Monitoring Palo Alto

Palo Alto Base Pack PowerPack version 101

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Palo Alto firewalls in SL1 using the *Palo Alto Base Pack* PowerPack.

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

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 Base Pack PowerPack Monitor?

The *Palo Alto Base Pack* 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

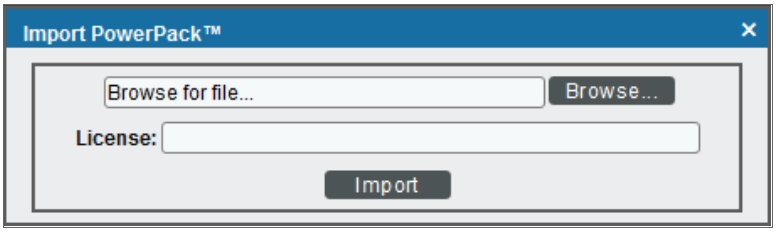
Installing the Palo Alto Base Pack PowerPack

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

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of 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.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
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 appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal 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. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Discovery

Configuration and Discovery

The following sections describe how to configure and discover Palo Alto firewalls for monitoring by SL1 using the *Palo Alto Base Pack* PowerPack:

Prerequisites for Monitoring Palo Alto Firewalls

Before you can monitor Palo Alto firewalls in SL1 using the *Palo Alto Base Pack* 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 SL1 to monitor Palo Alto firewalls, you must create the SNMP and Basic/Snippet credentials that enable SL1 to connect with those firewalls.

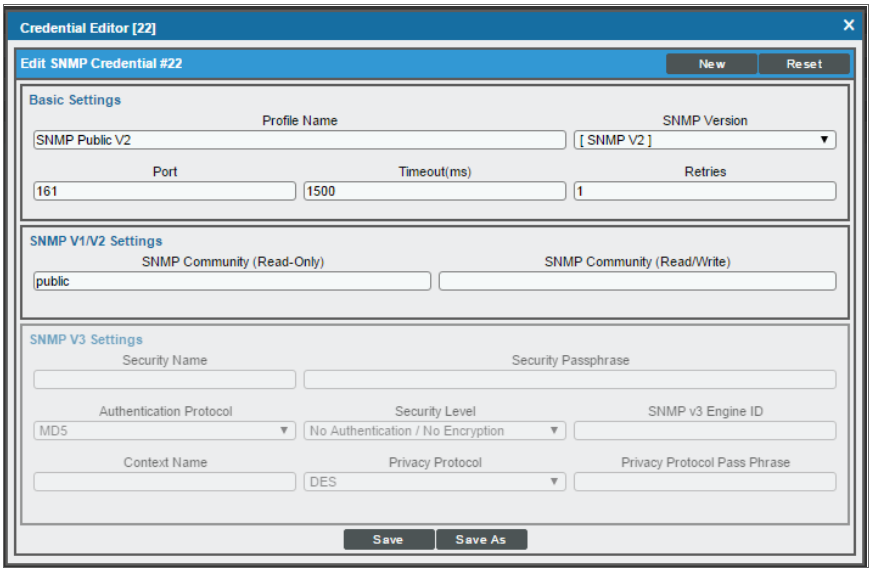
NOTE: The *Palo Alto Base Pack* PowerPack currently supports only basic authentication for discovery; it does not support the use of an API key.

Creating an SNMP Credential

Some of the Dynamic Applications in the *Palo Alto Base Pack* PowerPack use SNMP to collect information about Palo Alto firewalls. To use these Dynamic Applications, you must first define an SNMP credential that enables SL1 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:



- ***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.

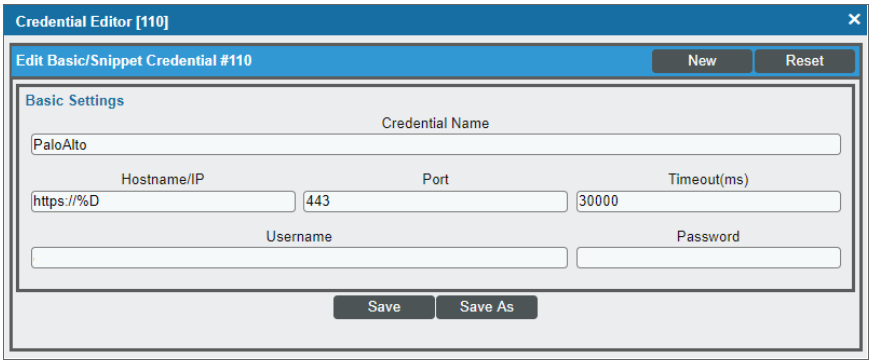
4. Supply values in the other fields on this page as needed. In most cases, you can accept the default values for the other fields.
5. Click the **[Save]** button.

