

# Tenable and Fortinet Integration Guide

Last Revised: September 26, 2025

---



## Table of Contents

Introduction .....	3
Integration Overview .....	4
Integrate with Fortinet .....	5
Fortinet NGFW Configuration Audit .....	5
Import Fortinet NGFW Logs .....	14
Dashboards and Reports .....	16

---

# Introduction

---

This document describes how to deploy Tenable Security Center and Nessus® for integration with the FortiGate next-generation firewall (NGFW) platform by Fortinet. Please email any comments and suggestions to Tenable Support.

Monitoring the security settings of your Fortinet 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 Fortinet 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.

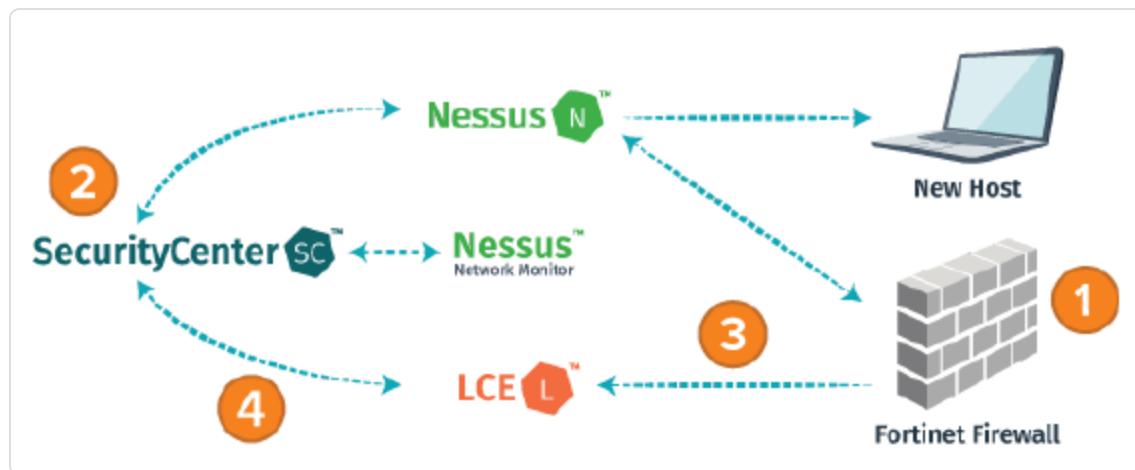
Benefits of integrating Tenable Tenable Security Center with Fortinet include:

- 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 Nessus Network Monitor
- 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

# Integration Overview

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

In addition to configuration audits, Tenable can also import real-time log data from Fortinet firewalls into its Log Correlation Engine® (LCE®) to help identify assets on networks not monitored by Nessus Network Monitor. Once hosts are identified they can be automatically assigned to dynamic asset lists and audited with Nessus to detect any possible vulnerabilities or misconfigurations.



Nessus Manager version 6.x, Tenable Vulnerability Management, and Tenable Security Center version 4.8 and higher support Fortinet integration. Nessus, Tenable Vulnerability Management and Tenable Security Center solutions work with Fortinet FortiOS versions 4.3 and above.

