



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.

(i) **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

2

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.

4. Turn on the option Premier in the Advanced Settings.

SONIC WALL	Capture Client Managem	ent Shivadas_Pre,	01-CC0000C0FF	C7	•	(
	ENGINE SETTINGS		٠	ADVANCED SETTINGS		
- Activities & Logs	Reputation 🕜 🕐	Intrusion Detection (0	Agent Configuration	Manage Settings	
Web Activity	Documents, Scripts 🔵 🕐	Static Al	0			
	Lateral Movement 🛛 🗇	Static Al - Suspicious	0	Deep visionity		
Assets	Anti Exploitation / ⑦	Behavioral AI - Executables	0 ?	Process ?	File 🕐	
Delizion	Potentially Unwanted 🔵 📀 Applications				DNS 🕐	
Policies				IP (?)	Registry Keys ?	
- Client				Scheduled Tasks 💿	Login 🕐	
Threat Protection				Behavioral Indicators ③	Command Scripts 💿	
Web Content Filtering				Crass Process (2)	Data Macking (?)	
– Blacklist				Cross Process		
Exclusions				Install Browser Extensions	(3)	
 Device Control 						

(i) **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.

() | 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.

$\leftrightarrow \rightarrow$	C 🛱 Sonicwall.sentinelone.net/dashboard		< ☆ 끄 (◎ :
$\langle 0 \rangle$	Global / SentcWall CC Demo	ngulanty Marketoloce Help	∧ (CC Premium SSO) ∨
	DASHBOARD	Offline Help	
		Customer Porta	a
		Dash API Doc	. 2024, 7:11:08 PM + 😑
	Threatlandscape	About	
Ō	Threat Lanual apu	70000	
	Unresolved Threats List 30 Days ···· Infected Endpoints ··· Blog Feed	MITREATT&C	
	Anatomy of a t Vigilance vs. lo	Cloud Incident SentinelOne's eFire Ransomware	
	Luarn how Sent stopped a cloud	inelOne's Vigilance MDR ransomware incident in we deal the delibility	
	NO DATA TO SHOW Revel down	ovided the visibility ine recovery,	
ୢ	This may be the answer you are looking for. If Last Updated at Sep 10, 2024, 7:23:00 PM not, try changing your filters to make them		
	Threats by Detection Engine Last 3 Months	Threats by Type Last 3	
103			

2. 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.

Singularity. Data Lak	е	>	SonicWall CC D	emo Lo	sgs	Search 🗸	Star Custom	n Rules	Docs v	produc		@sonicwall.e	com ~
XDR - Q Search											Last 4 hours	• Search	
PRODUCTS ActivityFeed						< Share -					= 5 =	🌣 Display	9 Help
FIELDS		7 mai	tching events 5 m	inutes/bar _{Expa}	and Grapt						3	:11 - 7:11 pm (UTC	C+5:30
dataSource.vendor severity	1			4:00 PM			5:00				6:30 PM		
			Event Time	Name		Event	type Ever	nt Source					Event
account.id account.name			Sep 10 2024 1 9:11:01	⑦ ActivityFeed									
account_id account_name activity id			Sep 10 2024 1 9:09:43	⑦ ActivityFeed	đ								
 activity_type activity_uuid 			Sep 10 2024 1 8:58:59	⑦ ActivityFeed	d								
 context created_at 			Sep 10 2024 1 8:58:58	 ActivityFeed 									
ø data.account_name													

For more information on Threat Hunting, refer to Deep Visibility in SentinelOne help.

Hunter Chrome Extension

3

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:

QL (37)				
l ql • 0 /	37			Cle
SquirrelV SquirrelV contains loader. Th Squirre	irrelWaffle/Qakbot Loa Vaffle is delivered through XLM macros that execute his query hunts for the dro IWaffle	der Behavior a a dropper, a malicious E PowerShell to retrieve a opper's attempt to do so.	ixcel or Word docum nd launch the Squirr As of December 30,	eent, which elWaffle 2021, the
Hunt for versions of Squirre	irrelWaffle Loader Know known file names of the So of SquirrelWaffle loaders w IWaffle	wn Versions quirrelWaffle loader. The with other file names are	e list is subject to upo being detected in th	dates as new ne wild.
U Vulr	nerable Log4j2 versions	(CVE-2021-44228)		
Hunt for l run an ap run in a n	known hashes of the vulne plication that is vulnerable on-exploitable context) to	erable log4j library. A ma e (yet, in some cases, the o CVE-2021-44228. Appl	chine that returns re library might not be lications that match	esults will likely in use / might this query

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).

