

Capture Client

Deep Visibility Getting Started  
Guide

SONICWALL®

# Contents

- Overview** ..... 3
- About Deep Visibility** ..... 4
  - Default Retention Period for Deep Visibility Data ..... 4
  - Getting Started ..... 4
  - Accessing SentinelOne Help ..... 5
  - Finding Threat Hunt Queries in SentinelOne ..... 6
- SentinelOne Hunter Chrome Extension** ..... 7
  - Installing SentinelOne Hunter Chrome Extension ..... 7
  - SentinelOne Hunter Modes ..... 8
    - SentinelOne Hunter Scraper Mode ..... 9
    - SentinelOne Library Mode ..... 10
  - Licensing SentinelOne Hunter Chrome Extension ..... 10
- Rogues Detection** ..... 11
  - Rogues Detection- FAQs ..... 11
- Useful References** ..... 12
- SonicWall Support** ..... 13
  - About This Document ..... 14

# Overview

Capture Client Premier leverages the complete package offered by SentinelOne, enabling Deep Visibility for the users. Deep Visibility feature is a unique solution that helps security teams gain comprehensive insight to all endpoints. Users can prioritize the endpoint responses through a streamlined interface. This does not require additional installation as it is already integrated to SentinelOne's single agent architecture.

This document describes on how to get started with the Deep Visibility feature from a Capture Client console.

① **NOTE:** SentinelOne offers detailed documentation on Deep Visibility that can be accessed when you are logged in to SentinelOne console. For more information, refer to [Accessing SentinelOne Help](#).

## Topics:

- [About Deep Visibility](#)
- [Getting Started](#)
- [Accessing SentinelOne Console](#)
- [Finding Threat Hunt Queries in SentinelOne](#)
- [SentinelOne Hunter Chrome Extension](#)
- [Installing SentinelOne Hunter Chrome Extension](#)
- [Accessing SentinelOne Help](#)
- [Useful References](#)

# About Deep Visibility

Capture Client Premier powered by SentinelOne's Deep Visibility feature helps you to search across endpoints for all Indicators of Compromise (IOC), adding benign detection data to the EPP data of the core solution.

Data is collected from each device and sent to cloud for storage, deep visibility reporting, and threat hunting. The autonomous agent analyzes the events, processes, and files.

Every element of a story is linked to Storyline. This gives you the full picture of what has happened on a device and reason for it to happen. Thus the Storyline also helps you save time by searching easily to view the full chain of events.

Deep visibility helps users to gain insights into file integrity and data integrity and monitors traffic at the end of the tunnel, which allows an unprecedented tap into all traffic without the need to decrypt or interfere with the data transport. This empowers users with a rich environment for threat hunting that includes powerful filters and the ability to take containment actions, along with fully automated detection and response.

## Default Retention Period for Deep Visibility Data

Default data retention period for Deep Visibility is 14 days. However, data retention can be extended on a request basis, with additional cost.

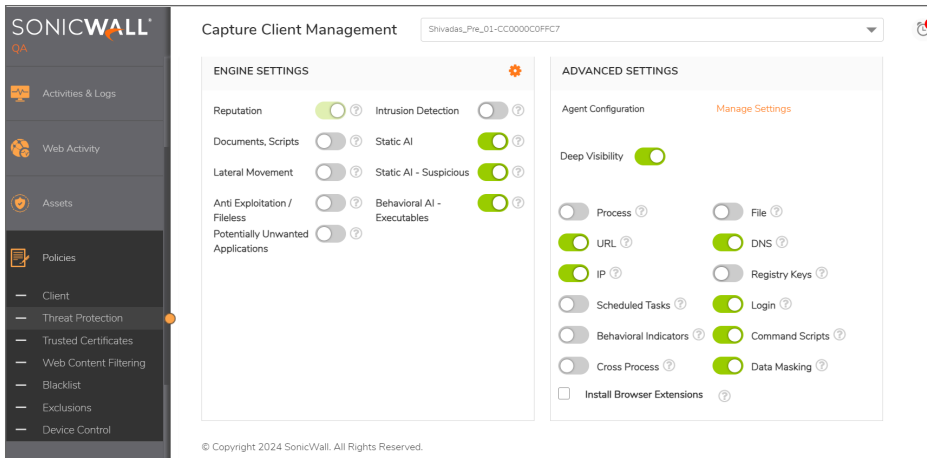
For more information on Deep Visibility Data Volume Retention, Connectivity, and Encrypted Data Inspection, refer to the [Deep Visibility SentinelOne Help](#).

