

Capture Client

Premier Administration Guide

SONICWALL®

Contents

Overview	3
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
Hunter Chrome Extension	7
Installing SentinelOne Hunter Chrome Extension	7
SentinelOne Hunter Modes	9
SentinelOne Hunter Scraper Mode	10
SentinelOne Library Mode	10
Licensing SentinelOne Hunter Chrome Extension	10
Network Control	11
Getting Started with Network Control	11
Configurable Network Quarantine	13
Network Status	14
Network Quarantine Operations	14
Remote Shell	16
SentinelOne Remote Shell Use Case 1	16
SentinelOne Remote Shell Use Case 2	18
Rogues Detection	19
Rogues Detection- FAQs	19
Useful References	20
SonicWall Support	21
About This Document	22

Overview

Capture Client Premier Administration Guide provides an overview of the advance features that are offered by SentinelOne - Deep Visibility, Network Control, Remote Shell and Rogues Detection features. These features included in the Capture Client Premier license offers a unique solution that can help security teams gain comprehensive insight across their 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 access, and get started with these four features through Capture Client console.

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

Topics:

- [Deep Visibility](#)
- [Hunter Chrome Extension](#)
- [Network Control](#)
- [Remote Shell](#)
- [Rogues Detection](#)
- [Useful References](#)

Deep Visibility

The Capture Client Deep Visibility Feature powered by SentinelOne, 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

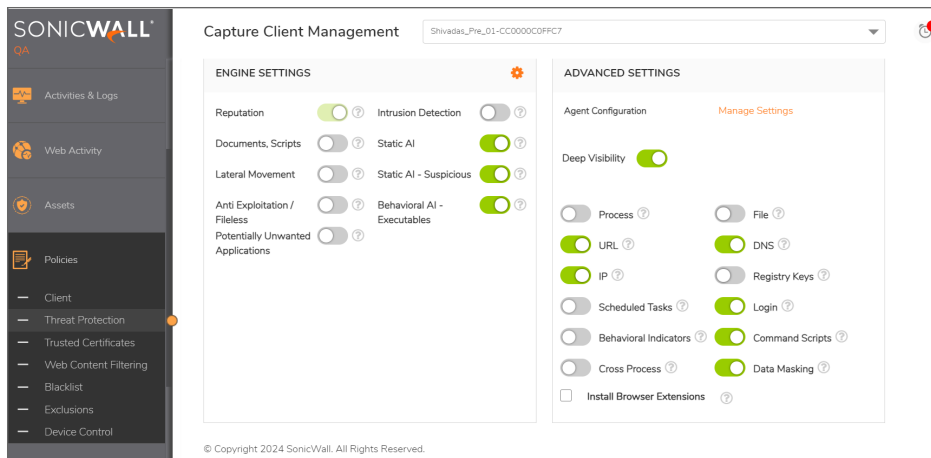
Default data retention period for Premier is 14 days. However, data retention can be extended on a request basis, with additional cost.

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.

- Turn on the option Premier 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.

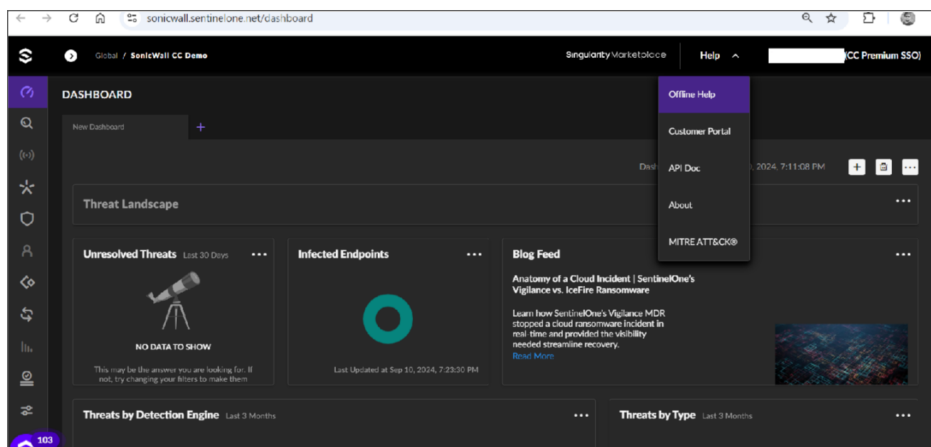
Accessing SentinelOne Help

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

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

To access SentinelOne help:

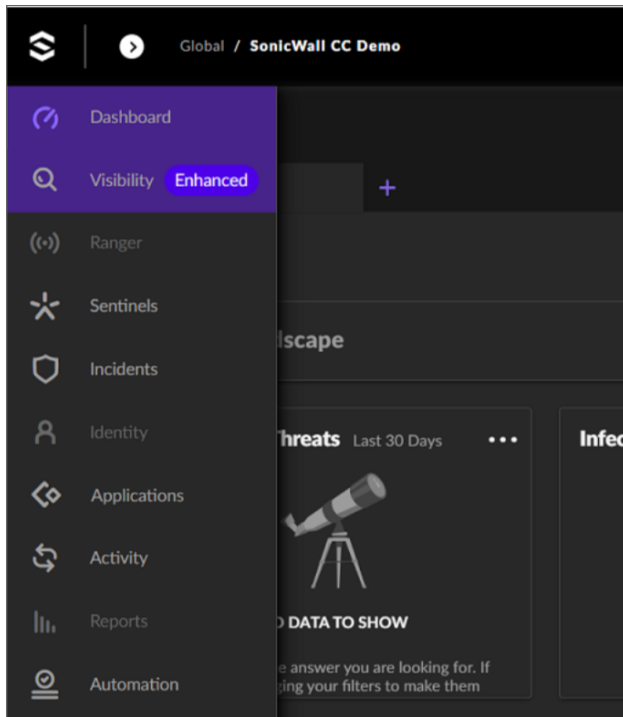
- Click  to access the documentation from SentinelOne console.



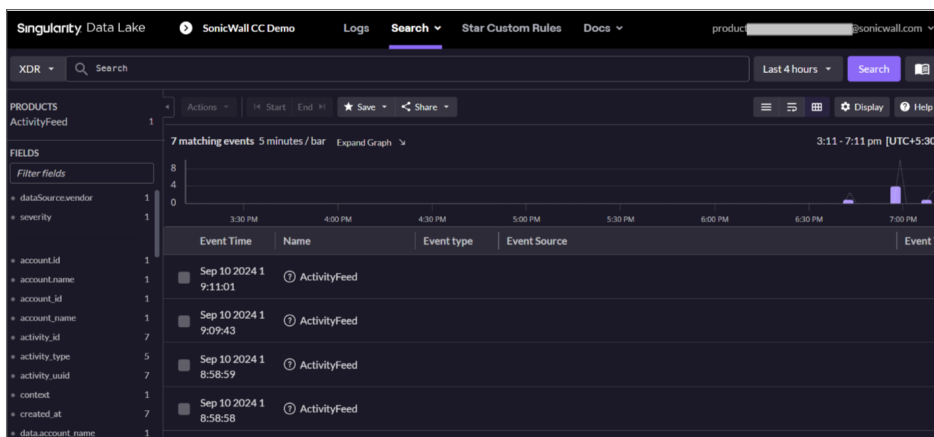
- Click **Help** to view the SentinelOne documentation page.

Finding Threat Hunt Queries in SentinelOne

The SentinelOne console opens when you access the Deep Visibility feature from Capture Client console. Navigate to **Visibility**.



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 [Deep Visibility](#) in SentinelOne help.

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 upto 15 queries in your SentinelOne Premier console page to search for the selected data across your organization.