# Integrate with Fortinet

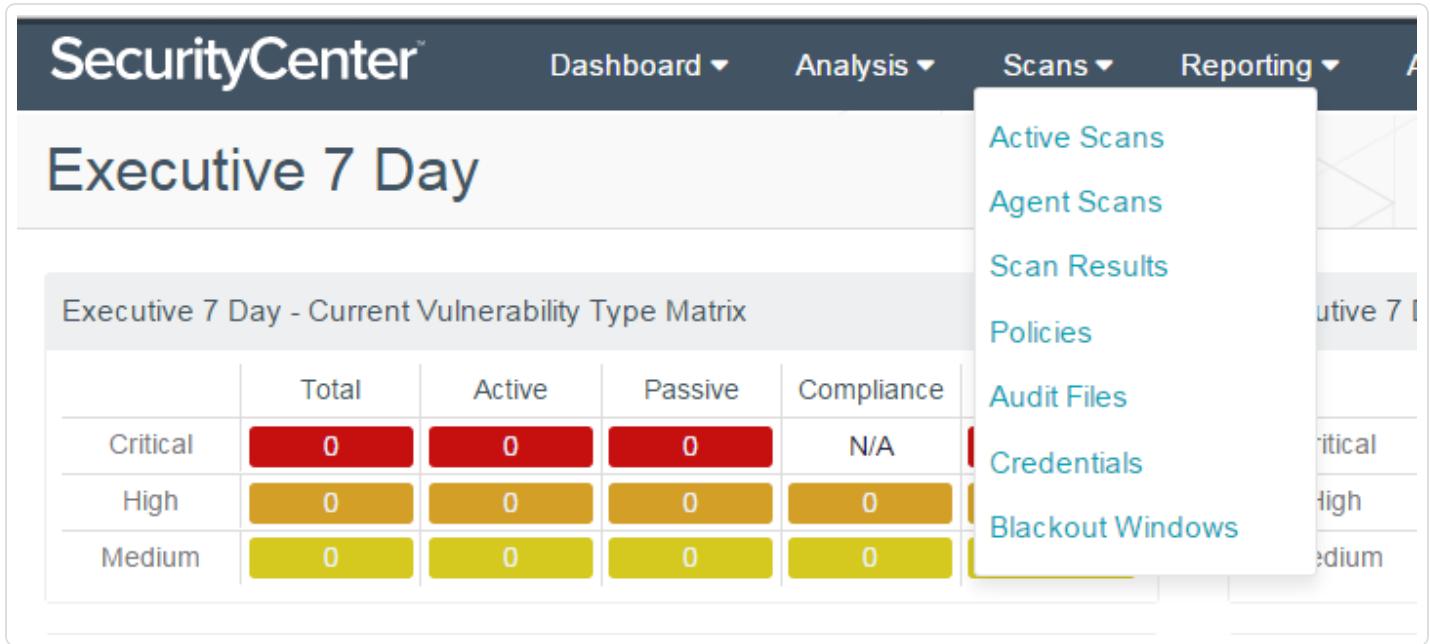
[Fortinet NGFW Configuration Audit](#)

[Import Fortinet NGFW Logs](#)

[Dashboards and Reports](#)

## Fortinet NGFW Configuration Audit

To begin the integration configuration, log in to Tenable Security Center, click **Scans** and select **Audit Files**.



The screenshot shows the Tenable Security Center interface. The top navigation bar includes 'SecurityCenter', 'Dashboard', 'Analysis', 'Scans', 'Reporting', and other options. A dropdown menu is open under 'Scans', showing 'Audit Files' as the selected option. Below the navigation, a section titled 'Executive 7 Day' displays a 'Current Vulnerability Type Matrix' table. The table has columns for 'Total', 'Active', 'Passive', and 'Compliance', and rows for 'Critical', 'High', and 'Medium' severity levels. All cells in the table contain the value '0'.

	Total	Active	Passive	Compliance
Critical	0	0	0	N/A
High	0	0	0	0
Medium	0	0	0	0

Click **+Add** and select **FortiGate FortiOS** from the list of available audit file templates.

**SecurityCenter**

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

## Add Audit File

### Templates

Adtran NetVanta	BlueCoat ProxySG	Brocade FabricOS	Check Point GAiA	Cisco IOS
Extreme ExtremeXOS	FireEye	FortiGate FortiOS	HP ProCurve	Huawei VRP
NetApp Data ONTAP	Palo Alto Networks PAN-OS	RHEV	SonicWALL SonicOS	Unix
Windows File Contents				

### Custom

**Advanced**  
Create a custom audit file.

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

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

## Edit FortiGate FortiOS Audit File

General

Name\* FortiGate Audit File

Description FortiGate Audit File

Submit Cancel

Click **Credentials** and click **+Add**.