## Getting Started

To get started with Deep Visibility from Capture Client console:

1. Log in to Capture Client Management console as a Premier tenant.
2. Select the required account or tenant.
3. Go to **Policies > Threat Protection** on the left menu.

4. Turn on the option Deep Visibility in the **Advanced Settings**.



① **NOTE:** If the option **Data Masking** is enabled, you may not be able to view the file names and paths of ZIP, TAR, RAR, PDF, and MS Office files. It is recommended not to turn on this feature unless necessary, as many files are masked and displayed as anonymous data.

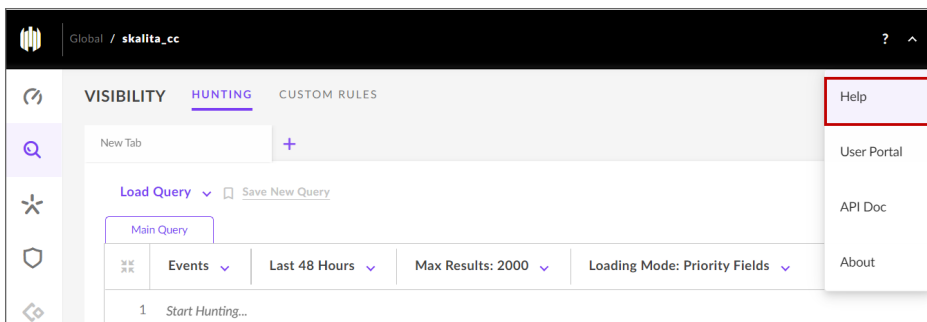
## Accessing SentinelOne Help

SentinelOne offers comprehensive documentation to help the users understand more about Deep Visibility.

① | **NOTE:** You can access the documentation only when you are logged in to the SentinelOne console.

To access SentinelOne help:

1. Click  to access the documentation from SentinelOne console.

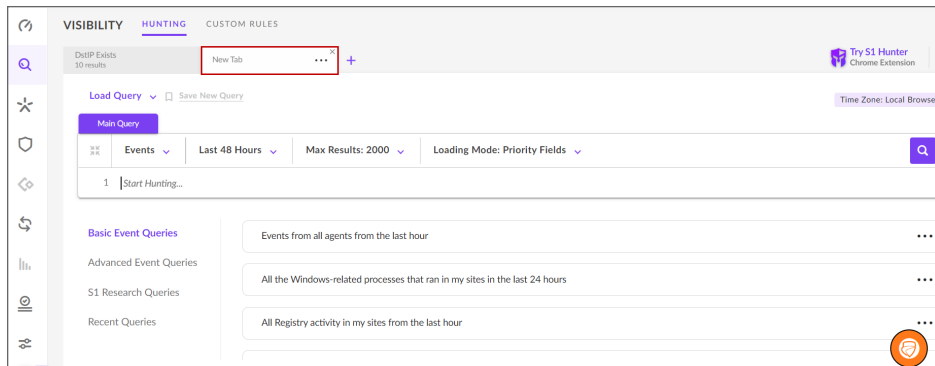


2. Click **Help** to view the SentinelOne documentation page.

# Finding Threat Hunt Queries in SentinelOne

The Visibility pane opens by default in SentinelOne when you access the Deep Visibility feature from Capture Client console.

Click on the Hunting tab, and the threat hunt query library is displayed under the query builder.



For more information on Threat Hunting, refer to [Threat Hunting](#) in SentinelOne help.

# SentinelOne Hunter Chrome Extension

SentinelOne Hunter Chrome Extension works with Deep Visibility to hunt for indicators of interest or queries captured from your browser. Hunter opens up to 15 queries in your SentinelOne Deep Visibility console page to search for the selected data across your organization.

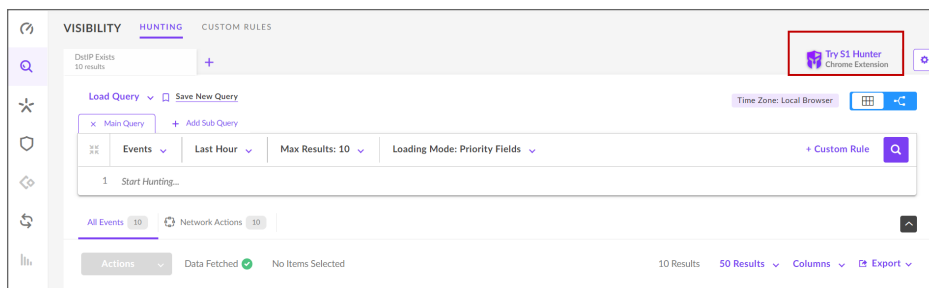
## Topics:

- [Installing SentinelOne Hunter Chrome Extension](#)
- [SentinelOne Hunter Modes](#)
- [Licensing SentinelOne Hunter Chrome Extension](#)


## Installing SentinelOne Hunter Chrome Extension

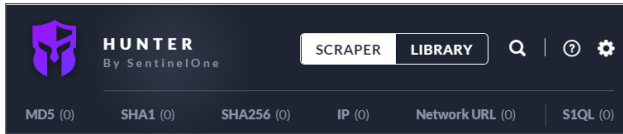
To install SentinelOne Hunter Chrome Extension:

1. Click **Try S1 Hunter Chrome Extension** on SentinelOne console:



2. Click **Download** and the SentinelOne Hunter Chrome displays the option to add it to chrome.
3. Click **Add to Chrome** and **Add Extension** to complete the process of adding SentinelOne Hunter to Chrome.

4. Click  to open the extension from the Chrome browser.
5. Select SentinelOne Hunter. The **Settings** window is displayed.
6. Specify the **Management URL**.
7. Click **Save**.
8. Select the **Scraper** or **Library** Mode as required.

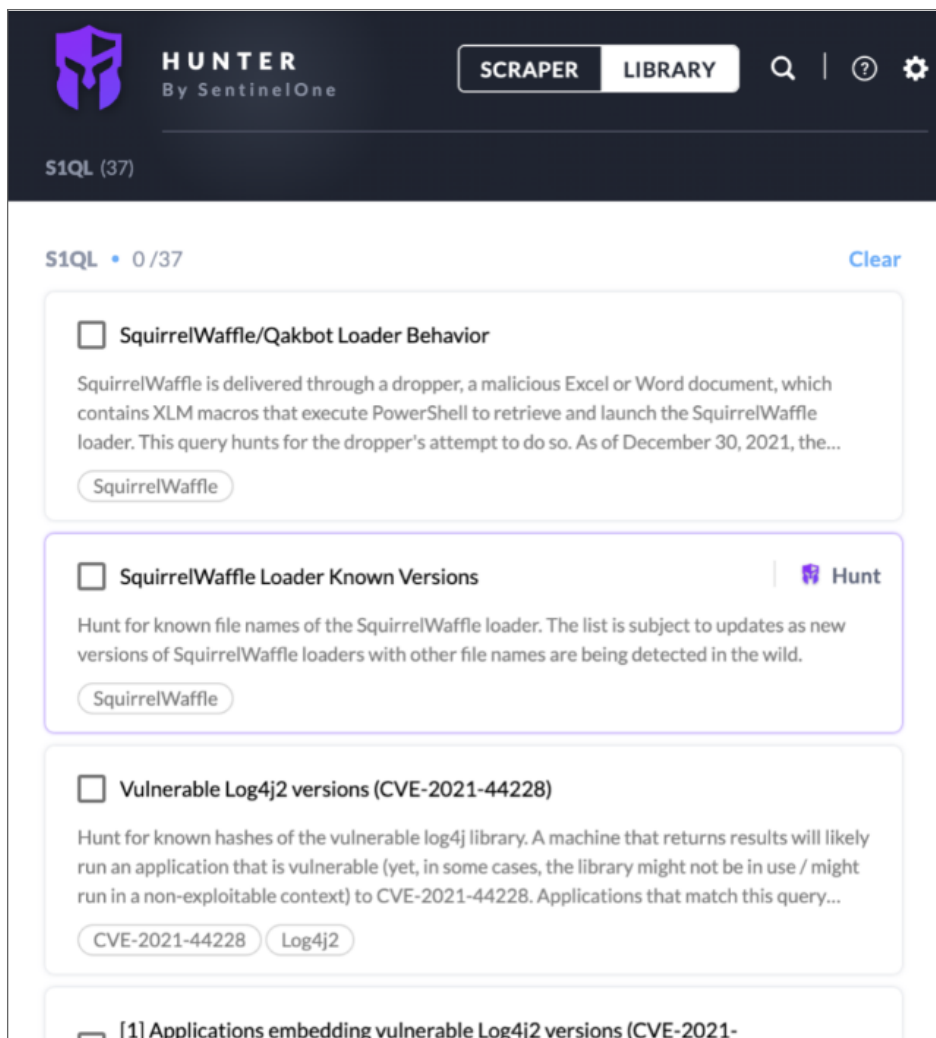


For more information on using Hunter Chrome Extension for Deep Visibility, refer to [SentinelOne Hunter Chrome Extension](#).

