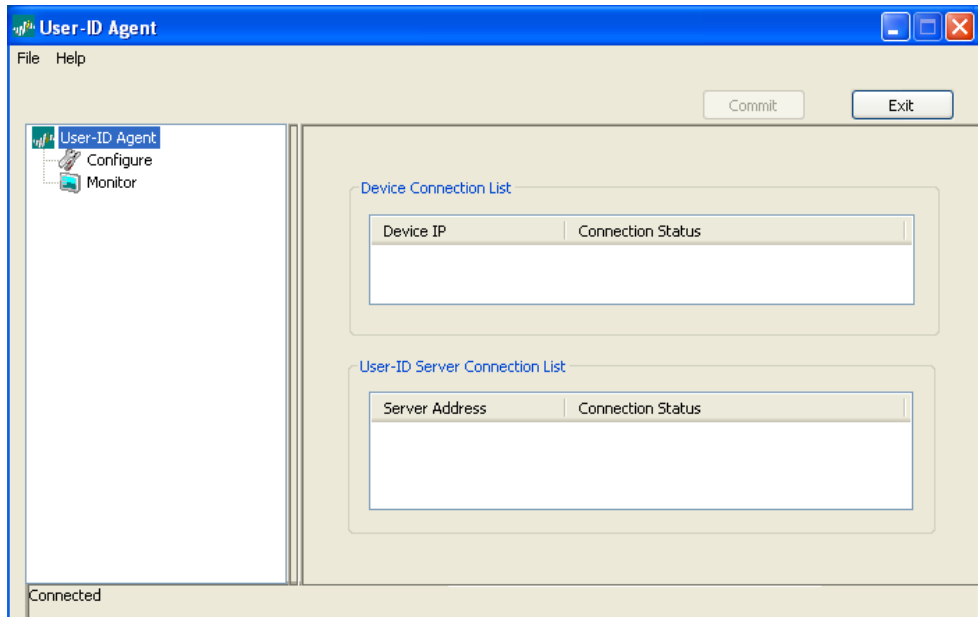


Configuring User-ID Agent Software

It is assumed that the Palo Alto Networks User-ID Agent software is already installed on the Windows host discussed in the previous sections. It is a basic windows installer so no additional coverage of the install process will be included here.

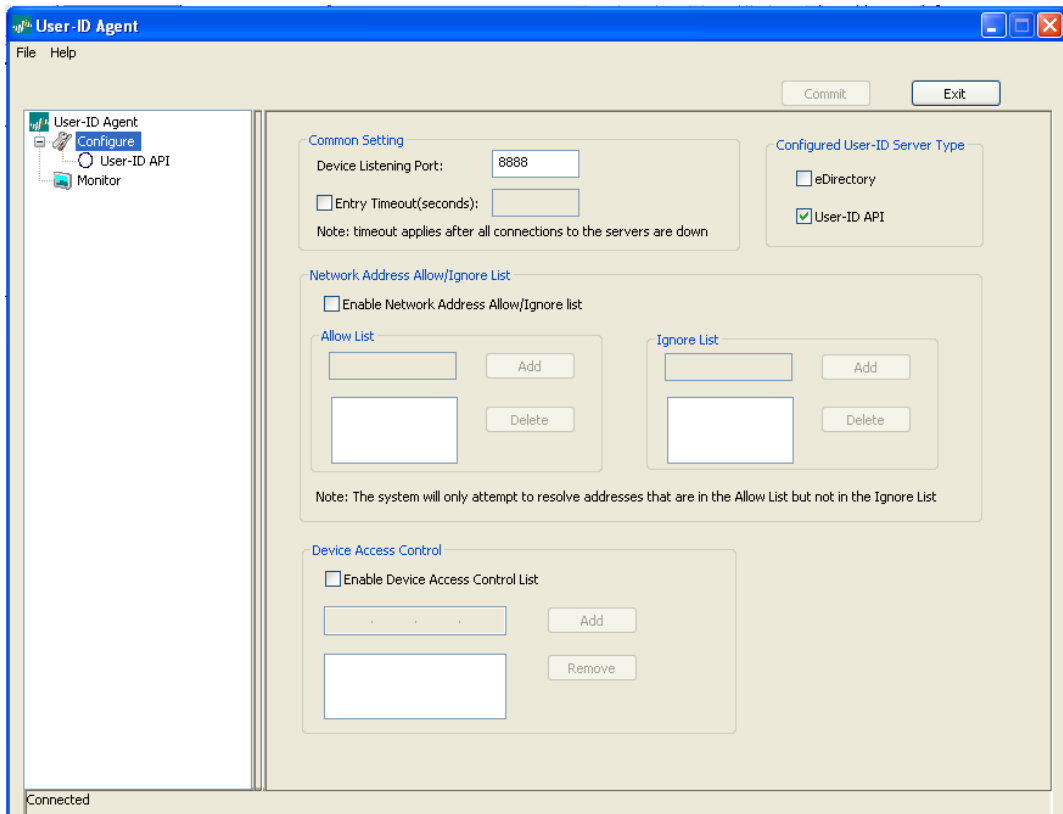
Once installed, you can launch the Agent software from the **Start > Program Files > Palo Alto Networks > User-ID Agent** menu option.

