

# Tenable for Palo Alto Networks

## Introduction

This document describes how to deploy Tenable SecurityCenter® and Nessus® for integration with Palo Alto Networks next-generation firewalls (NGFW). Please email any comments and suggestions to [support@tenable.com](mailto:support@tenable.com).

Monitoring the security settings of your Palo Alto Networks firewalls is critical for maintaining your network's security posture. Unless your vulnerability management (VM) platform is equipped with configuration assessment checks specifically designed for Palo Alto firewalls, your network may be exposed to unnecessary risk.

Additionally, better VM platforms offer continuous listening through passive vulnerability monitoring to help bridge the vulnerability intelligence gap in between periodic active scans and audits. However, placing passive monitors on every network segment throughout a global enterprise can be impractical. Although more organizations are turning to SIEMs (security information and event management) to uncover hidden threats, most SIEMs take months to deploy and are costly to acquire and maintain.

Benefits of integrating Tenable SecurityCenter with Palo Alto Networks include:

- Maintain compliance with industry best practices for firewall hardening
- Achieve real-time, 100% asset discovery by detecting new hosts connected to network segments not monitored by Tenable Passive Vulnerability Scanner® (PVS™)
- Discover system vulnerabilities and security misconfigurations of mobile devices and virtual machines not present during the last periodic full-network scan
- Maintain compliance with government and industry regulations that mandate log aggregation, such as PCI, HIPAA, FISMA, and more
- Uncover advanced cyberthreats by correlating Palo Alto firewall log data against log data from other network and security devices

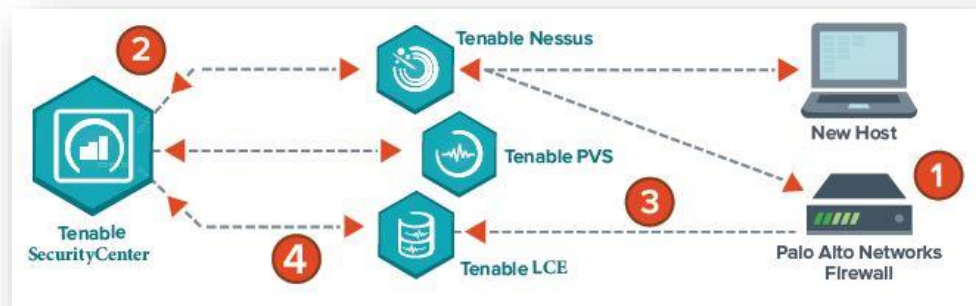
## Integration Overview

SecurityCenter and Nessus offer a series of plugins specifically designed to audit Palo Alto Networks physical and virtual NGFWs to identify security misconfigurations and ensure best-practice hardening guidelines are followed. To perform the audit, SecurityCenter (via Nessus) initiates a credentialed scan of the Palo Alto NGFW, authenticating credentials through the Palo Alto XML API. Once completed, detailed findings of the Palo Alto audit can be reviewed within SecurityCenter scan results, dashboards, and reports.

In addition to configuration audits, Tenable can also import real-time log data from Palo Alto NGFWs into its Log Correlation Engine® (LCE®) to help identify assets on networks not monitored by Tenable PVS. Once hosts are identified they can be

automatically assigned to dynamic asset lists and audited with Nessus to detect any possible vulnerabilities or misconfigurations.

Tenable LCE also allows the log data gathered from Palo Alto NGFWs to be accessed and correlated against other network and security data sources to help uncover hidden cyberthreats and maintain compliance with government and industry regulations.



Nessus Manager version 6.x, Tenable.io, and SecurityCenter and SecurityCenter Continuous View version 4.8 and higher support Palo Alto Networks integration. Nessus, Tenable.io, and SecurityCenter solutions work with Palo Alto Networks PAN-OS versions 4.x through 7.x.

## Integrating with Palo Alto Networks

### Palo Alto NGFW Configuration Audit

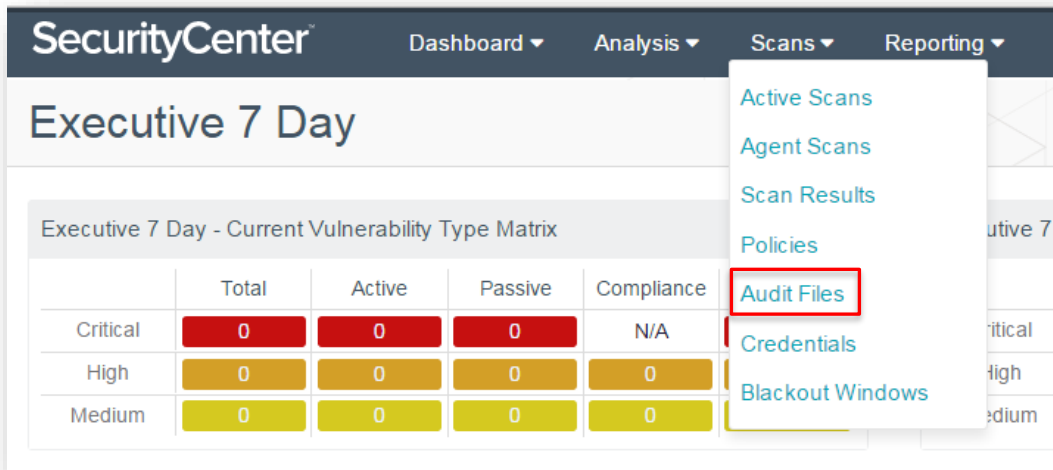
Integrating SecurityCenter and Palo Alto to perform audit checks requires configuration in both SecurityCenter and PAN-OS.