Creating a Basic/Snippet Credential

To configure SL1 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 Base Pack* PowerPack to connect with those devices.

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

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** button and then select *Create Basic/Snippet Credential*. The **Credential Editor** page appears.
3. 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.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

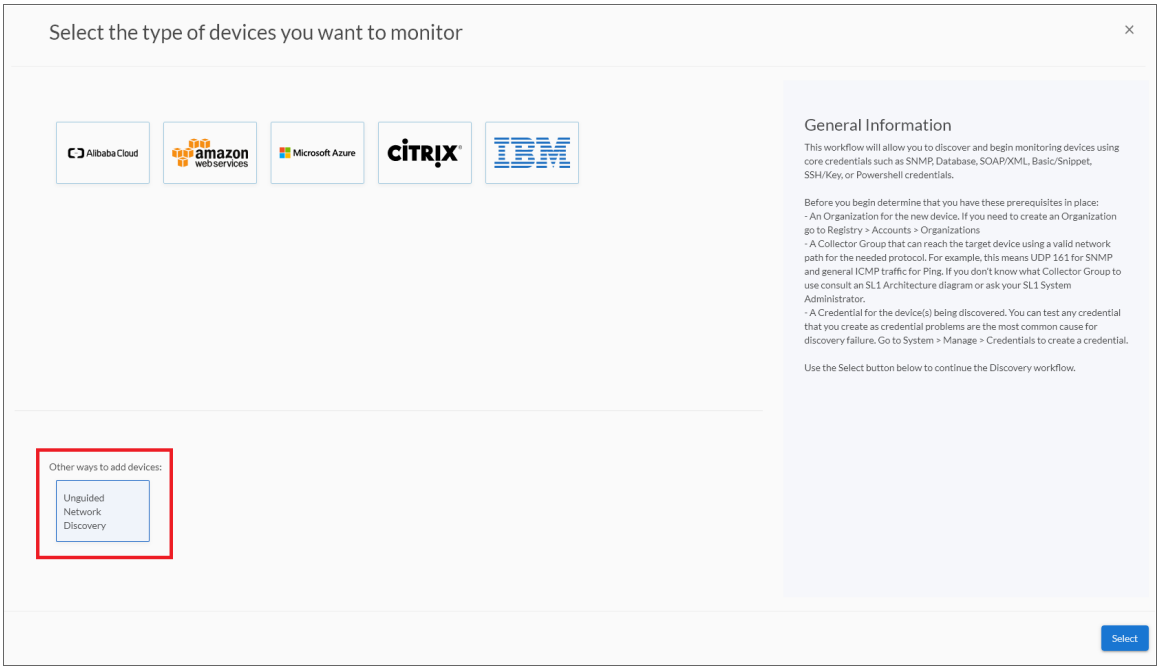
Discovering Palo Alto Devices

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 Base Pack* PowerPack will automatically align to the devices, enabling you to view configuration and performance data about the devices.

NOTE: This PowerPack discovers virtual Palo Alto devices that respond to SNMP. However, if they are provisioned, SL1 will not model them. SL1 will model the devices if they exist when the next discovery session is run.