The following start up screen will be displayed:



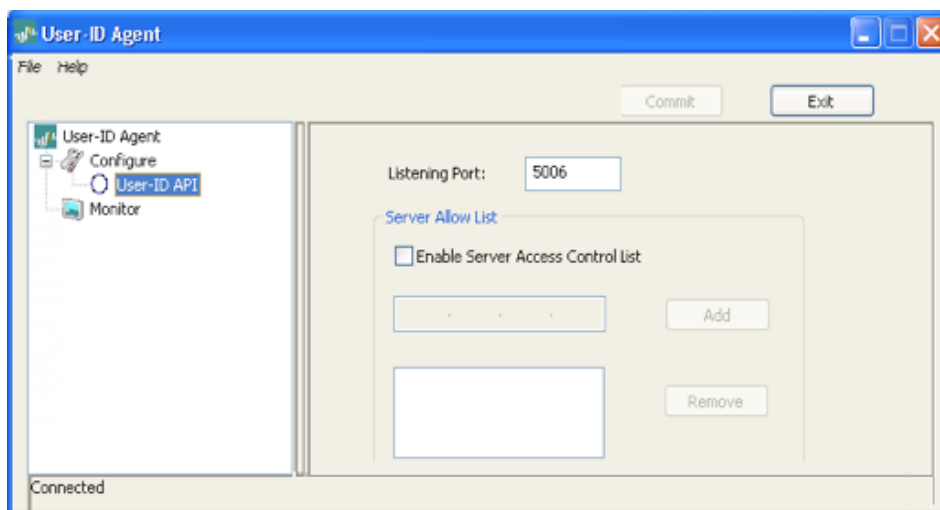
Click the **Configure** option in the left navigation pane to complete the configuration of the Agent software.

From the **Configure** screen the **Device Listening Port** must be configured to match that of the setting on the Palo Alto Networks firewall in the previous section. In our example the port selected was 8888.