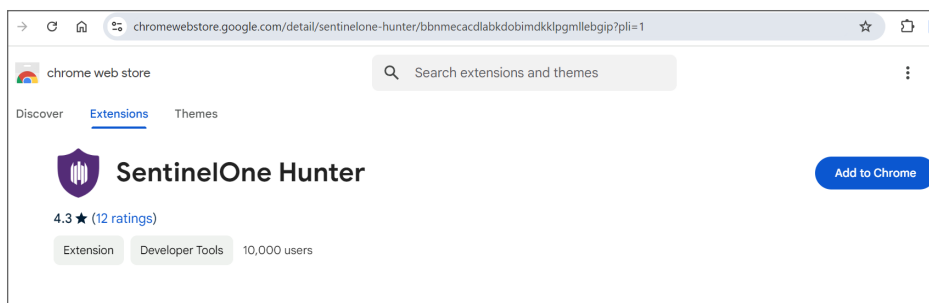
Topics:

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

Installing SentinelOne Hunter Chrome Extension


To install SentinelOne Hunter Chrome Extension:

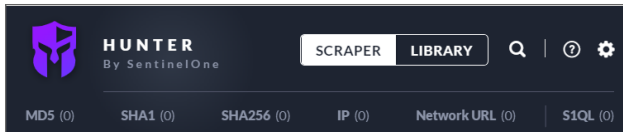
1. Get the Hunter Chrome extension from [Chrome Extension Web Store](#). The SentinelOne Hunter icon shows in your browser extensions.



The SentinelOne Hunter icon shows in your browser extensions. If you do not see the icon, click on **Extensions** to open all extensions.

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 Premier, refer to [Hunter Chrome Extension](#).

SentinelOne Hunter Modes

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

The screenshot shows the SentinelOne Hunter interface in Library mode. The header features the SentinelOne logo, the text "HUNTER By SentinelOne", and two tabs: "SCRAPER" and "LIBRARY". To the right of the tabs are icons for search, help, and settings. Below the header, the text "S1QL (37)" is displayed. The main content area shows a list of queries, each with a checkbox, a title, a description, and a search bar. The first query is "SquirrelWaffle/Qakbot Loader Behavior", the second is "SquirrelWaffle Loader Known Versions", and the third is "Vulnerable Log4j2 versions (CVE-2021-44228)".

S1QL (37) Clear

SquirrelWaffle/Qakbot Loader Behavior

SquirrelWaffle is delivered through a dropper, a malicious Excel or Word document, which contains XLM macros that execute PowerShell to retrieve and launch the SquirrelWaffle loader. This query hunts for the dropper's attempt to do so. As of December 30, 2021, the...

SquirrelWaffle

SquirrelWaffle Loader Known Versions Hunt

Hunt for known file names of the SquirrelWaffle loader. The list is subject to updates as new versions of SquirrelWaffle loaders with other file names are being detected in the wild.

SquirrelWaffle

Vulnerable Log4j2 versions (CVE-2021-44228)

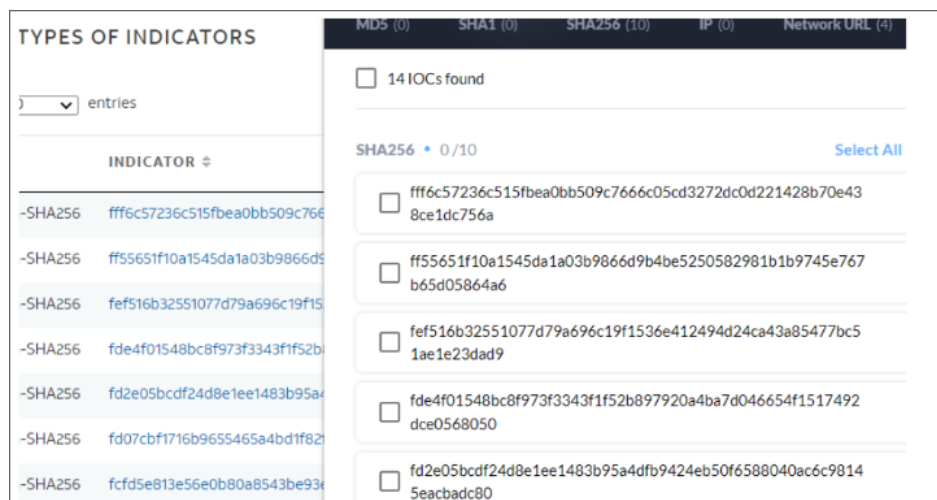
Hunt for known hashes of the vulnerable log4j library. A machine that returns results will likely run an application that is vulnerable (yet, in some cases, the library might not be in use / might run in a non-exploitable context) to CVE-2021-44228. Applications that match this query...