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

## Audit Files

Active Scans	Agent Scans	Scan Results	Policies	Audit Files	Credentials	Blackout Windows	
Name ▾	Type			FortiGate Audit File	FortiGate FortiOS 1.13	Full Access	SC_Manager

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 ▾

## Add Credential

### General

Name\*

Description

### Credential

Type

Community\*

Next, create the scan policy by navigating to “Policies” and clicking **+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.

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

## Add Policy

### Template

 <b>Host Discovery</b> A simple scan to discover live hosts and open ports.	 <b>Basic Network Scan</b> A full system scan suitable for any host.	 <b>Credentialated Patch Audit</b> Authenticate to hosts and enumerate missing updates.	 <b>Web Application Tests</b> Scan for published and unknown web vulnerabilities.	 <b>Windows Malware Scan</b> Scan for malware on Windows systems.
 <b>Policy Compliance Auditing</b> Audit system configurations against a known baseline.	 <b>Internal PCI Network Scan</b> Perform an internal PCI DSS (11.2.1) vulnerability scan.	 <b>SCAP and OVAL Auditing</b> Audit systems using SCAP and OVAL definitions.	 <b>Bash Shellshock Detection</b> Remote and local checks for CVE-2014-6271 and CVE-2014-7169.	 <b>GHOST (glibc) Detection</b> Local checks for CVE-2015-0235.
 <b>PCI Quarterly External Scan</b> Approved for quarterly external scanning as required by PCI.				

### Custom

 <b>Advanced Scan</b> Configure a scan without using any recommendations.
--

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.

General

Name\* FortiOS\_Audit\_Policy

Description FortiOS\_Audit\_Policy

Configuration

Advanced Custom

Discovery Custom

Choose your own advanced settings.

Choose your own discovery settings.

Custom

Default

Submit Cancel

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

Compliance

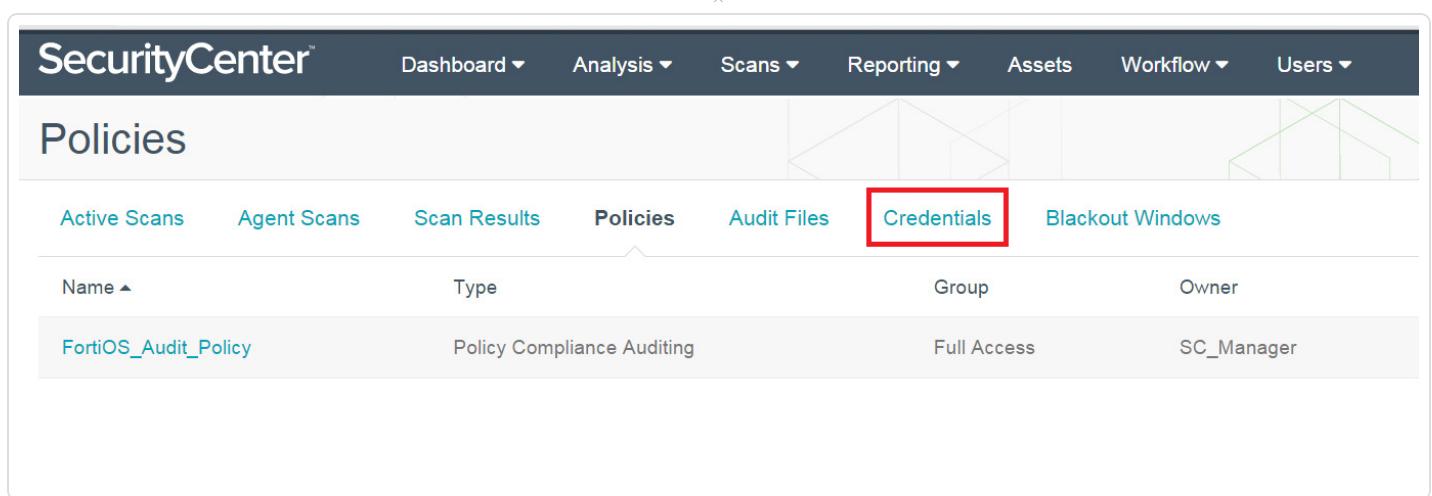
FortiGate FortiOS

FortiGate Audit File

Selected

Submit Cancel

In the “Policies” section, navigate to **Credentials**.