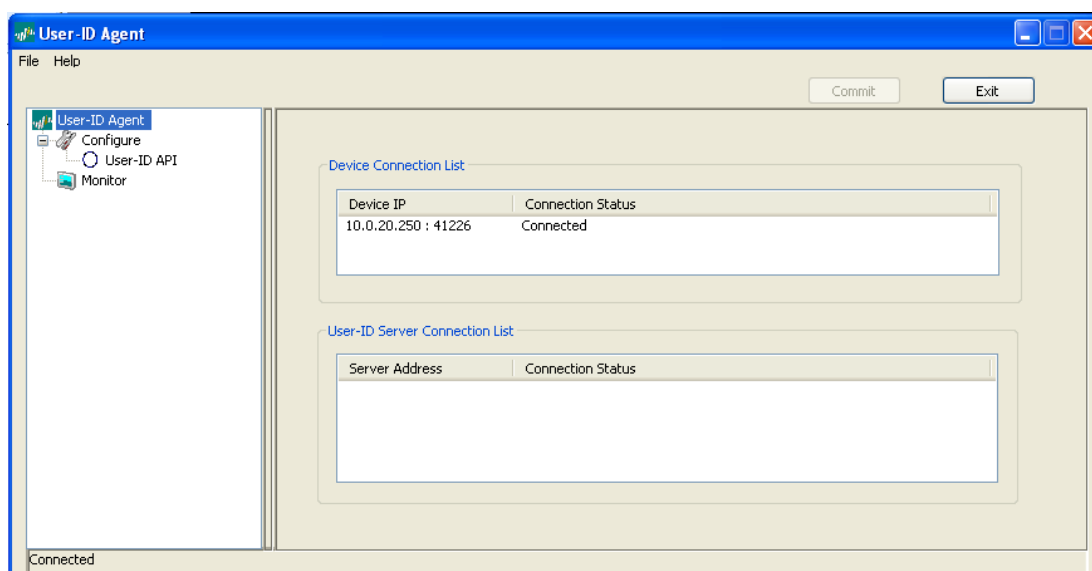
Additionally ensure that the **User-ID API** option has been checked. You will then see the option below **Configure** that allows further configuration of the **User-ID API** settings.

From the User-ID API configuration screen, leave the default listening port as **5006** as this is what the Amigopod default setting is in the Palo Alto Networks User-ID Services plugin.



Now returning to main screen by clicking on the User-ID Agent option at the top of the left navigation pane a successful connection from the Palo Alto Networks firewall should be displayed as shown below.

If the connection from the Palo Alto Networks firewall is not displayed in the **Device Connection List** as shown below you should investigate general connectivity between the Palo Alto Networks firewall and the Windows host along with any host based firewall on Windows that might be blocking the inbound connections.



At this point, all of the configuration steps are complete and your deployment is now ready for testing.

5 Verify Integration

Create Test Account in Amigopod

In order to test the integration between Amigopod and Palo Alto Networks we need to get a valid RADIUS authenticated session initiated on the Aruba wireless network.

From the Amigopod **Guest Manager > Create Guest** menu option, enter the details for a new test account and click the **Create Guest** button to save the account to the Amigopod database.

The screenshot displays the Amigopod Guest Manager interface. At the top, a table lists account details:

Username	Role	Status	Expiration
carlos@amigopod.com	aruba-guest	Enabled	2010-02-13 00:31

Below the table are several action buttons: [Reset password](#), [Change expiration](#), [Remove](#), [Edit](#), [Sessions](#), and [Print](#). A message states: "The guest account was successfully updated."

The **Account Details** section contains the following information:

- Guest username: carlos@amigopod.com
- Guest password: paloalto
- Account status: Enabled
- Account expiration: Account will expire at Saturday, 13 February 2010, 12:31 AM
- Sponsor name: admin

At the bottom, there are options to "Open print window using template...", "Send SMS receipt", and "Send email receipt to carlos@amigopod.com".

Login to Guest Wireless Network

Verify Wireless Connection and IP Addressing

The next step is to successfully connect to the Aruba wireless network and receive a valid IP address from the configured DHCP server. As can be seen from the screen shot below from the Aruba User Interface, the test wireless client (**10.0.20.60**) has successfully associated with the Amigopod SSID and is yet to authenticate via the Amigopod captive portal interface.

The screenshot shows the Aruba Controller Clients interface. The **Search** section includes filters for **Authenticated** (set to All), **User Name**, **Role**, **AP Name**, **BSSID**, **MAC Address**, **IP Address**, **Authentication Method**, and **ESSID**. The **Search Results** section displays a table of clients:

Client	User Name	MAC address	Client IP	User Role	Authentication Method	ESSID	AP Name	Phy Type	Age	Roaming
<input type="radio"/>		00:04:23:92:b4:e8	192.168.217.1	Guest-Logon-Role		amigopod	00:0b:86:cc:4a:36	802.11b	1 mins	Wireless
<input type="radio"/>		00:04:23:92:b4:e8	192.168.229.1	Guest-Logon-Role		amigopod	00:0b:86:cc:4a:36	802.11b	1 mins	Wireless
<input type="radio"/>		00:04:23:92:b4:e8	10.0.20.60	Guest-Logon-Role		amigopod	00:0b:86:cc:4a:36	802.11b	1 hrs 19 mins	Wireless

At the bottom, there are navigation buttons: [Status](#), [Profile](#), [Client Activity](#), [Packet Capture](#), [Locate](#), [Debug](#), [Disconnect](#), [Blacklist](#), [Ping](#), and [802.11K Report](#).