CVE-2021-44228 Log4j2

[1] Applications embedding vulnerable Log4j2 versions (CVE-2021-

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 ([SentinelOne Library Mode](#)) 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 require to access the **Signal Hunting Library** that contains additional threat hunting queries, you need to purchase its subscription license separately.

Network Control

Network Control helps you manage the endpoint firewall settings through Capture Client Management Console (CMC).

Use the **Firewall** tab to define the network traffic to be allowed in and out of endpoints.

Topics:

- [Getting Started with Network Control](#)
- [Configurable Network Quarantine](#)
- [Network Status](#)
- [Network Quarantine Operations](#)

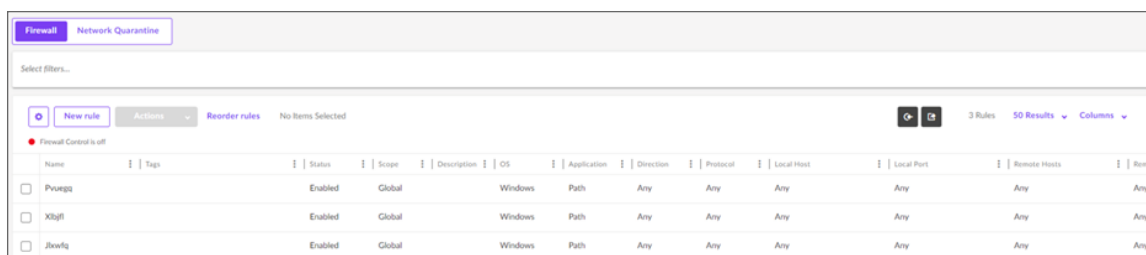
Getting Started with Network Control

To get started with the configuration of Network Control:

1. Navigate to SentinelOne Management console.
2. In the **SENTINELS** toolbar, click on **Network Control**.



The Firewall opens.



① **NOTE:** You can use a single unified rule base for all Operating Systems. Each rule in the rule base can be applied to one or more operating systems.

3. Click on **New Rule**. The **Create New Rule** window opens.



Create New Rule

* Rule Name

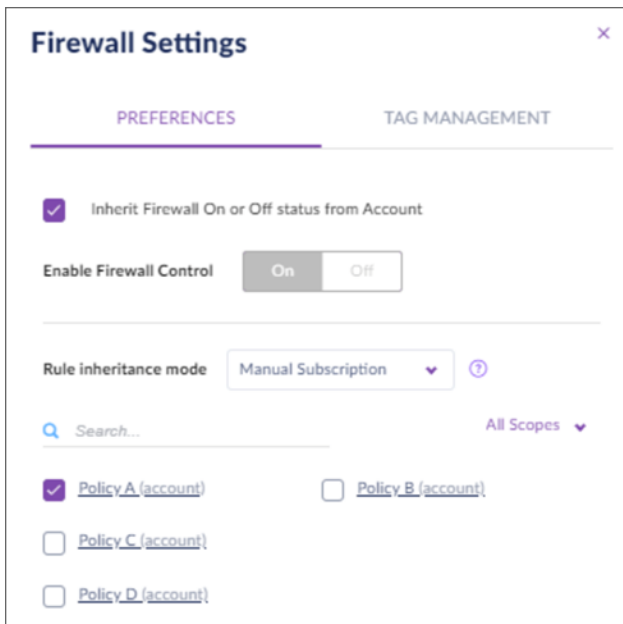
* OS Type

4. Specify the **Rule Name** and **OS Type**.
5. Create **Tags** that represent the Firewall policies.
6. Add **Rules** to the **Tag** (Rules function as a policy - a set of rules in a specific order).

