

# Network Sentry

## Palo Alto User Agent Integration

Version: 5.3

Date: 10/16/2012



---

## Copyright Notice

---

Copyright © 2012 by Bradford Networks, Inc. All rights reserved worldwide. Use, duplication, or disclosure by the United States government is subject to the restrictions set forth in DFARS 252.227-7013(c)(1)(ii) and FAR 52.227-19.

### Liability Disclaimer

Bradford Networks, Inc. reserves the right to make changes in specifications and other information contained in this document without prior notice. In all cases, the reader should contact Bradford Networks to inquire if any changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL BRADFORD NETWORKS, ITS EMPLOYEES, OFFICERS, DIRECTORS, AGENTS, OR AFFILIATES BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF BRADFORD HAS BEEN ADVISED OF, HAS KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

### Trademark, Service Mark, and Logo Information

Bradford Networks, the Bradford Networks logo, and Bradford Network Sentry are copyrighted by Bradford Networks, Inc. All other trademarks and registered trademarks are the property of their respective owners.

### Contact Information

Bradford Networks, Inc., 162 Pembroke Road, Concord, NH 03301 USA

Phone: 603.228.5300

Fax: 603.228.6420

Web site: <http://www.bradfordnetworks.com>

Information: [cm\\_questions@bradfordnetworks.com](mailto:cm_questions@bradfordnetworks.com)

Sales: [sales@bradfordnetworks.com](mailto:sales@bradfordnetworks.com)

Support: [support@bradfordnetworks.com](mailto:support@bradfordnetworks.com)

### ***Document Notes***

This document is an excerpt from the Administration And Operation document. Links with page numbers indicate that additional information is provided in this document. For example, see [Modify Groups on page 10](#). Links with no page numbers indicate that additional information can be found in the main Administration And Operation document. For example, see [Modify Groups](#).

# Palo Alto Integration

When the Palo Alto User Agent is configured in Network Sentry as a pingable device, Network Sentry sends a message to Palo Alto each time a host connects to the network or the host IP address changes, such as when a host is moved from the Registration VLAN to a Production VLAN. The message includes User ID and IP Address. This information identifies the user to Palo Alto allowing it to apply user specific policies.

## Implementation

To integrate with the Palo Alto User Agent you should be aware of and configure the following items:

### Palo Alto

- Palo Alto Networks User-ID Agent must be Version 4.0 or higher.
- The XML API must be enabled to allow communication with Network Sentry. Under User Identification > Setup make sure **Enable User-ID XML API** is set to **Yes**. This option is configured on the Agent Setup dialog under the Agent Service tab.

### Network Sentry

- Hosts that will be affected by or managed by the Palo Alto User Agent must be registered to a User. If no user is associated with the host, only the IP Address is sent to the Palo Alto User Agent and it cannot apply a policy without a User ID. Make sure that registration methods such as, the Persistent Agent, Device Profiler, or login scripts are not set to register hosts as devices.
- Add the Palo Alto User Agent as a pingable device in Network Sentry. See the instructions below for the steps.
- Network Sentry and the Palo Alto User Agent communicate via SSL. SSL certificates on the Palo Alto User Agent Server are automatically imported into the .keystore file on your Network Sentry Control Server or Server.
- In Event Management, the event **Communication Lost With Palo Alto User Agent** is automatically enabled. This event is generated when the Palo Alto User Agent cannot be reached. The Palo Alto User Agent is not being notified when hosts connect to the network, therefore, policies may not be applied. See [Enable And Disable Events](#) to disable the event if necessary.
- In Alarm Mapping, you can map the **Communication Lost With Palo Alto User Agent** event to an alarm if you wish to be notified when Network Sentry and the Palo Alto User Agent are no longer communicating. See [Add or Modify Alarm Mapping](#).

Device Name:	<input type="text" value="Palo Alto Agent Server"/>
IP Address:	<input type="text" value="192.168.6.160"/>
Physical Address	<input type="text" value="00:30:48:68:73:BA"/>
Domain:	Pingables
Device Type:	<input type="text" value="Server"/>
Palo Alto User Agent	<input checked="" type="checkbox"/>
XML API Port	<input type="text" value="5006"/>
Domain Name	<input type="text" value="qatest.bradfordnetworks.c"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 1: Add Pingable - Palo Alto User Agent

### Add Pingable

1. Click **Go > Topology**.
2. Select the **Domain** icon.
3. Right-click the domain and select **Add Pingable Device**.
4. Use the table of field definitions below to enter the data for the Palo Alto User Agent.
5. Click **Apply** to save.

Table 1: Field Definitions - Palo Alto User Agent

Field	Definition
<b>Device Name</b>	User specified name for the Palo Alto User Agent.
<b>IP Address</b>	IP address of the agent.
<b>Physical Address</b>	MAC address of the agent.
<b>Domain</b>	Network Sentry domain that will contain this device.
<b>Device Type</b>	List of types of devices that can be added as pingable devices in Network Sentry. For this configuration select Server.
<b>XML API Port</b>	Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent.
<b>Domain Name</b>	Fully Qualified Domain Name for your network users' domain.