



Monitoring Palo Alto

Beta Version

Palo Alto PowerPack version 100

Table of Contents

Introduction	3
What is Palo Alto?	3
What Does the Palo Alto PowerPack Monitor?	4
Installing the Palo Alto PowerPack	4
Configuring and Discovering Palo Alto Firewalls	6
Prerequisites	6
Creating Credentials for Palo Alto	7
Creating an SNMP Credential	7
Creating a Basic/Snippet Credential	8
Discovering Palo Alto Devices	9

Chapter 1

Introduction

Overview

This manual describes how to monitor Palo Alto firewalls in the ScienceLogic platform using the *Palo Alto PowerPack*.

The following sections provide an overview of Palo Alto firewalls and the *Palo Alto PowerPack*:

- [What is Palo Alto? 3](#)
- [What Does the Palo Alto PowerPack Monitor? 4](#)
- [Installing the Palo Alto PowerPack 4](#)

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is Palo Alto?

Palo Alto Networks is a provider of enterprise network security solutions. Their products include physical and virtual firewalls, the WildFire cloud-based service, and the Panorama network security management platform.

What Does the Palo Alto PowerPack Monitor?

The *Palo Alto* PowerPack includes the following features:

- Dynamic Applications to collect configuration and performance data about Palo Alto firewalls
- Device Classes for each of the Palo Alto devices monitored
- Event Policies and corresponding alerts that are triggered when Palo Alto devices meet certain status criteria

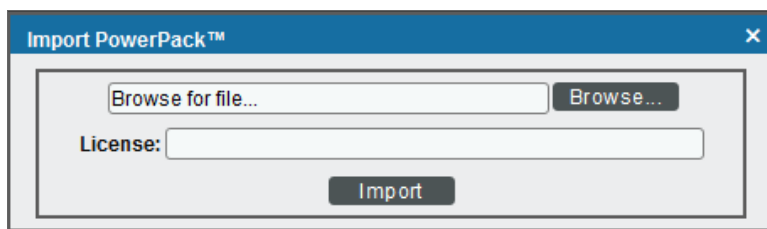
Installing the Palo Alto PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Palo Alto* PowerPack.

To download and install a PowerPack:

TIP: By default, installing a new version of a PowerPack overwrites all content in that PowerPack that has already been installed on the target system. You can use the **Enable Selective PowerPack Field Protection** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the **System Administration** manual.)

1. Download the PowerPack from the [ScienceLogic Customer Portal](#).
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Configuring and Discovering Palo Alto Firewalls

Overview

The following sections describe how to configure and discover Palo Alto firewalls for monitoring by the ScienceLogic platform using the *Palo Alto* PowerPack:

<i>Prerequisites</i>	6
<i>Creating Credentials for Palo Alto</i>	7
<i>Creating an SNMP Credential</i>	7
<i>Creating a Basic/Snippet Credential</i>	8
<i>Discovering Palo Alto Devices</i>	9

Prerequisites

Before you can monitor Palo Alto firewalls in the ScienceLogic platform using the *Palo Alto* PowerPack, you must have the following information:

- SNMP community strings for the devices you want to monitor
- IP addresses for each device you want to monitor
- Username and password for a user with access to the devices you want to monitor

NOTE: The monitored firewalls must be running PAN-OS version 8.0 or later to ensure the proper collection of tunnel performance data.

Creating Credentials for Palo Alto

To configure the ScienceLogic platform to monitor Palo Alto firewalls, you must create the SNMP and Basic/Snippet credentials that enable the platform to connect with those firewalls.

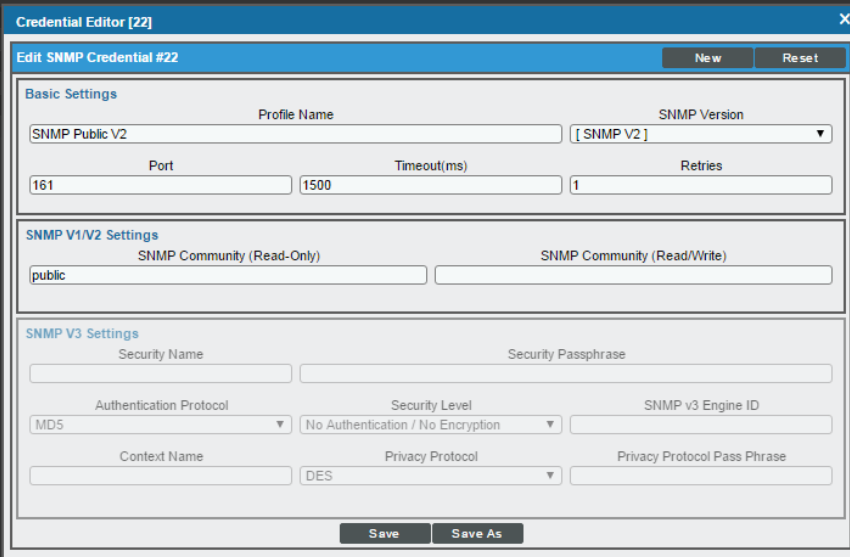
NOTE: The *Palo Alto* PowerPack currently supports only basic authentication for discovery; it does not support the use of an API key.