Login via Captive Portal page

Assuming your Wired or Wireless Access controller is setup correctly when a web browser is opened on the test wireless laptop the browsing session should be automatically redirect to the Amigopod Web Login page.

Login using the test account created in the previous step. Once you have been successfully authenticated you will be either redirected to a configured landing page or onto your original destination.

Verify Successful RADIUS Authentication

You can now verify the successful RADIUS authentication from the Amigopod interface by going to the **RADIUS Services > Server Control** option and reviewing the RADIUS log for an entry matching your test user.

RADIUS Server Time

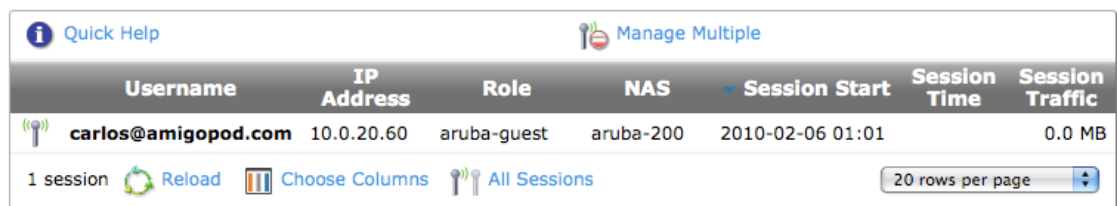
The RADIUS server time is currently: **Sat Feb 6 01:04:10 2010 +1100**

RADIUS Log Snapshot

The most recent entries in the RADIUS server log file are shown below.

```
Sat Feb 6 01:01:19 2010 : Auth: Login OK: [carlos@amigopod.com] (from client aruba-200 port 0 cli 00042392B4E8)
```

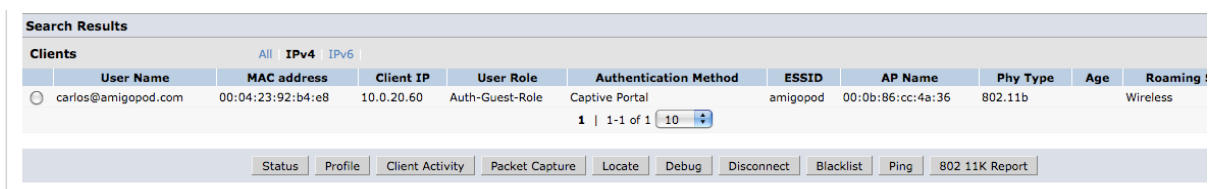
You can also go to the **Guest Manager > Active Sessions** menu option and review the entry for your test user.



Username	IP Address	Role	NAS	Session Start	Session Time	Session Traffic
carlos@amigopod.com	10.0.20.60	aruba-guest	aruba-200	2010-02-06 01:01		0.0 MB

Verify Successful Wireless Authentication

From the Aruba controller you can also verify the user authentication and see that the test user is now known to the controller and the authentication method was Captive Portal.