Within PAN-OS, the following configuration tasks are required:

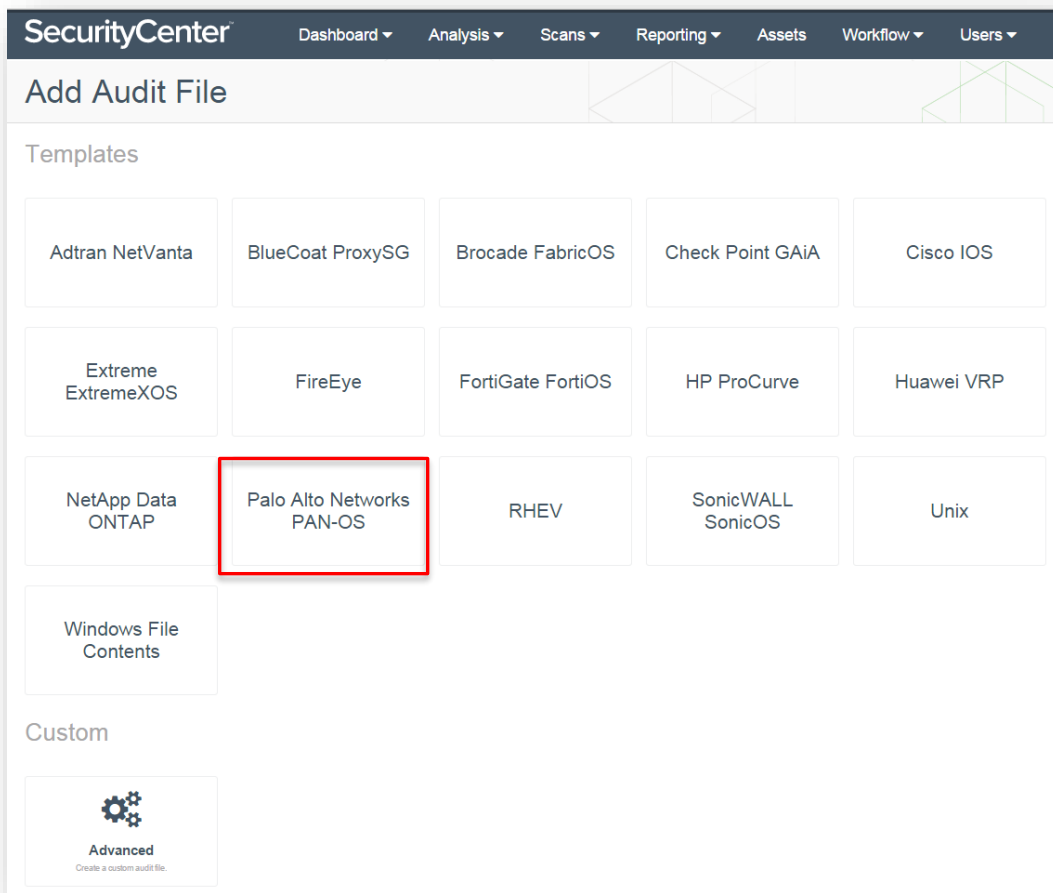
- Create a service account for SecurityCenter
- Grant SecurityCenter access to the PAN-OS management interface
- Configure SNMP to be allowed by local security policies

For detailed instruction on configuring PAN-OS for integration please refer to the [Palo Alto PAN-OS Administrator's Guide](#).

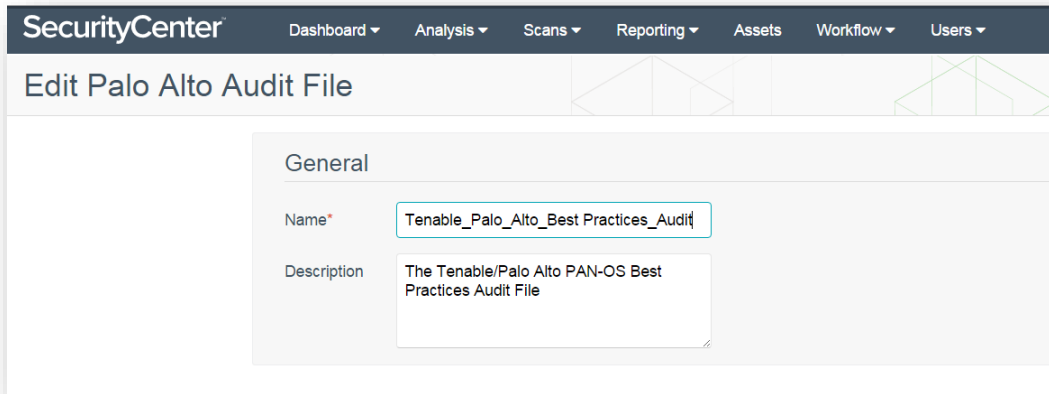
Once the configuration steps for PAN-OS are complete, log in to SecurityCenter, click “Scans”, and select “Audit Files”.



Click “+Add” and select “Palo Alto Networks PAN-OS” from the list of available audit file templates.



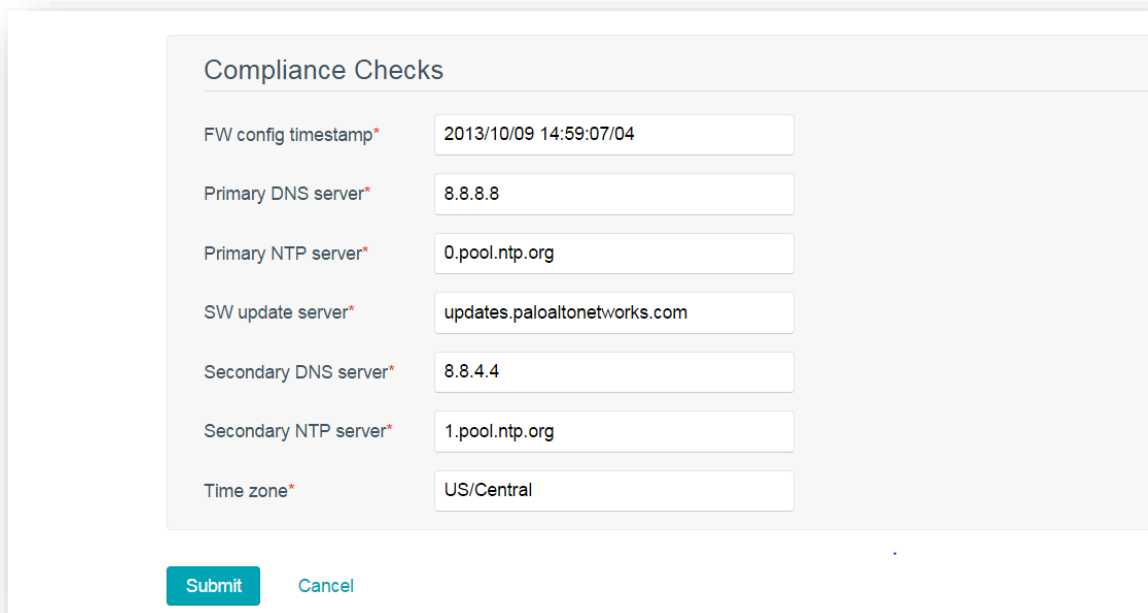
In the “General” section, enter a name for the audit file and a description (optional).