Name ▲	Type	Group	Owner
FortiOS_Audit_Policy	Policy Compliance Auditing	Full Access	SC_Manager

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

Within the “Credential” section, click the drop-down next to “Type” and select **SSH**. Click the **Authentication Method** drop-down and select the correct option for your environment. Enter the SSH username used to authenticate to the Fortinet firewall and then click **Choose File** to select the **Private Key** file. Next, enter the **Passphrase** and then click the **Privilege Escalation** drop-down and select **None**. Click **Submit**.

General

Name\* FortiOS\_SSH\_Credentials

Description FortiOS\_SSH\_Credentials

Credential

Type SSH

Authentication Method Public Key

Username\* SSH\_User

Private Key\* Choose File

Passphrase .....

Privilege Escalation None

Submit Cancel

To create an audit scan of Fortinet 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 FortiGate FortiOS 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.

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

## Add Active Scan

[General](#)
[Settings](#)
[Targets](#)
[Credentials](#)
[Post Scan](#)

### General

Name\*

Description

Policy\*

### Schedule

Schedule On Demand

[Submit](#)
[Cancel](#)

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

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

## Add Active Scan

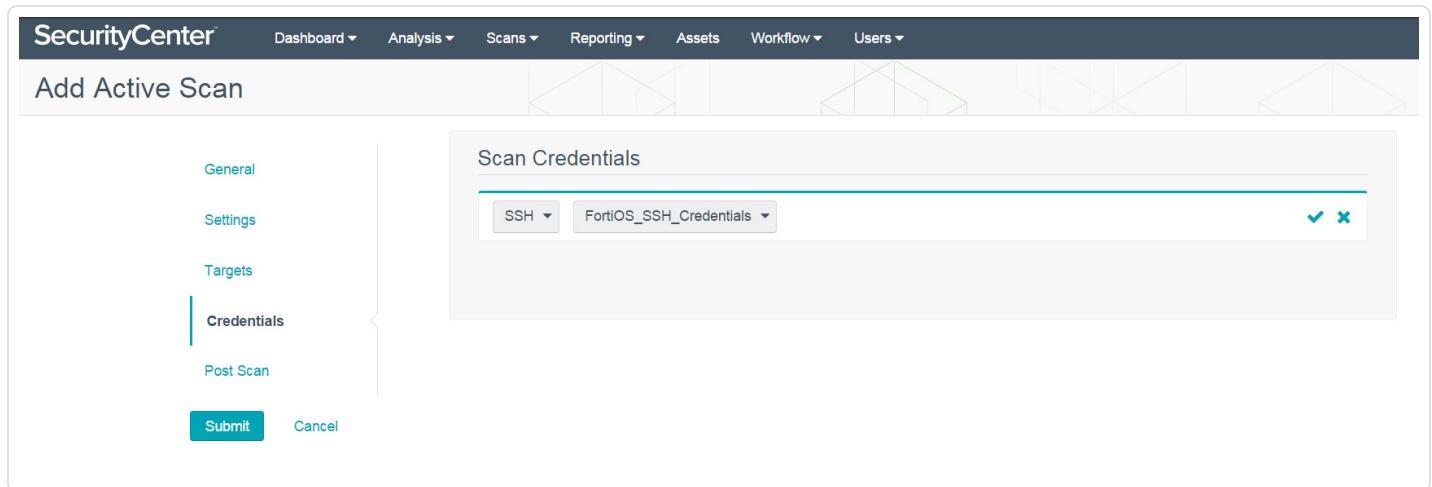
[General](#)
[Settings](#)
[Targets](#)
[Credentials](#)
[Post Scan](#)

Target Type

IPs / DNS Names\*

[Submit](#)
[Cancel](#)

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



**Note:** Integrating Tenable Security Center and Fortinet to perform audit checks requires configuration in both Tenable Security Center and FortiOS. For detailed instruction on configuring FortiOS for integration, please refer to the [Fortinet FortiGate/FortiOS Admin Guide](#).