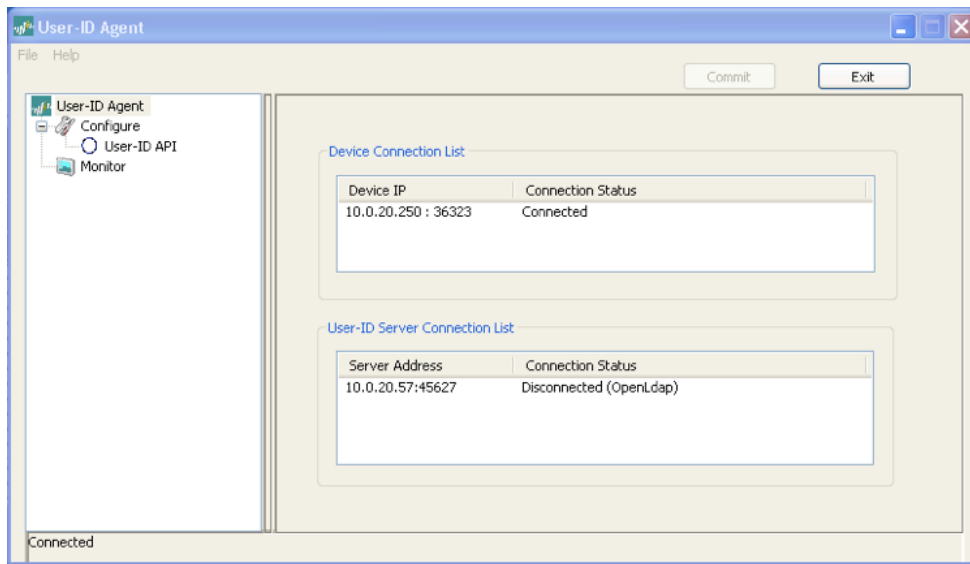


User Name	MAC address	Client IP	User Role	Authentication Method	ESSID	AP Name	Phy Type	Age	Roaming
carlos@amigopod.com	00:04:23:92:b4:e8	10.0.20.60	Auth-Guest-Role	Captive Portal	amigopod	00:0b:86:cc:4a:36	802.11b		Wireless

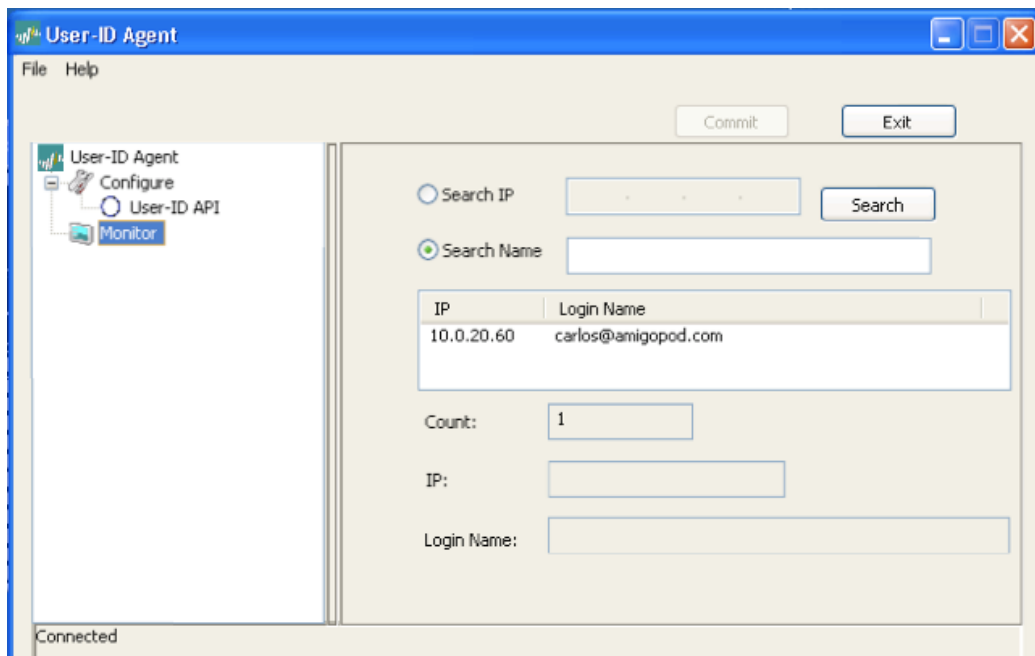
Monitor User-ID Agent

Based on this successful RADIUS authentication transaction, the Amigopod Palo Alto Networks User-ID plugin will have executed an XML API call to the User-ID Agent software to inform the Palo Alto Networks of the new IP Address to User mapping.