The screenshot shows the SecurityCenter interface with a navigation bar at the top containing 'Dashboard', 'Analysis', 'Scans', 'Reporting', 'Assets', 'Workflow', and 'Users'. The main heading is 'Edit Palo Alto Audit File'. Below this, the 'General' section is visible, containing two input fields: 'Name\*' with the value 'Tenable\_Palo\_Alto\_Best Practices\_Audit' and 'Description' with the value 'The Tenable/Palo Alto PAN-OS Best Practices Audit File'.

Configure each option within the “Compliance Checks” section. Each option will be pre-populated by default. The info contains default values set in the audit database. The information will need to be customized for each environment.

Once the “Compliance Checks” configuration is complete, click “Submit”.



The screenshot shows the 'Compliance Checks' section of the SecurityCenter interface. It contains several configuration fields, each with a pre-populated value:

Field	Value
FW config timestamp*	2013/10/09 14:59:07/04
Primary DNS server*	8.8.8.8
Primary NTP server*	0.pool.ntp.org
SW update server*	updates.paloaltonetworks.com
Secondary DNS server*	8.8.4.4
Secondary NTP server*	1.pool.ntp.org
Time zone*	US/Central

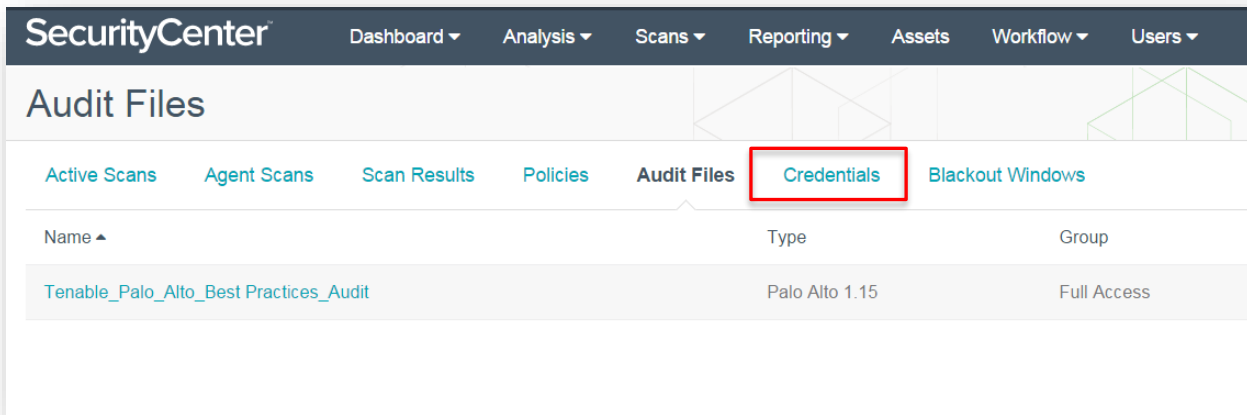
At the bottom of the section, there are two buttons: 'Submit' (highlighted in blue) and 'Cancel'.

The table below contains a description of each “Compliance Checks” option:

Table 1: Compliance Checks Options

Option	Description
FW config timestamp	Firewall configuration timestamp of the Palo Alto Networks device
Primary DNS server	Primary DNS server (Domain Name Server) of the Palo Alto Networks device
Primary NTP server	Primary NTP (Network Time Protocol) server of the Palo Alto Networks device
SW update server	The content update URL for Palo Alto Networks devices. The recommended setting is “updates.paloaltonetworks.com”.
Secondary DNS server	Secondary DNS server (Domain Name Server) of the Palo Alto Networks device
Secondary NTP server	Secondary NTP (Network Time Protocol) server of the Palo Alto Networks device
Time zone	Time zone of the Palo Alto Networks device

Click “Credentials” and click “+Add”.



In the “General” section, enter a name for the SNMP credentials and a description (optional). Under the “Credential” section, click the drop-down and select “SNMP”. In the “Community” box, enter the SNMP community string. Click “Submit”.

**SecurityCenter** Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾

## Edit Credential

**General**

Name\* PAN-OS\_SNMP\_Credentials

Description PAN-OS SNMP Credentials

**Credential**

Type SNMP

Community\* public

Submit Cancel

To create the scan policy, click “Policies” and then click “+Add”.