## SentinelOne Hunter Modes

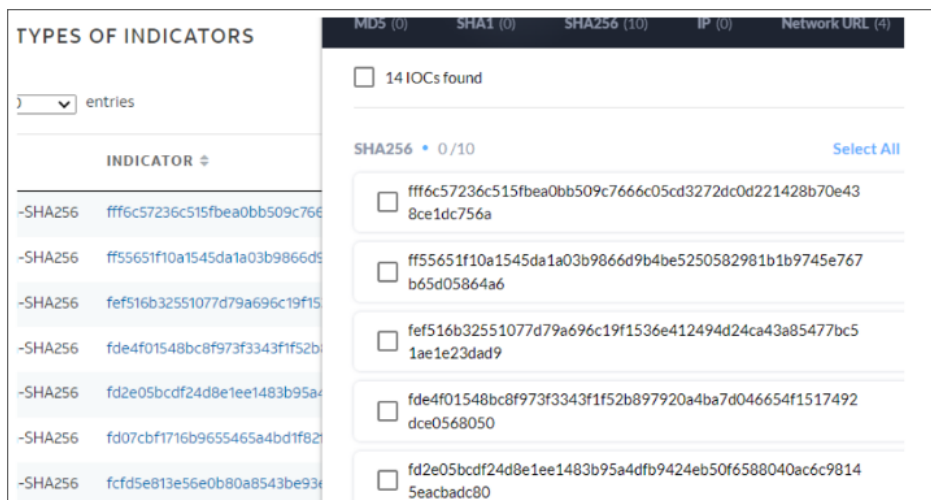
SentinelOne Hunter has two modes - **Scraper** mode and **Library** mode:





## SentinelOne Hunter Scraper Mode

In Scraper mode, Hunter captures these indicators from information open in the current browser tab. This includes IP addresses, Network URLs (DNS requests), and hashes (MD5, SHA-1, and SHA-256).



## SentinelOne Library Mode

In Library mode, Hunter opens a collection of SentinelOne queries.

You need to select one or more queries to run them easily in your management console ([Management URL](#)) and SentinelOne updates the Library dynamically.

## Licensing SentinelOne Hunter Chrome Extension

SentinelOne Hunter Chrome Extension does not require additional license. You can use Scraper or Library modes without additional license.

① **NOTE:** If you have to access the **Signal Hunting Library** that contains additional threat hunting queries, you need to purchase its subscription license separately.

# Rogues Detection

Rogues detection powered by SentinelOne gives visibility of endpoints connected to your network that are not currently protected. If Rogues detection feature is turned on, SentinelOne Agents scan the local subnet to identify and manage the connected endpoints on which the Agent is not yet installed.

Rogues thus provides the enterprise-wide visibility of unprotected endpoints, discovering gaps in the deployment, providing the snapshot of unsecured endpoints for which Agent shall be installed.

## Rogues Detection- FAQs

- *I see data in Rogues when the setting in Rogues is "Scanning Enabled on Networks with 2 Agents". But data is not displayed when the value is set as 10 or a higher value. Why?*  
If the criteria set is, "Scanning Enabled on Networks with 2 Agents", there has to be at least two agents in that network node for the agents to look for unprotected endpoints.  
If it is set to 10 or 100 and you are not getting results, it means that the criteria is not met; there are less than 10 or 100 Sentinel Agents in that Network.
- *I can see some devices where S1 Agent is installed from a different account as Rogues. Why?*  
When a Rogue scans and finds an endpoint it takes the Mac address and compares the database data for the Account where the endpoint resides.  
If the corresponding Mac address is not found it is considered a Rogue endpoint.
- *What is the difference between Ranger and Rogues Detection features offered by SentinelOne?*  
Rogues Detection is a light version of Ranger.

## Useful References

Given below are some of the useful references for Deep Visibility.

These links are accessible only when you are logged in to Capture Client console.

① **NOTE:** SentinelOne offers detailed documentation on Deep Visibility that can be accessed only when you are logged in to SentinelOne console. For more information, refer to [Accessing SentinelOne Help](#).

Click on the name to go to the reference:

- [Threat Hunting-Usecases](#)
- [Searching For-Behavioral-Indicators](#)
- [Customizing Hunting Rules](#)
- [Star Custom Rules](#)
- [Creating Deep Visibility Queries](#)
- [Deep Visibility Query Syntax](#)
- [Managing Deep Visibility Browser Extension](#)
- [Deep Visibility FAQs](#)
- [Rogues Overview](#)

# 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. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services at <https://sonicwall.com/pes>.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

Capture Client Deep Visibility Getting Started Guide  
Updated - January 2024  
232-005824-00 Rev D

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