Returning to the main screen of the User-ID Agent we can see that the Amigopod has successfully sent an XML API update informing about the new IP Address to User identity mapping.



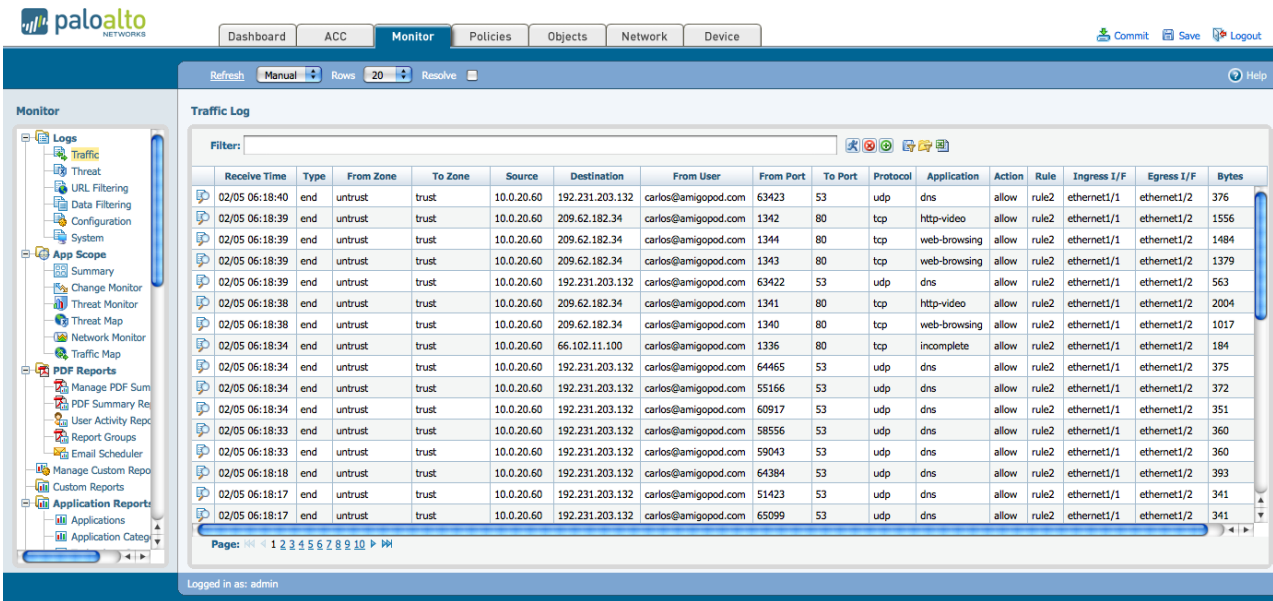
Additionally by clicking on the **Monitor** option in the left navigation pane we can verify the test user details have been successfully received.