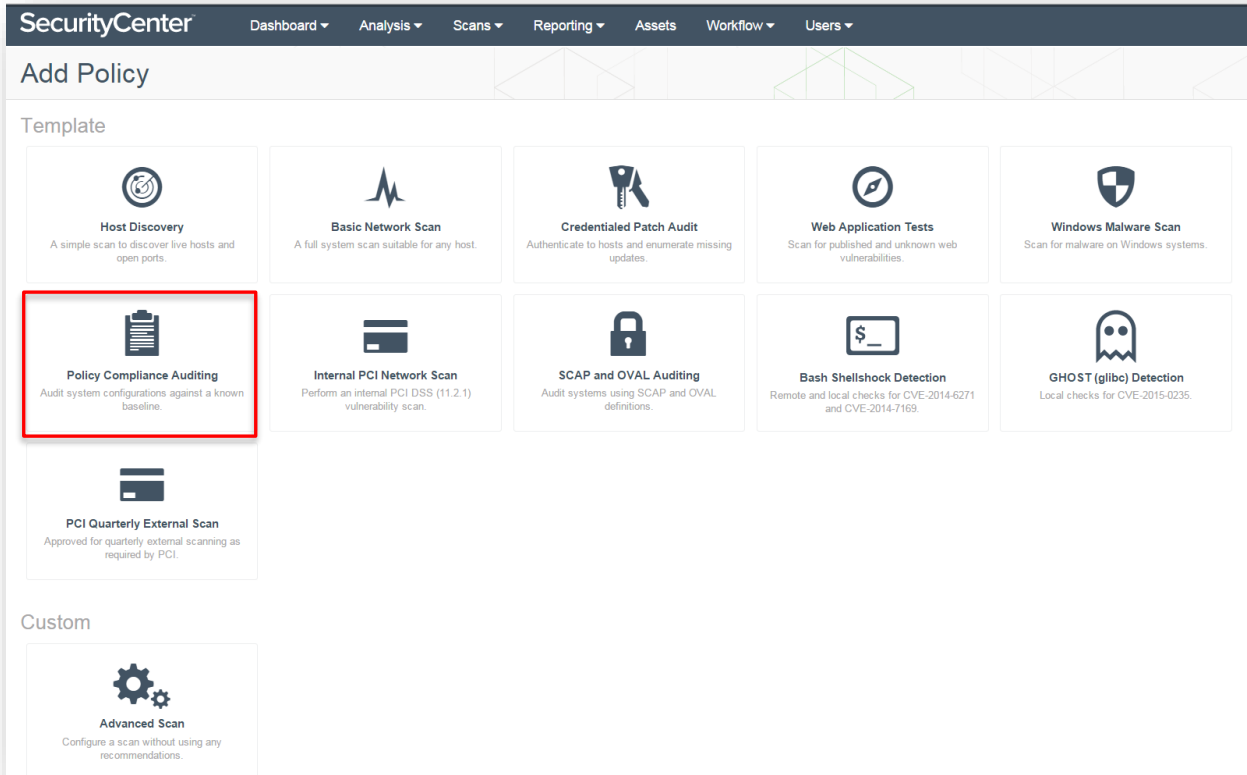
**SecurityCenter** Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾

## Credentials

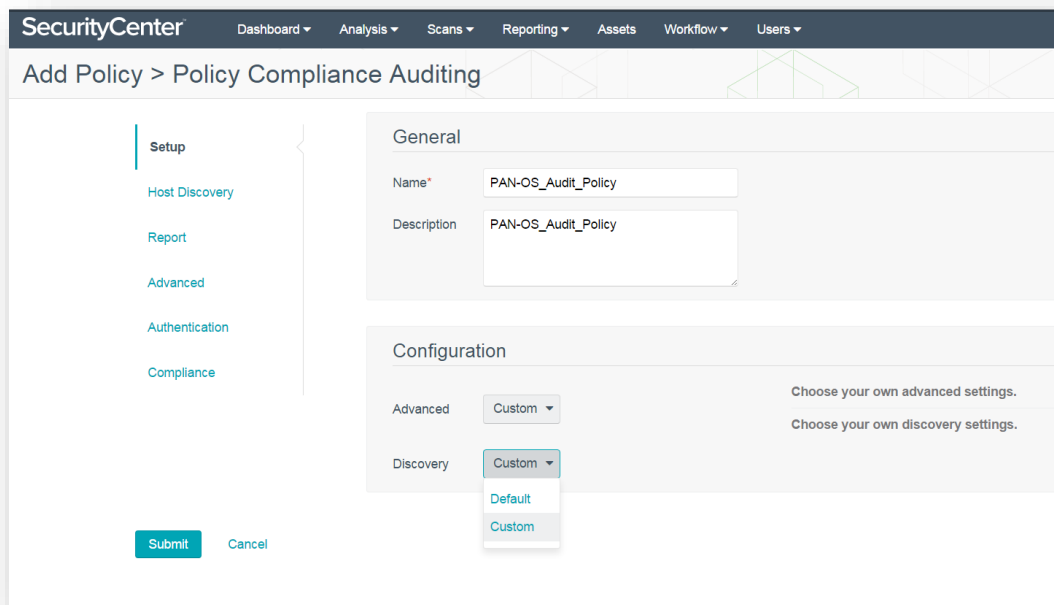
Active Scans Agent Scans Scan Results **Policies** Audit Files Credentials Blackout Windows

Name	Type	Group
PAN-OS_SNMP_Credentials	SNMP	Full Access

Select the “Policy Compliance Auditing” template.