## Import Fortinet NGFW Logs

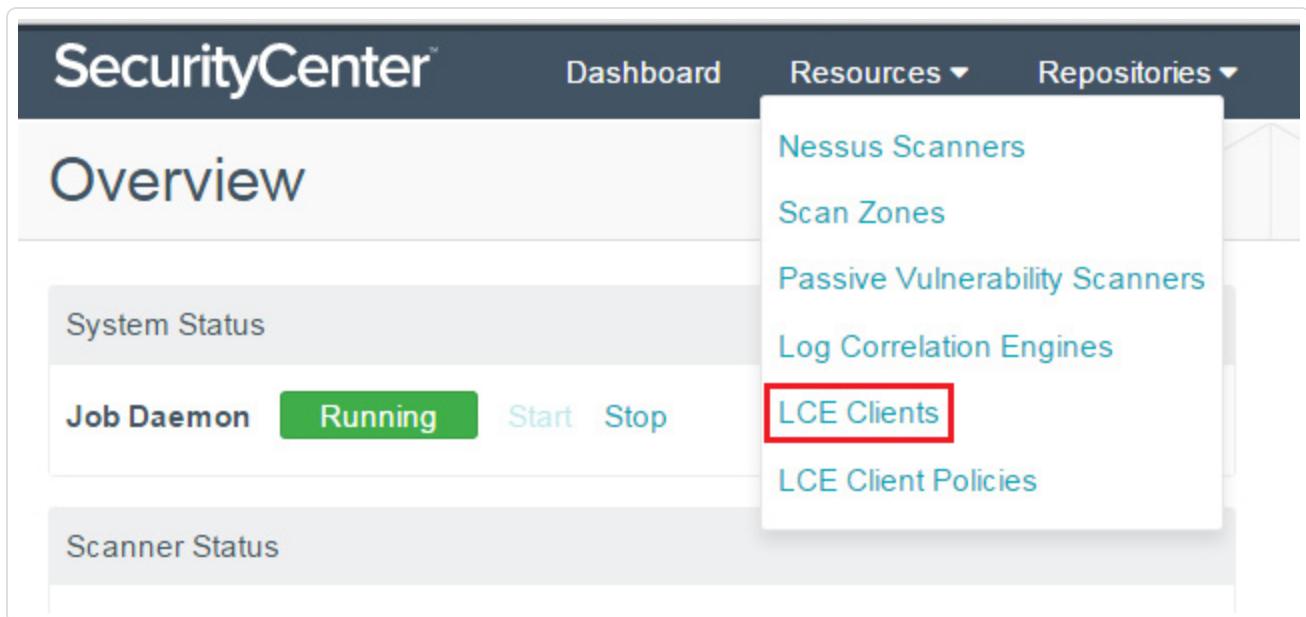
Real-time log data from Fortinet NGFWs can be imported into Tenable Security Center (via LCE). Integration requires configuration changes within FortiOS and within Tenable Security Center, as well as the installation and configuration of Tenable NetFlow Monitor.

To begin the integration, download the Tenable NetFlow Monitor LCE client from the [Tenable Downloads](#) page.

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

**Note:** 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 Tenable Security Center using an admin account and navigate to “Resources.” Select **LCE Clients**.



