

SonicOS 7.0

Endpoint Security

Administration Guide

SONICWALL®

Contents

- Endpoint Security** 3
- Status 4
- Settings 4

- SonicWall Support** 6
- About This Document 7

Endpoint Security

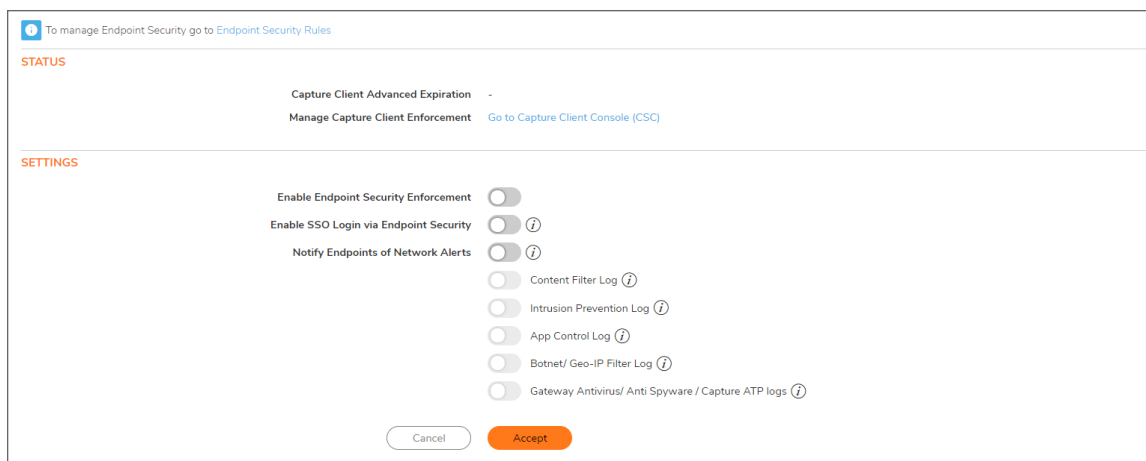
With **Endpoint Security**, you can manage logs for your product subscriptions and licensed security products in one location. Security products include Capture Client, Content Filtering, Intrusion Prevention, App Control, Botnet/GeoIP Filtering, and Gateway Anti-Virus/Anti Spyware/Capture ATP.

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](#)
- [Settings](#)

Status

STATUS

Capture Client Expiration 06/30/2024

Capture Client Management [Go to Capture Client Console](#)

① **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

SETTINGS

Enable Endpoint Security Enforcement

Enable SSO Login via Endpoint Security ⓘ

Notify Endpoints of Network Alerts ⓘ

Content Filter Log ⓘ

Intrusion Prevention Log ⓘ

App Control Log ⓘ

Botnet/ Geo-IP Filter Log ⓘ

Gateway Antivirus/ Anti Spyware / Capture ATP logs ⓘ

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.

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 Security Administration Guide

Updated - April 2024

Software Version - 7.0

232-005329-00 Rev C

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

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