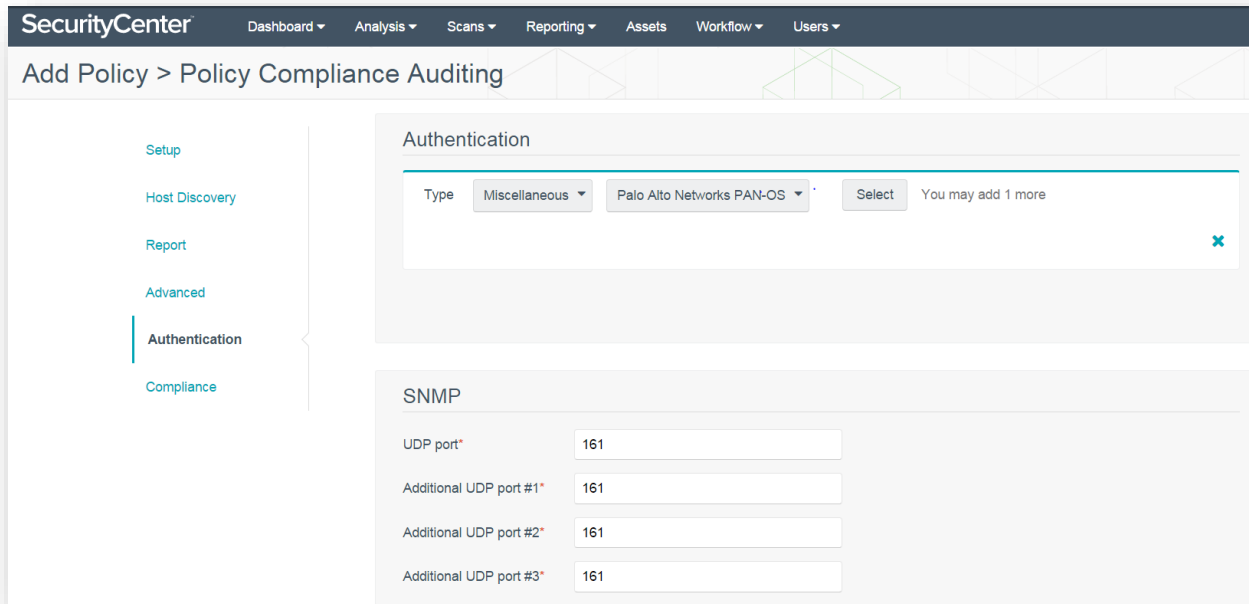


In the “Setup” section, enter a name for the audit policy and a description (optional). The options under “Configuration” can be left as “Default” or set to “Custom”. If the configuration options are set to “Custom”, the “Advanced” and “Host Discovery” categories will be enabled in the left-hand menu. Leaving the options as “Default” will keep those items hidden.

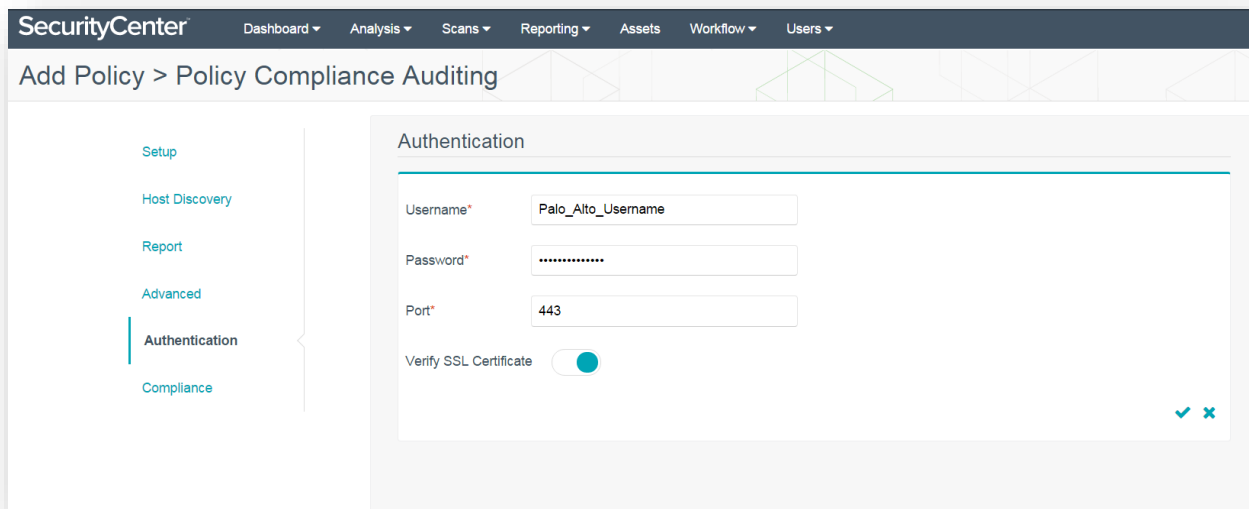


Navigate to the “Authentication” section, and click “+Add Authentication Settings”. Under the “Authentication” section, click the drop-down next to “Type” and select “Miscellaneous”. Click the second drop-down and select “Palo Alto Networks PAN-OS” and then click “Select”.

SNMP ports default to port 161. Configure ports to correspond to SNMP port settings in PAN-OS.

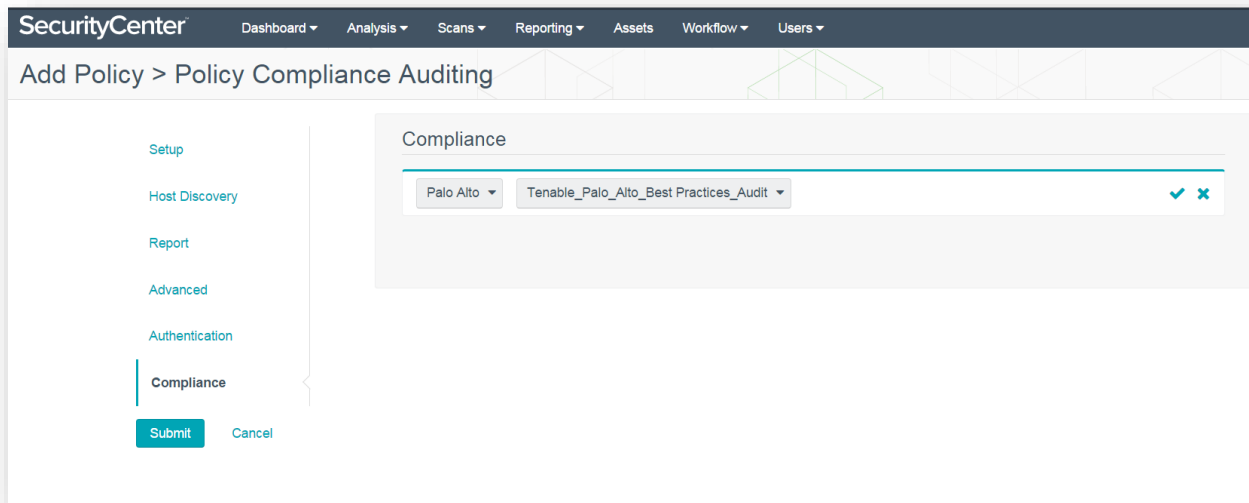


In the “Authentication” section, enter the “Username” and “Password” to allow SecurityCenter to authenticate to PAN-OS. Specify the “Port” (default is 443) and enable or disable “Verify SSL Certificate” (enabled by default). Click the checkmark to finalize the settings.