SecurityCenter™

Dashboard Resources ▾ Repositories ▾

## Overview

System Status

Job Daemon Running Start Stop

Scanner Status

Nessus Scanners

Scan Zones

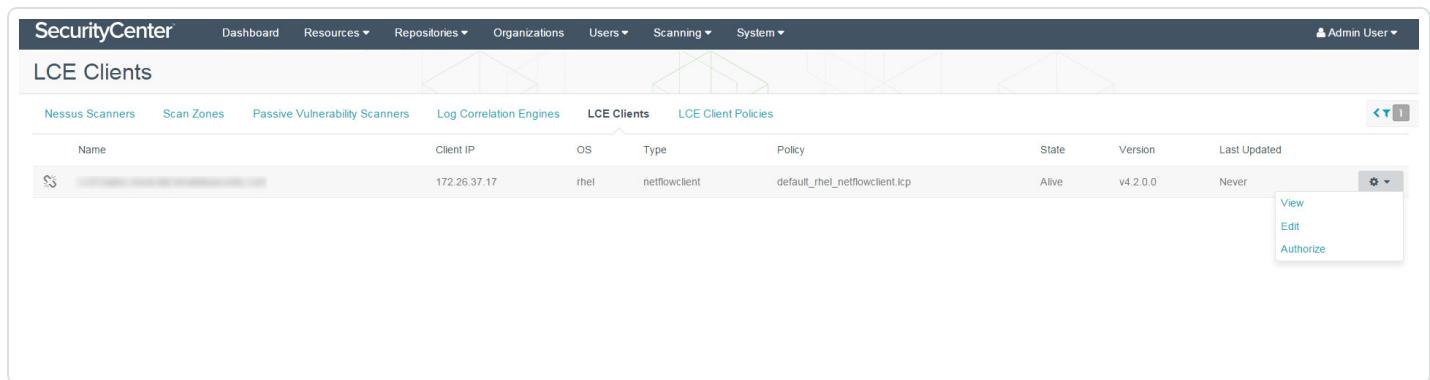
Passive Vulnerability Scanners

Log Correlation Engines

LCE Clients

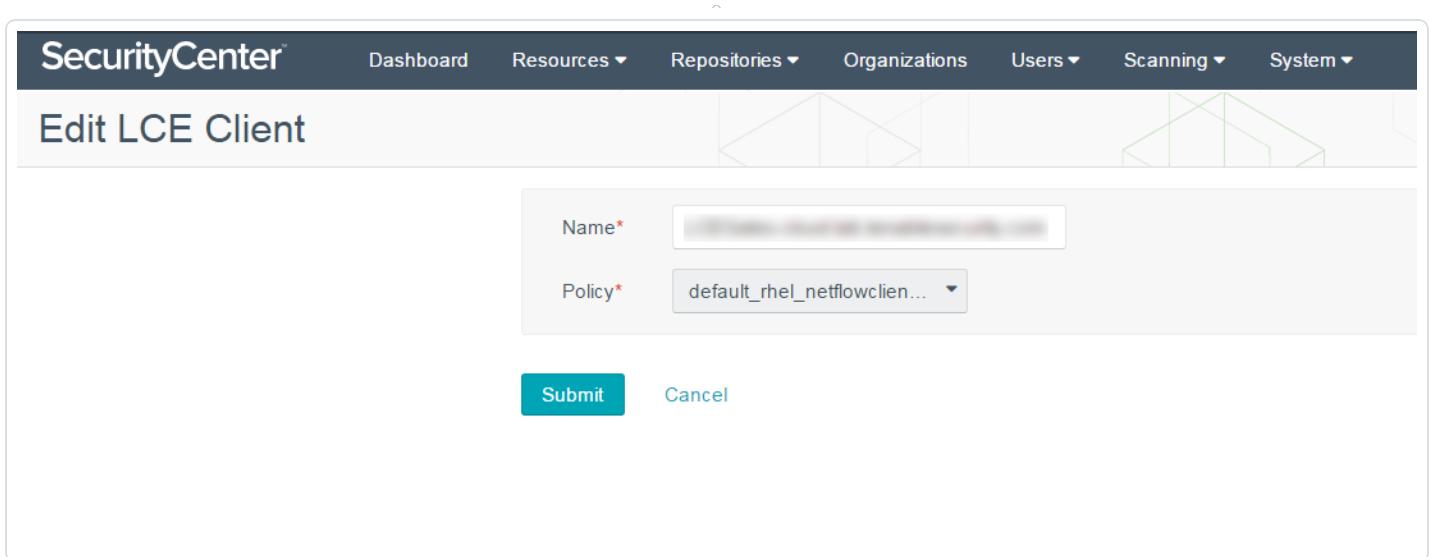
LCE Client Policies

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.