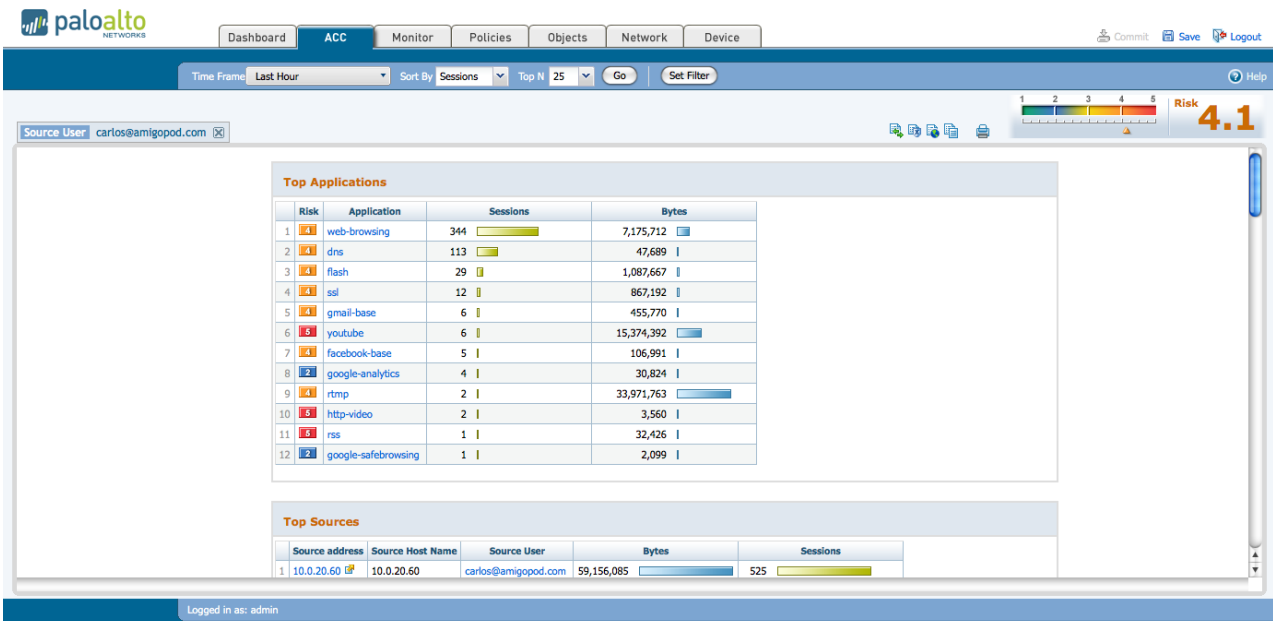
Verify User Identity Availability

The final test is to verify that the IP Address to User identity mapping has been successfully committed to the Palo Alto Networks firewall from the User-ID Agent.

From the Palo Alto Networks user interface select the **Monitor** tab to display the most recent traffic analysis. You should now see the **From User** column successfully populated with the user identity of the test user created in Amigopod.