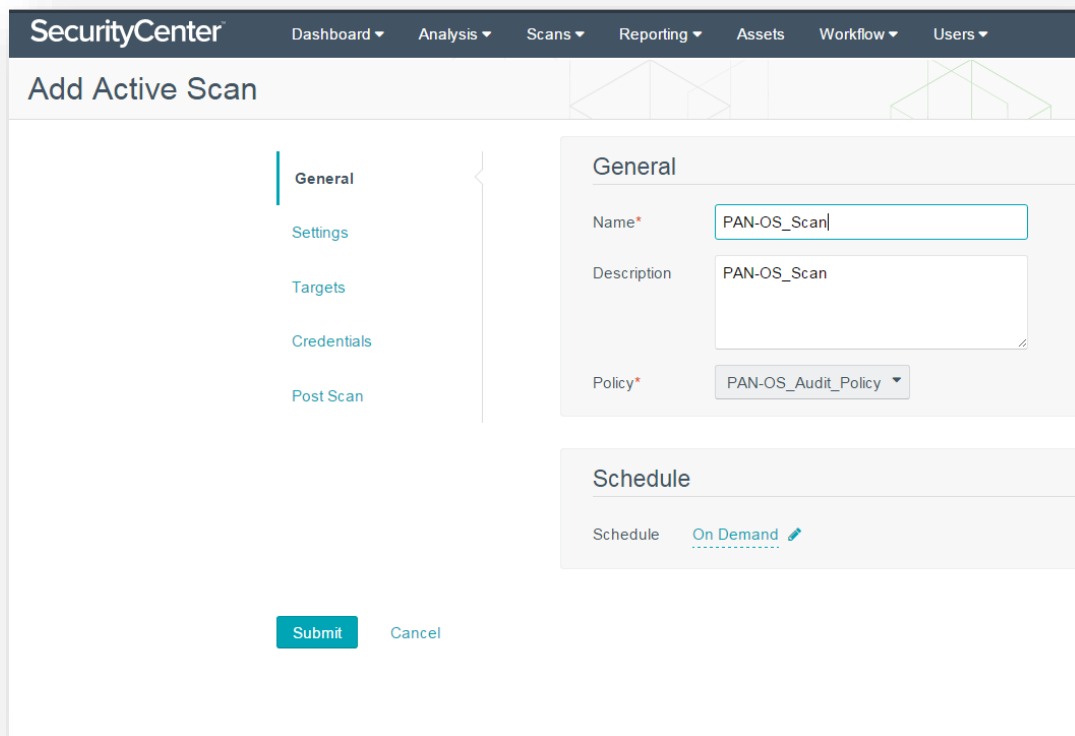


Navigate to the “Compliance” section and click “+Add Audit File”. In the “Compliance” section, click the “Select a Type” drop-down and select “Palo Alto”. Next, click the “Select an Audit File” drop-down and select the previously configured Palo Alto audit file. Click the checkmark to finalize the settings.

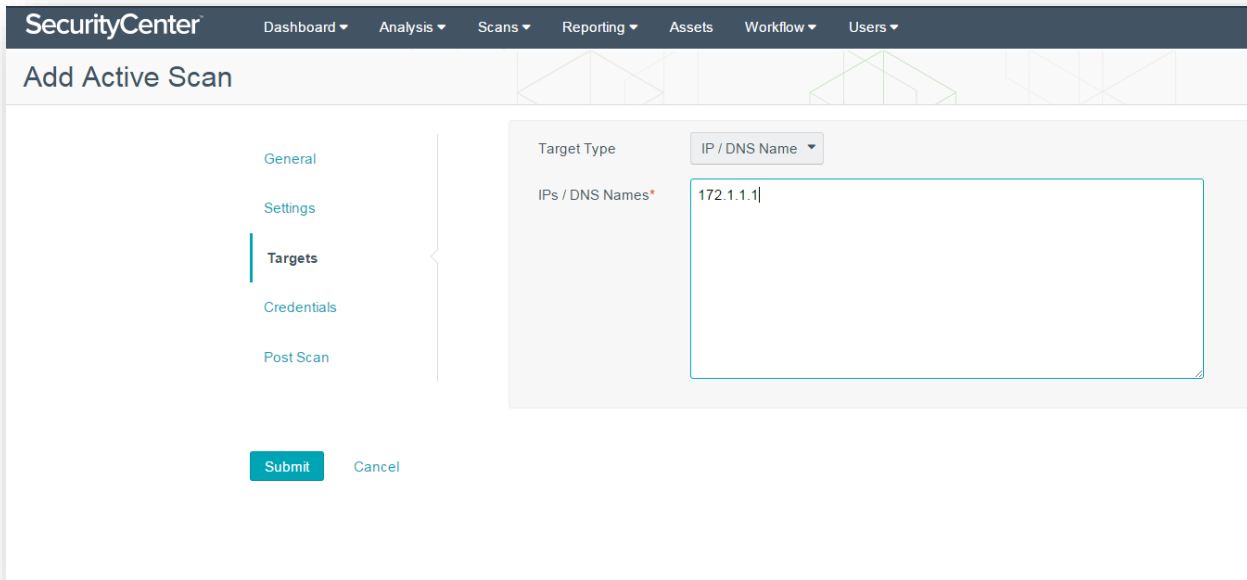


To create an audit scan of Palo Alto NGFWs, click on “Scans” and select “Active Scans”. Click on “+Add”.