Name	Tags
Block implant	Policy A
Potential CoronaBlue	Policy A
CoronaBlue	Policy A
Test with locations	Policy A Policy B
Investigate RPi	Policy B

7. Manage inheritance with granular inheritance modes.

① **NOTE:** Rules can be fully inherited, not inherited, or inherited based on tags. Firewall On or Off status is separated from rule inheritance.



8. Apply rules based on an endpoint's location. Use the new Description field in rules to add details. If a rule had a "tag" from a version before Liberty, that string is moved to the **Description** field when upgraded to Liberty.

- ① | **IMPORTANT:** There are no default rules. All traffic is allowed if you do not block it explicitly.
- ① | **IMPORTANT:** When SentinelOne Firewall is enabled on Windows endpoints, it becomes the active firewall. SentinelOne Firewall takes the control but it does not change rules from other firewall solutions on the endpoint.

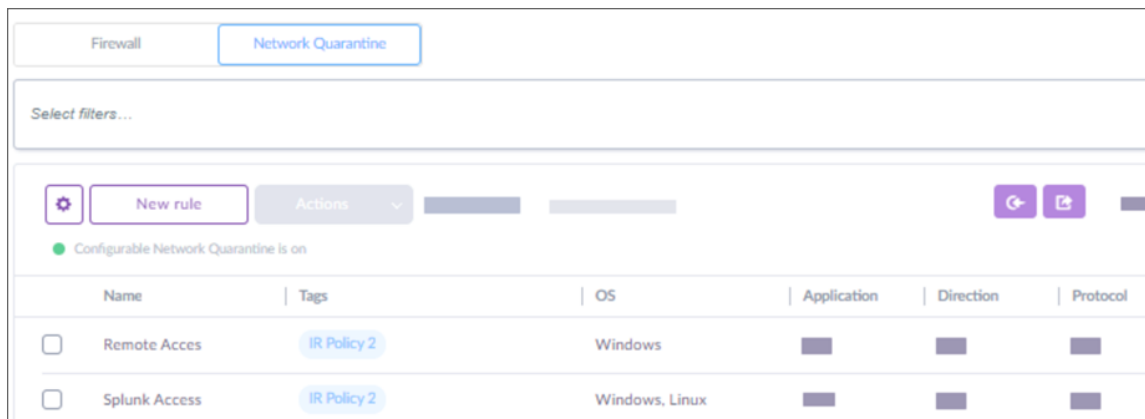
Configurable Network Quarantine

One of the basic mitigation actions for an infected endpoint is to Disconnect it from the Network and put it in **Network Quarantine**. This ensures that a threat cannot attack other endpoints, or communicate with the external network from the infected endpoint.

You can set the automatic **Disconnect from Network** option in the **Policy Settings**. Endpoints are only disconnected if a threat is found, after the threat is executed. Endpoints are not disconnected if a threat is detected pre-execution (by the Reputation or Static AI engines) because the threat is not active.

With **Network Quarantine**, you can configure rules to allow specific network traffic to communicate with quarantined endpoints. By default, only the Agents can communicate with the Management Console if they are disconnected from the network.

For example, allow remote access from specific IP addresses to the infected endpoints to investigate or respond to incidents. Or allow the endpoints to send data to a specific server.



Network Status

Both Firewall and Network Quarantine control the network traffic that goes to and from endpoints. They are operative based on the Network Status of each endpoint.