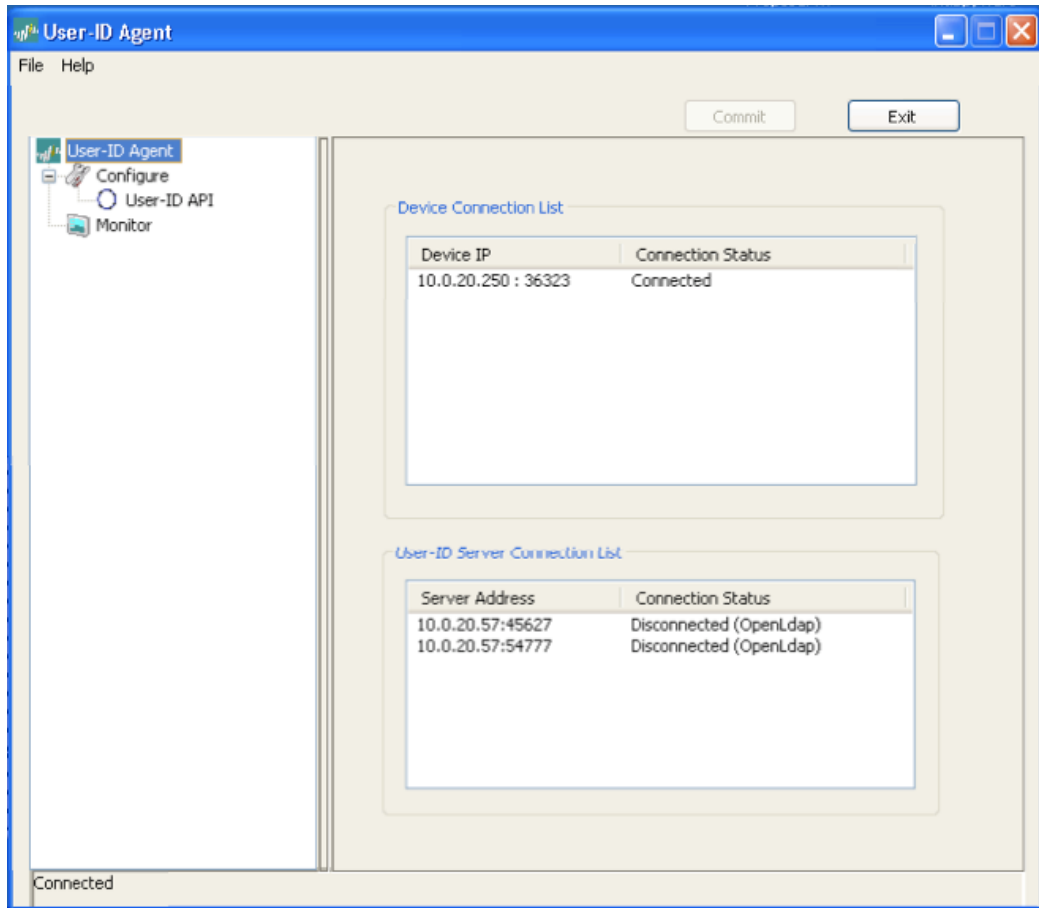


One of the most powerful sections of the Palo Alto Networks user interface is the **Application Command Centre (ACC)** where an intuitive drill down interface can be used to navigate the various traffic flows through the firewall, filtering on any criteria of interest. For example, the following screen shot is using a filter based on the user identity passed to the Palo Alto Networks firewall via the Amigopod API integration.



Logout and Verify User Mapping Removed

Use the Access Controller's logout procedure to successfully terminate the Guest Access session and hence initiate a RADIUS stop record being sent from the Access Controller to the Amigopod. This will trigger another API update from the Amigopod to the User-ID Agent running on the Windows host.



Returning to the **Monitor** tab on the Palo Alto Networks user interface you can now see that all subsequent traffic from the IP address in question (10.0.20.60) is no longer associated with a particular user.

Traffic Log

Filter:

	Receive Time	Type	From Zone	To Zone	Source	Destination	From User	From Port	To Port	Protocol	Application	Action	Rule	Ingress I/F	Egress I/F	Bytes
	02/05 06:38:56	end	untrust	trust	10.0.20.60	10.0.20.1		0	0	icmp	ping	allow	rule2	ethernet1/1	ethernet1/2	888
	02/05 06:38:50	end	untrust	trust	10.0.20.60	10.0.20.1		0	0	icmp	ping	allow	rule2	ethernet1/1	ethernet1/2	888
	02/05 06:38:47	end	untrust	trust	10.0.20.45	10.0.20.57		1889	80	tcp	web-browsing	allow	rule2	ethernet1/1	ethernet1/2	16653
	02/05 06:38:44	end	untrust	trust	10.0.20.60	10.0.20.1		0	0	icmp	ping	allow	rule2	ethernet1/1	ethernet1/2	592
	02/05 06:38:05	end	untrust	trust	10.0.20.60	119.31.248.68	carlos@amigopod.com	1869	80	tcp	web-browsing	allow	rule2	ethernet1/1	ethernet1/2	1918
	02/05 06:37:53	end	untrust	trust	10.0.20.60	192.231.203.3	carlos@amigopod.com	55537	53	udp	dns	allow	rule2	ethernet1/1	ethernet1/2	267

6 Summary

The necessity for application and user level visibility is today compounded by the explosion in requests for on demand Internet access. Whether its corporate guest access, a coffee shop hotspot or free wireless at a sporting event, users want to connect as easily and quickly as possible from a range of devices. This introduces a series of security challenges for IT administrators who ultimately are responsible for ensuring not only the ongoing security of the users and then network, but also for being able to provide historical forensic information about application usage.

By deploying Amigopod and Palo Alto Networks technology, customers have the benefit of an integrated solution to both the operational and security requirements of providing network access to non Active Directory users. In the corporate environment, nontechnical operators can easily provision temporary guest accounts through Amigopod, and IT administrators have full application level visibility of individual guest traffic through the Palo Alto Networks GUI. In public access deployments where visitors often self-register themselves, the User-ID integration will provide an unprecedented level of visibility and control for network operators.

In addition to the User-ID integration, Amigopod also now provides support for the new Palo Alto Networks Vendor Specific Radius dictionary. This enables additional support for authenticating SSL VPN users created on Amigopod and using radius return attributes to apply the appropriate policy. Similarly, this technique can be used for role based administration access for firewall administrators.