SonicOS 7.0

Endpoint Security

Administration Guide

SONICWALL®

Contents

1

Endpoint Security

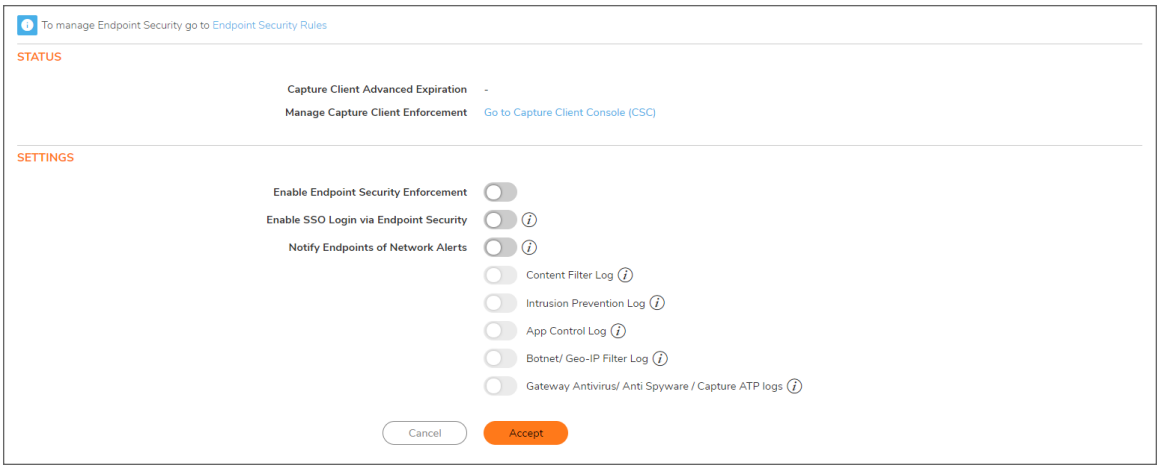
With **Endpoint Security**, you can manage logs for your product subscriptions and licensed security products in one location. Security products include Capture Client, Content Filtering, Intrusion Prevention, App Control, Botnet/GeoIP Filtering, and Gateway Anti-Virus/Anti Spyware/Capture ATP.

When enabled, Capture Client leverages cloud sandbox file testing, comprehensive reporting, and enforcement for endpoint protection, while providing consistent assurance of client security, with easy-to-use and actionable intelligence and reporting.

Endpoint Security can secure your endpoints no matter where they are located and help you keep them clean of malware while enforcing access and content rules.

To configure the settings for Endpoint Security:

1. Navigate to **POLICY | Endpoint Security**.



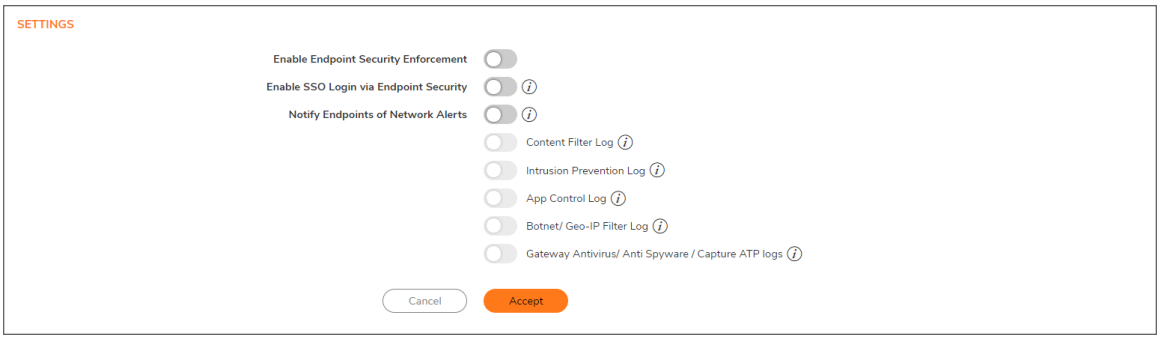
Topics:

Status

NOTE: To manage Endpoint Security, configure the Endpoint Security Rules at **POLICY | Rules and Policies > Endpoint Rules**.

- **Capture Client Advanced Expiration** displays the status of your subscription service to Capture Client Advanced, indicating how much time is remaining in your service.
- **Capture Client Management** provides a link to log into the Capture Client Console. Click that link to launch the console and login to manage your service.

Settings



Enabling services in the Settings section:

1. Click **Enable Endpoint Security Enforcement** to activate the service.
2. Click **Enable SSO Login via Endpoint Security** to periodically send logged in OS user information (domain/username format) from your Endpoint Security endpoints to your SonicWall firewalls. You can see the logged in user status listed under **Users**.
3. Click **Notify Endpoints of Network Alerts** when an event is blocked on your firewall or other modules (GAV/IPS/ATP, Botnet/Geo-IP, and so on), Endpoint Security can notify you with a message to alert you or specific end users directly. Currently, this features supports only Client SentinelOne (Capture) Enforcement.
4. Enabling the **Content Filter Log** provides logging for CFS Events to Capture Client endpoint devices.
5. Enabling the **Intrusion Prevention Log** provides logging for IPS Events to Capture Client endpoint devices.

6. Enabling the **App Control Log** provides logging for APP Control Events to Capture Client endpoint devices.
7. Enabling the **Botnet/Geo-IP Filter Log** provides logging for Botnet/Geo-IP Events to Capture Client endpoint devices.
8. Enabling the **Gateway Anti-Virus/Anti Spyware/Capture ATP logs** provides logging for GAV/GAS/ATP Events to Capture Client endpoint devices.
9. Click **Accept** when you have finished.

2

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

SonicOS Endpoint SecurityAdministration Guide
Updated - April 2024
Software Version - 7.0
232-005329-00 Rev C

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035