Name	Client IP	OS	Type	Policy	State	Version	Last Updated
172.26.37.17	rhel	netflowclient	default_rhel_netflowclient.lcp	Alive	v4.2.0.0	Never	<span style="border: 1px solid #ccc; padding: 2px 5px;">More</span>

To complete the Tenable Security Center configuration, 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.



The screenshot shows the 'Edit LCE Client' page in the Tenable Security Center. The top navigation bar includes 'Dashboard', 'Resources', 'Repositories', 'Organizations', 'Users', 'Scanning', and 'System'. The main content area is titled 'Edit LCE Client'. A form is displayed with the following fields:

- Name\***: A text input field containing a blurred value.
- Policy\***: A dropdown menu set to 'default\_rhel\_netflowclient...'.

At the bottom of the form are two buttons: 'Submit' (in a teal box) and 'Cancel'.

**Note:** To complete the integration, please refer to the [Fortinet FortiGate/FortiOS Admin Guide](#) for detailed instructions on how to configure a syslog server and enable log forwarding.

Once configured, log data from the Fortinet NGFW will be imported into Tenable Security Center 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 Fortinet NGFW configuration audits and the collection of log data can be easily viewed and analyzed through Tenable Security Center's pre-defined, customizable dashboards and reports.

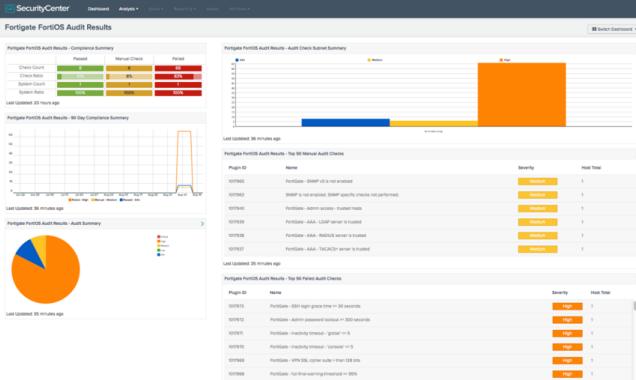
## SecurityCenter

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

, Member

### Add Dashboard Template

#### Fortigate FortiOS Audit Results



**Description**

Governance, Risk Management, and Compliance (GRC) is a substantial part of any information assurance program. A GRC requires information systems to be audited, regardless of the standard to which the audit is performed. This dashboard provides the audit results for Fortigate FortiOS.

One of the initial steps in a successful GRC program is to set configuration guidelines and establish a supportable set of security policies. SecurityCenter Continuous View (SC CV) can measure compliance using audit files that cover a wide range of major regulations and other auditable standards. Tenable provides over 500 audit files, which are available for download from the Tenable Support Portal [<https://support.tenable.com/support-center>], in categories such as operating systems, applications, databases, and network devices. Tenable products can be used to audit systems based on SCAP content, and many Tenable audit policies have been certified by the Center for Internet Security (CIS). More information about audit files can be found in the Tenable Discussion Forums [<https://discussions.nessus.org>], Tenable Support Portal

**Category:** Compliance & Configuration Assessment

**Created:** Dec 14, 2015 19:04

**Updated:** Dec 14, 2015 19:04

### FortGate FortiOS Audit Results Dashboard Template

- 17 -



# Fortigate FortiOS Audit Report

February 20, 2016 at 12:07pm 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.

FortiGate FortiOS 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

FortiGate FortiOS Audit Report Table of Contents