Creating an SNMP Credential

Some of the Dynamic Applications in the *Palo Alto* PowerPack use SNMP to collect information about Palo Alto firewalls. To use these Dynamic Applications, you must first define an SNMP credential that enables the ScienceLogic platform to communicate with the firewalls.

To configure an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and then select *Create SNMP Credential*. The **Credential Editor** page appears.
3. Complete the following fields:



The screenshot shows the 'Credential Editor [22]' window. At the top, it says 'Edit SNMP Credential #22' with 'New' and 'Reset' buttons. The form is divided into three sections: 'Basic Settings', 'SNMP V1/V2 Settings', and 'SNMP V3 Settings'. In 'Basic Settings', 'Profile Name' is 'SNMP Public V2', 'SNMP Version' is '[SNMP V2]', 'Port' is '161', 'Timeout(ms)' is '1500', and 'Retries' is '1'. In 'SNMP V1/V2 Settings', 'SNMP Community (Read-Only)' is 'public' and 'SNMP Community (Read/Write)' is empty. In 'SNMP V3 Settings', 'Security Name' and 'Security Passphrase' are empty, 'Authentication Protocol' is 'MD5', 'Security Level' is 'No Authentication / No Encryption', 'SNMP v3 Engine ID' is empty, 'Context Name' is empty, 'Privacy Protocol' is 'DES', and 'Privacy Protocol Pass Phrase' is empty. At the bottom are 'Save' and 'Save As' buttons.

- **Profile Name.** Type a name for the credential.
- **SNMP Version.** Select *SNMP V2*.
- **SNMP Community (Read Only).** Type the community string for the Palo Alto firewalls you want to monitor.

- Supply values in the other fields on this page as needed. In most cases, you can accept the default values for the other fields.
- Click the **[Save]** button.

Creating a Basic/Snippet Credential

To configure the ScienceLogic platform to monitor Palo Alto devices, you must also create a Basic/Snippet credential. This credential enables some of the Dynamic Applications in the *Palo Alto PowerPack* to connect with those devices.

To create a Basic/Snippet credential for Palo Alto devices:

- Go to the **Credential Management** page (System > Manage > Credentials).
- Click the **[Actions]** button and then select *Create Basic/Snippet Credential*. The **Credential Editor** page appears.
- Complete the following fields:

- **Credential Name.** Type a name for the credential.
 - **Hostname/IP.** Type "https://%D".
 - **Port.** Type "443".
 - **Timeout.** Type "30000".
 - **Username.** Type the username for a user account with access to the Palo Alto firewalls.
 - **Password.** Type the password for the Palo Alto user account.
- Click the **[Save As]** button.
 - When the confirmation message appears, click **[OK]**.

Discovering Palo Alto Devices

After you have created the necessary credentials, you can discover the Palo Alto devices that you want to monitor. Several minutes after the discovery session has completed, the Dynamic Applications in the Palo Alto PowerPack will automatically align to the devices, enabling you to view configuration and performance data about the devices.

To discover the Palo Alto devices that you want to monitor:



1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button.
3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, complete the following fields:

The screenshot shows the 'Discovery Session Editor | Editing Session [16]' interface. It is divided into several sections:

- Identification Information:** Name 'PaloAlto', Description field.
- IP and Credentials:** IP Address/Hostname Discovery List with '10.64.162.28'. Includes 'Upload File' and 'Browse for file...' buttons.
- SNMP Credentials:** A list of credentials with '[PaloAlto_SNMP]' selected.
- Other Credentials:** A list of other credentials with '[PaloAlto]' selected.
- Detection and Scanning:** Initial Scan Level, Scan Throttle, Port Scan All IPs, and Port Scan Timeout, all set to '[System Default (recommended)]'. Includes a 'Detection Method & Port' list with 'UDP: 161 SNMP' selected, and 'Interface Inventory Timeout (ms)' set to '600000' and 'Maximum Allowed Interfaces' set to '10000'. There is a 'Bypass Interface Inventory' checkbox.
- Basic Settings:** 'Discover Non-SNMP' is unchecked, 'Model Devices' is checked, and 'DHCP' is unchecked. 'Device Model Cache TTL (h)' is set to '2'. 'Collection Server PID' is '1'. 'Organization' is '[System]'. 'Add Devices to Device Group(s)' is empty. 'Apply Device Template' is '[Choose a Template]'.

At the bottom, there are 'Save' and 'Save As' buttons, and a 'Log All' checkbox.

- **IP Address/Hostname Discovery List.** Type the IP address or addresses for the Palo Alto devices that you want to discover.
 - **SNMP Credentials.** Select the SNMP credential you created for the Palo Alto devices.
 - **Other Credentials.** Select the Basic/Snippet credentials you created for the Palo Alto devices.
 - **Model Devices.** Select this checkbox.
4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the **Discovery & Credentials** manual.

5. Click the **[Save]** button to save the discovery session, and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon () to run the discovery session.
7. The **Discovery Session** window appears. When the device(s) are discovered, click the device icon () to view the **Device Properties** page for each device.

© 2003 - 2017, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010