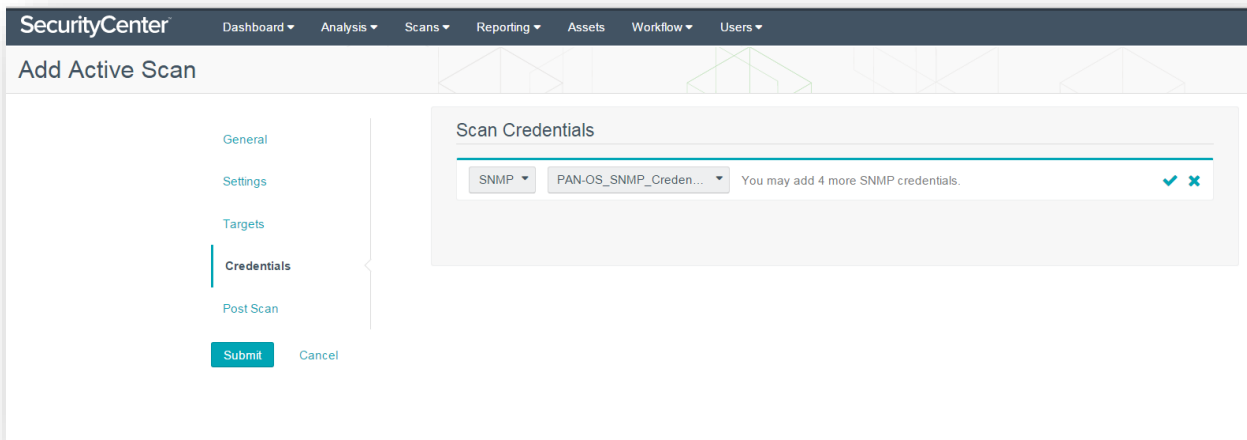
In the “General” section, enter a scan name and description (optional). Click the “Select a Policy” drop-down and select the previously configured Palo Alto audit policy. In the “Schedule” section, the scan can be configured to run “On Demand” (default), or it can be configured to run on a custom schedule as required.



Navigate to the “Targets” section and click the “**Target Type**” drop-down. Select “**IP/DNS Name**” and enter the Palo Alto NGFW IP address or DNS name.



Navigate to “Credentials” and click “+ Add Credential”. Click the drop-down and select “**SNMP**”. Once SNMP is selected, a second drop-down box will appear. Click the box and select the previously configured SNMP credentials for PAN-OS. Click the checkmark to finalize the settings.



## Importing Palo Alto NGFW Logs

Real-time log data from Palo Alto NGFWs can be imported into SecurityCenter (via LCE). Integration requires configuration changes within PAN-OS and within SecurityCenter, as well as the installation and configuration of Tenable NetFlow Monitor.

Within PAN-OS, the following configuration tasks are required:

- Configure Tenable Log Correlation Engine (LCE) as a syslog server
- Enable log forwarding to LCE
- Permit and Deny policy configuration
- Define NetFlow server IP address and port

For detailed instruction on configuring PAN-OS for integration please refer to the [Palo Alto PAN-OS Administrator's Guide](#).

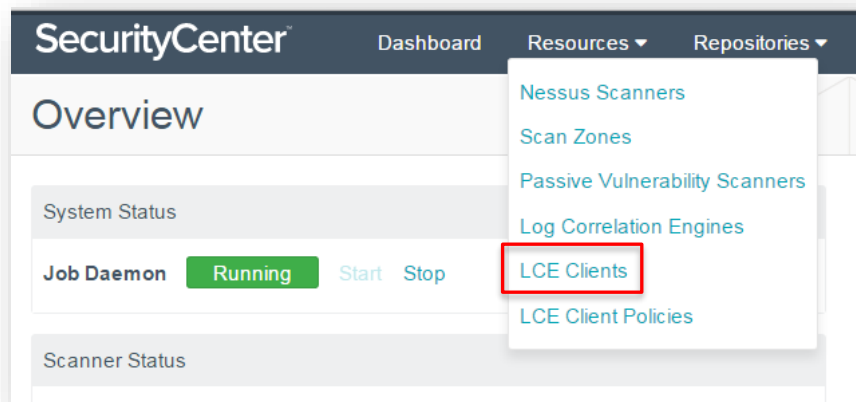
Once the PAN-OS configuration tasks are complete, download the Tenable NetFlow Monitor LCE client from the [Tenable Support Portal](#).

Install the Tenable NetFlow Monitor LCE client. Please refer to the [Log Correlation Engine 4.4 Client Guide](#) for detailed installation instructions.

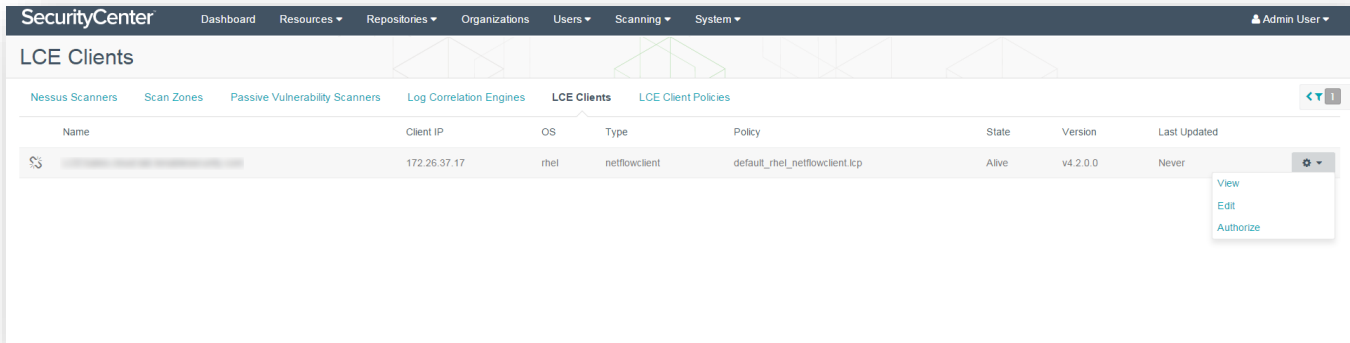


The Tenable NetFlow Monitor LCE client can be run directly on the LCE server. It must be configured to connect to either the localhost (127.0.0.1) or the IP address of the LCE server. Multiple LCE Client types (such as the LCE Log Agent and the Tenable NetFlow Monitor) can be run at the same time as well.