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

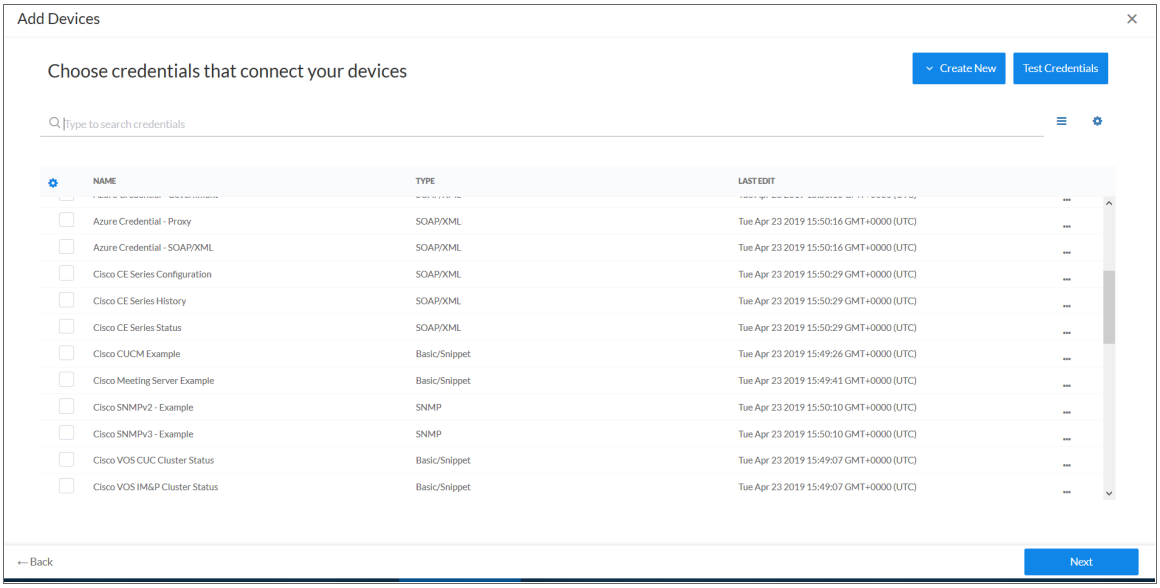
1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



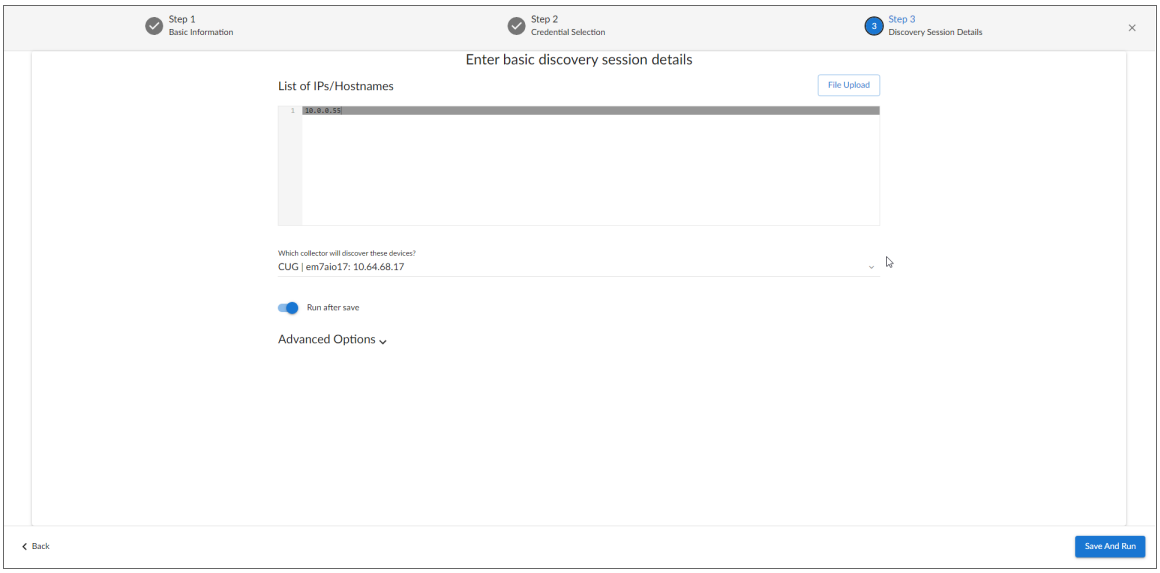
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:

    - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
    - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears:



6. On the **Credentials** page, locate and select the *SNMP credential* and the *Basic/Snippet credential* you created.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



8. Complete the following fields:

   - ***List of IPs/Hostnames***. Type the IP address for the Palo Alto device.
   - ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
   - ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.