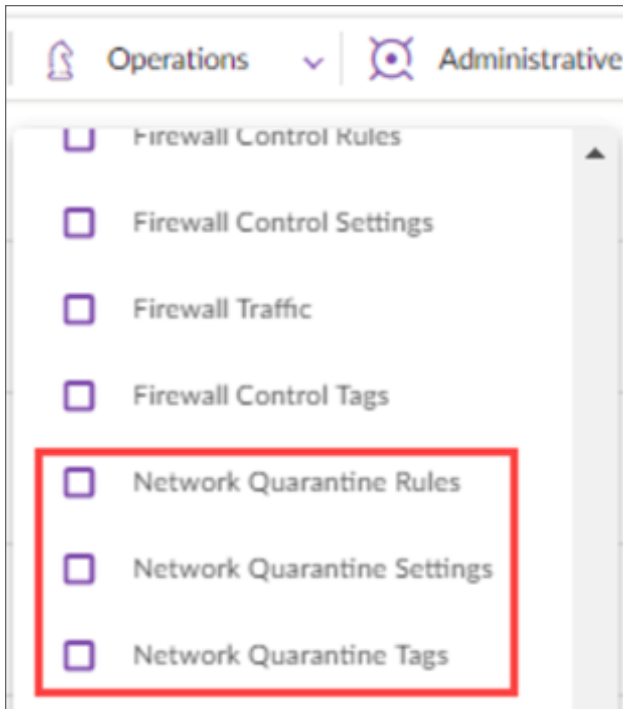


- Network Status - Connected: The endpoint is connected to the network or can connect normally.
- Network Status - Disconnected: The endpoint is disconnected from the network due to mitigation.

Network Quarantine Operations

You can configure the Network Quarantine Information in the Management Console.

1. To see Network Quarantine operations, go to **Activity > Operations**.



2. To enable notifications for Network Quarantine, go to **Notifications > Firewall Control**.

Notification Types	FIREWALL CONTROL NOTIFICATIONS	Email	Syslog
Administrative	Firewall Control Rules	<input type="checkbox"/>	<input type="checkbox"/>
Device Control	Firewall Control Settings	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Control	Firewall Control Tags	<input type="checkbox"/>	<input type="checkbox"/>
Locations	Firewall Traffic	<input type="checkbox"/>	<input type="checkbox"/>
Malware	Network Quarantine Rules	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Mitigation	Network Quarantine Settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Operations	Network Quarantine Tags	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ranger/Rogues			

Remote Shell

Remote Shell helps to remotely perform troubleshooting on the endpoints and supports advanced forensic investigations that can be useful during the incident.

The Remote Shell feature works on Windows, macOS, and Linux without the need for additional third party tools.

Remote Shell feature requires Multi Factor Authentication (MFA) and Only Available on Request.

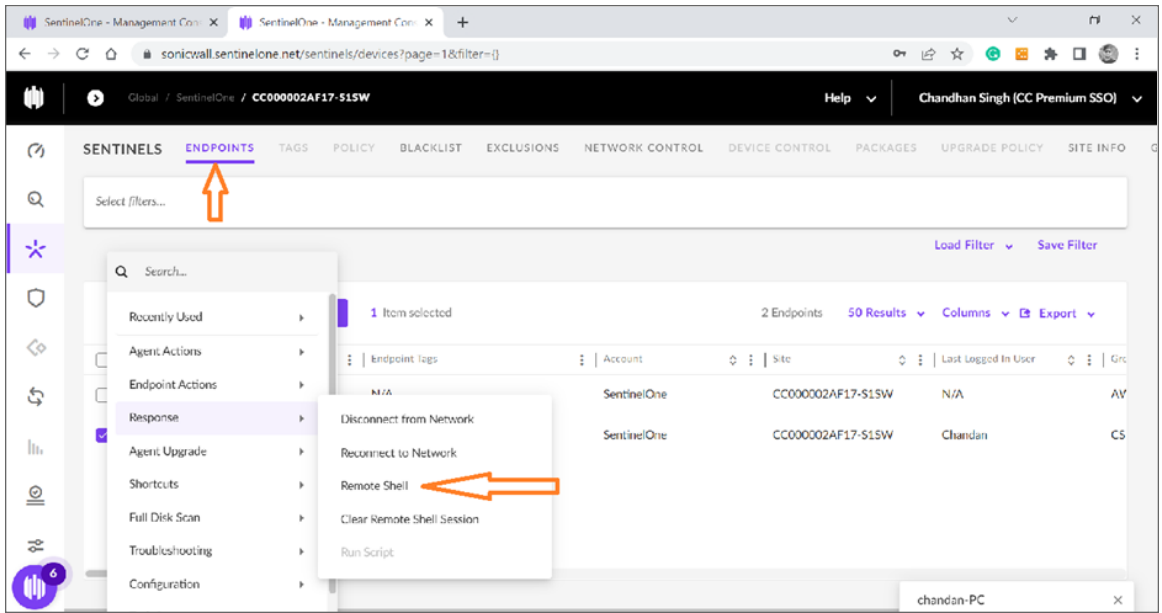
Topics:

- [SentinelOne Remote Shell Use Case 1](#)
- [SentinelOne Remote Shell Use Case 2](#)

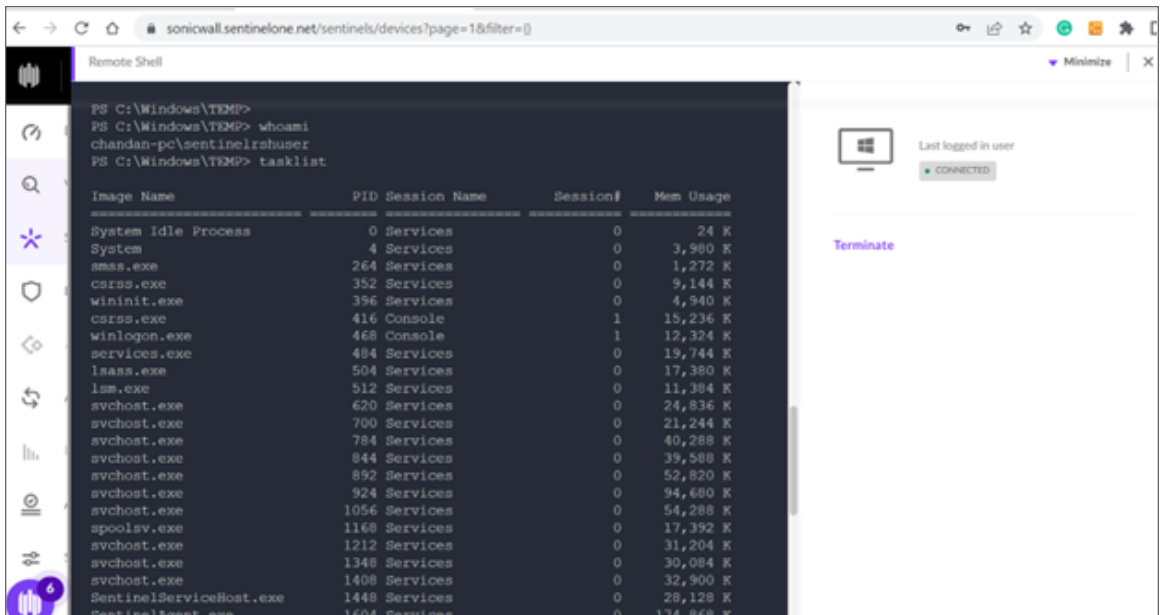
SentinelOne Remote Shell Use Case 1

You can gain the terminal access of the test instance and view the tasklist:

1. On **SentinelOne Tenant**, go to navigate to **Menu > Sentinels** and select the **Endpoints** Tab.
2. Select the Endpoint you want to take remote shell access, and click **Response -> Remote Shell**.



- After you successfully gained terminal access of the test instance (Shared test machine or your individual), type – “tasklist” to see the list of running processes. You can run the other troubleshooting commands.



SentinelOne Remote Shell Use Case 2

1. On endpoint:

Go to start, open run and type - C:\Program Files

Create a notepad file and name it as "calc.exe"

Open CMD prompt and run `REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "calc" /t REG_SZ /F /D "C:\Program Files\calc.exe"`

2. On Remote shell terminal, run

```
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\run\calc" /f
```

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 Premier.

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

① **NOTE:** To access the following links and overall SentinelOne Knowledge base, you will be required to create an account on the portal community.sentinelone.com.

Click on the name to go to the reference:

- [Deep Visibility FAQs](#)
- [Searching for Behavioural Indicators](#)
- [Star Custom Rules](#)
- [Creating Deep Visibility Queries](#)
- [Deep Visibility Query Syntax](#)
- [Managing Deep Visibility Browser Extension](#)
- [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.

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

Capture Client PremierAdministration Guide
Updated - September 2024
232-006172-00-00 Rev A

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