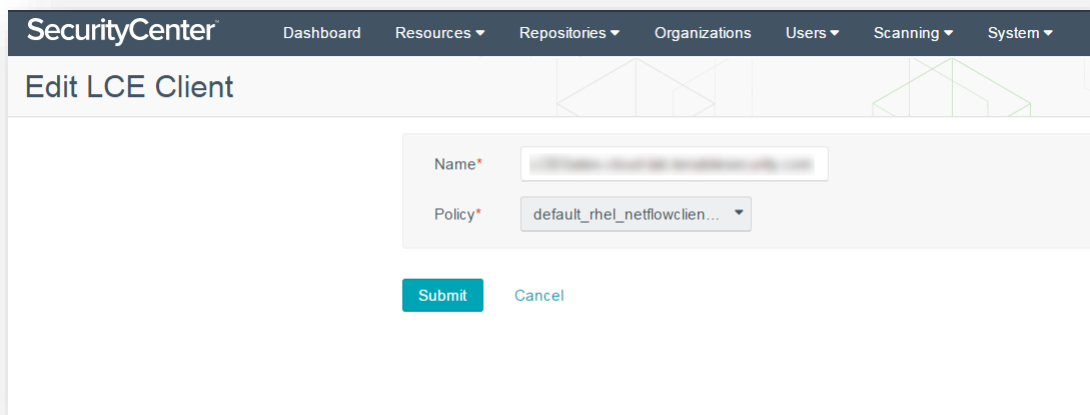
Log in to SecurityCenter using an admin account and navigate to “Resources” and select “LCE Clients”.



Click the drop-down arrow to the right of the “netflowclient” and select “Authorize”. If successful, a pop-up message stating it has been successfully authorized will appear.



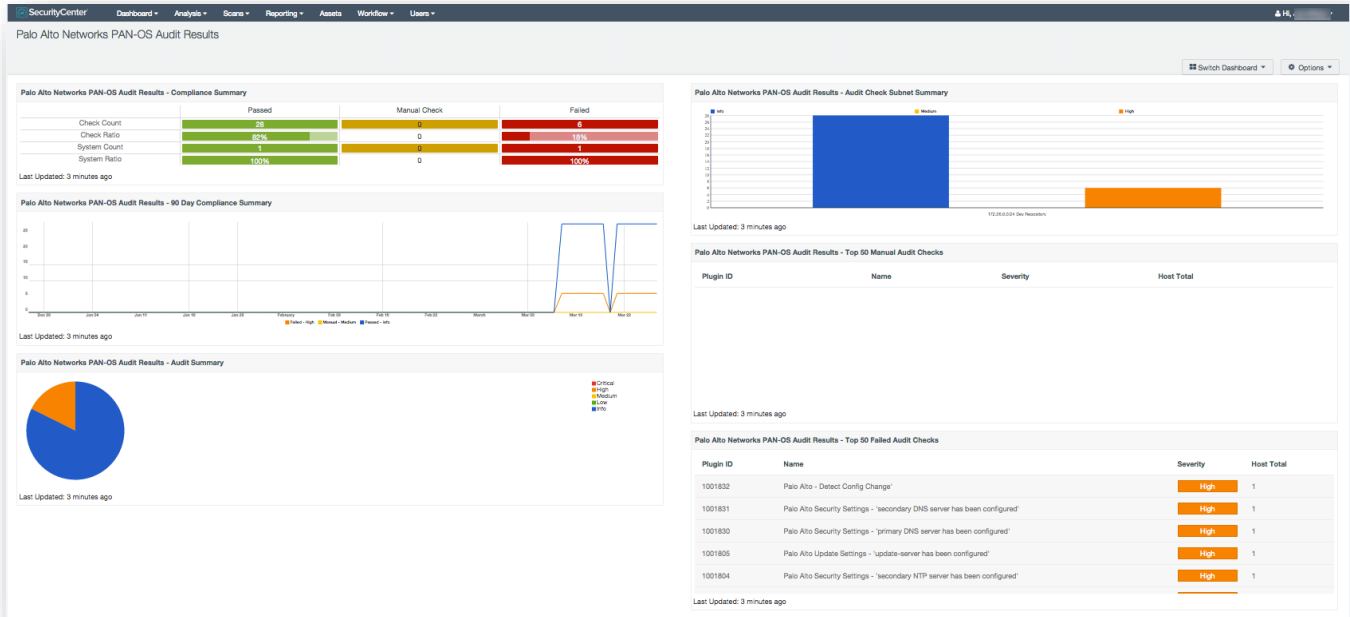
Click on the “netflowclient” to edit the LCE client and assign a policy. Click the “Policy” drop-down to select the desired policy. Click “Submit”. If successful, a pop-up message stating “LCE Client Edited Successfully” will appear.



Once configured, log data from the Palo Alto NGFW will be imported into SecurityCenter to help achieve 100% asset discovery. The log data can also be correlated against other data sources to uncover any potential advanced threats and to help organizations meet compliance obligations.

## Dashboards and Reports

Information obtained through Palo Alto NGFW configuration audits and the collection of log data can be easily viewed and analyzed through SecurityCenter's pre-defined, customizable dashboards and reports.



*Palo Alto Networks PAN-OS Audit Results Dashboard*

SecurityCenter™

## Palo Alto Networks PAN-OS Audit Report

February 2, 2016 at 3:33pm EST

[SC\_Manager]  
ORG\_1

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

*Palo Alto Networks PAN-OS Audit Report Title Page*

## Table of Contents

<b>About This Report</b> .....	<b>1</b>
<b>Executive Summary</b> .....	<b>2</b>
<b>Audit Summary</b> .....	<b>4</b>
3.2 - Failed Audits .....	5
3.3 - Manual Audits .....	6
3.4 - Passed Audits .....	7

### *Palo Alto Networks PAN-OS Audit Report Table of Contents*

## About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting [tenable.com](https://tenable.com).