     In the **Advanced options** section, click the down arrow icon ( ) to complete the following fields:

     - ***Model Devices***. Enable this setting.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

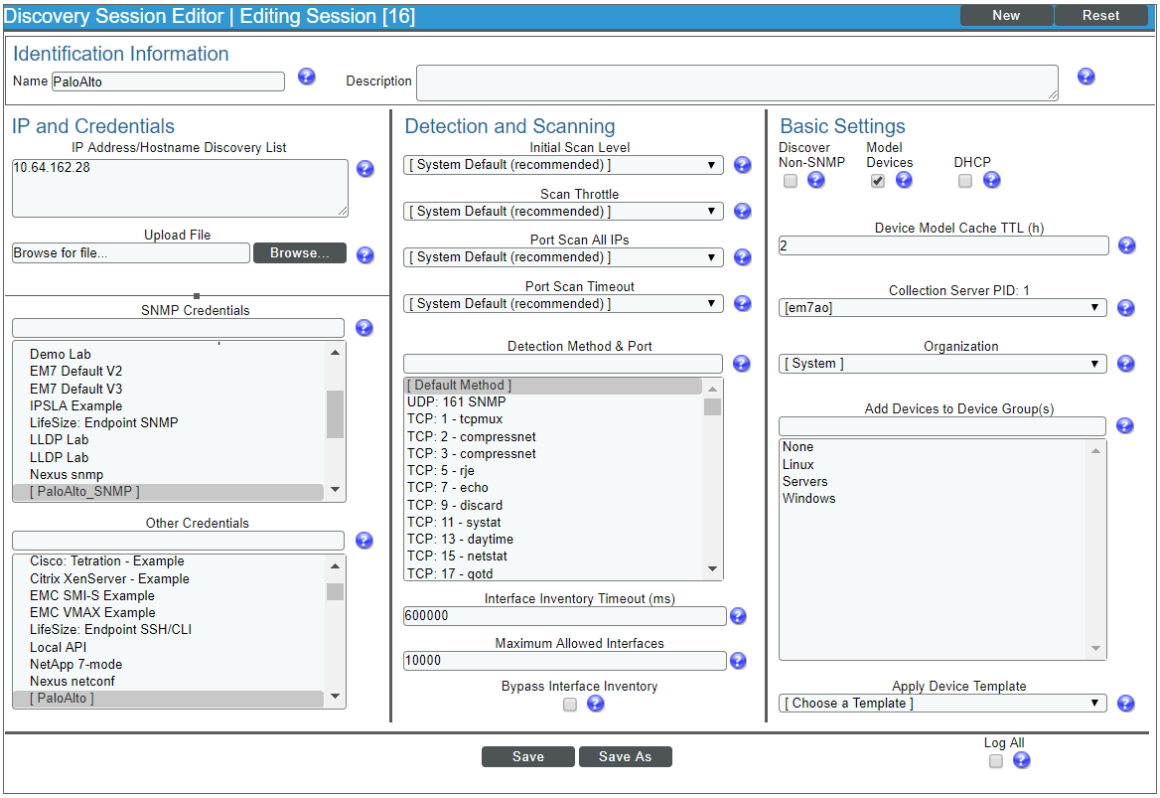
Discovering Palo Alto Devices in the SL1 Classic User Interface

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 Base Pack* PowerPack will automatically align to the devices, enabling you to view configuration and performance data about the devices.

NOTE: This PowerPack discovers virtual Palo Alto devices that respond to SNMP. However, if they are provisioned, SL1 will not model them. SL1 will model the devices if they exist when the next discovery session is run.

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

1. Go to the **Discovery Control Panel** page (System > Manage > Classic 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:



- ***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.

Chapter 3

Troubleshooting

Overview

The following sections describe resolutions to some issues you might encounter when monitoring Palo Alto firewalls:

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.

Troubleshooting Palo Alto API Requests

If you are experiencing an issue in SL1, you can verify whether it is an issue with SL1 or Palo Alto's API.

ScienceLogic suggests using an API tool, like Postman or cURL, to try to reproduce the issue in your Palo Alto system. When running the API testing tool, if you receive a message that the tool is not able to send a request or if the tool does not receive a response from the API, an issue is occurring in your Palo Alto system. For the examples below, ScienceLogic uses Postman.

Common Palo Alto API Issues and Resolutions

- If the API testing tool cannot send a request, you might be experiencing network connectivity issues. Check your connection by attempting to open a page in your web browser.
- Some firewalls might be configured to block non-browser connections. If this is the case, you will need to contact your Palo Alto administrator before running the API testing tool.
- Your API server might require client certificates. You can try adding a client certificate in the API testing tool settings.
- If you are including variables or path parameters with your API request, check that the final address is structured correctly. Unresolved request variables can result in an invalid server address.
- Check that the URL is correct and uses http:// or https://.
- For a full list of Palo Alto API code errors, see Palo Alto's documentation on PAN-OS XML API Error Codes.

Troubleshooting Commands

If your Dynamic Applications are failing, you can use SSH to access each Data Collector and then run the following commands. These commands verify the API endpoints that are used by the Dynamic Applications in the Palo Alto Base Pack PowerPack. If the command fails, you have identified which Dynamic Application is failing.

- To test the Discovery Snippet Code that is used for Dynamic Applications that use the API, run the following command:

```
curl -u USERNAME:PASSWORD -k "https://DEVICE_
IP/api/?type=report&async=yes&reporttype=predefined&reportname=top-
application-categories"
```

- To test the "Palo Alto: Traffic to Country Destination" Dynamic Application, run the following command:

```
curl -u USERNAME:PASSWORD -k "https://DEVICE_
IP/api/?type=report&async=nos&reporttype=predefined&reportname=top-
destination-countries"
```

- To test the "Palo Alto: Environmental Performance" Dynamic Application, run the following command:

```
curl -u USERNAME:PASSWORD -k "https://DEVICE_IP
/api/?type=op&cmd=<show><system><environmentals></environmentals></system><
/show>"
```

- To test the "Palo Alto: License Configuration" Dynamic Application, run the following command:

```
curl -u USERNAME:PASSWORD -k "https://DEVICE_
IP/api/?type=op&cmd=<request><license><info></info></license></request>"
```

- To test the "Palo Alto: GlobalProtect Configuration" Dynamic Application, run the following command:

```
curl -u USERNAME:PASSWORD -k "https://DEVICE_
IP/api/?type=op&cmd=<show><system><info/></system></show>"
```

- To get the Palo Alto version, run the following command:

```
curl -u USERNAME:PASSWORD -k "https://DEVICE_IP/api/?type=version"
```

Troubleshooting Dynamic Applications

There are additional common issues when using the Dynamic Applications included in the Palo Alto Base Pack PowerPack. Use the following steps to identify and troubleshoot issues.

SNMP Devices and Dynamic Applications

If your Dynamic Applications are not collecting data from an SNMP device, review your SNMP device credential to ensure the Data Collector can communicate with your SNMP device. If your credential is correct, perform a SNMP request to verify that the object IDs (OIDs) that are used by the Dynamic Applications are available in the SNMP device.

To verify that the OIDs are available to a Dynamic Application, perform an SNMP walk:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. In the **Device Manager** page, select the wrench icon () for a device on which you want to perform an SNMP walk.
3. In the **Device Properties** page, select the **[Toolbox]** tab. Select the SNMP Walker icon in the **Device Toolbox** pane.
4. The **SNMP Walker** modal appears. In the drop-down menu in the upper left, select the OID for the Dynamic Application you would like to verify.
5. Click the **[Walk]** button.
6. Verify that the OID returns a response. If an OID does not return a response, there may be an issue with your device.

Automatically Aligned Dynamic Applications

If your Dynamic Application is not collecting data, it is possible that the Dynamic Application is not automatically aligned to a component. To manually verify that a Dynamic Application is aligned, you can perform an SNMP walk.

To identify the Discovery OID available on a Dynamic Application and perform an SNMP walk:

1. Go to the Dynamic Applications Manager page (System > Manage > Dynamic Applications, or System > Manage > Applications in the classic SL1 user interface).
2. Find the Dynamic Application that you would like to verify and select the wrench icon ().
3. In the **Dynamic Applications Properties Editor** page, select the **[Collections]** tab.
4. In the **Collection Object Registry** pane (at the bottom of the page), find the Object Name 'Discovery' and make note of the SNMP OID. You will need it to perform an SNMP walk.
5. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic SL1 user interface).

6. In the **Device Manager** page, select the wrench icon () for a device on which you want to perform an SNMP walk.
7. In the **Device Properties** page, select the **[Toolbox]** tab. Select the SNMP Walker icon in the **Device Toolbox** pane.
8. The **SNMP Walker** modal appears. Next to the drop-down menu in the upper left, select the plus icon to manually enter an OID.
9. Enter the SNMP OID value from the 'Discovery' Object Name. Click the **[Walk]** button.
10. Verify that the OID returns a response. If the OID does not return a response, the Dynamic Application may not be automatically aligned.

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