TYPES	OF INDICATORS	MD5 (0) SHA1 (0) SHA256 (10) IP (0) Network URL (4)
) v entries		14 IOCs found
	INDICATOR \$	SHA256 • 0/10 Select All
-SHA256	fff6c57236c515fbea0bb509c766	fff6c57236c515fbea0bb509c7666c05cd3272dc0d221428b70e43 8ce1dc756a
-SHA256	ff55651f10a1545da1a03b9866ds	ff55651f10a1545da1a03b9866d9b4be5250582981b1b9745e767
-SHA256	fef516b32551077d79a696c19f15	b65d05864a6
-SHA256	fde4f01548bc8f973f3343f1f52b	fef516b32551077d79a696c19f1536e412494d24ca43a85477bc5 1ae1e23dad9
-SHA256	fd2e05bcdf24d8e1ee1483b95a4	fde4f01548bc8f973f3343f1f52b897920a4ba7d046654f1517492
-SHA256	fd07cbf1716b9655465a4bd1f82	L dce0568050
-SHA256	fcfd5e813e56e0b80a8543be93e	Gd2e05bcdf24d8e1ee1483b95a4dfb9424eb50f6588040ac6c9814 5eacbadc80

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.

(i) **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.

SENTINELS	ENDPOINTS	TAGS	NETWORK ROGUES	CLOUD ROGUES	POLICY	STAR CUSTOM RULES	BLOCKLIST	EXCLUSIONS	NETWORK CONTROL
Firewall	Network Quara	ntine							

The Firewall opens.

Fi	rewall Network	Quarantine										
Sele	ect filters											
	New rule Frewall Control is off	Actions - Reorder rules	No Items Selected							e ا	3 Rules 50 Results 🗸	Columns 👻
	Name	I Tags	E Status	Scope	I Description I OS	Application	Direction	Protocol	E Local Host	E Local Port	E Remote Hosts	Rem
	Pvuegq		Enabled	Global	Windows	Path	Any	Any	Any	Any	Any	Any
	Xibjfl		Enabled	Global	Windows	Path	Any	Any	Any	Any	Any	Any
	Jbowfq		Enabled	Global	Windows	Path	Any	Any	Any	Λαγ	Any	Any

- (i) **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	New Rule in Liberty							
* OS Type	Windows, MacOS, Linux	•						

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

Firewall Setting	gs		×
PREFERENCE	S	TAG MAI	NAGEMENT
Inherit Firewall On Enable Firewall Control	or Off status	from Account	
Rule inheritance mode	Manual Sub	scription 🗸	0
Q Search			All Scopes 🖌
Policy A (account)	(Policy B (acco	ount)
Policy C (account)			
Policy D (account)			

- 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.
- (i) | IMPORTANT: There are no default rules. All traffic is allowed if you do not block it explicitly.
- (i) **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 Al 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.

	Firewall	Network Quarantine				
Select f	filters					
¢ • •	New rule	Actions ~			G	
	Name	Tags	OS	Application	Direction	Protocol
	Remote Acces	IR Policy 2	Windows	-	-	-
	Splunk Access	IR Policy 2	Windows, Linux	-	-	-

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.

Threat Actions 🗸 Network Quarantine 🛧 Analyst Verdict 🗸		
0	Status The	Connect To Network
0	Sarus III	
	C) cur	Disconnect From Network

- 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	0			
Device Control	Firewall Control Settings	0			
Firewall Control	Firewall Control Tags	0			
Locations	Firewall Traffic	0			
Maiware	Network Quarantine Rules	0			
Operations	Network Quarantine Settings	0			
Ranger/Rogues	Network Quarantine Tags	0			
Mitigation Operations Ranger/Rogues	Network Quarantine Rules Network Quarantine Settings Network Quarantine Tags				

Remote Shell

5

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**.

🗰 SentinelOne - Management Coni X 👔 SentinelOne - Management Coni X 🕂									\sim		ы	×	
$\leftarrow \ \rightarrow$	← → C △ a sonicwall.sentinelone.net/sentinels/devices?page=18dfilter={}							07	ዸ ☆	@	*	•	:
•	ø	Global / SentinelOne / Co	C000002AF	17-515W			Help	~	Chandhan	Singh (CC	Premiu	um SSO)	*
0	SEN		TAGS	POLICY BLACKLIST	EXCLUSIONS	NETWORK CONTROL	DEVICE CONTROL PA	CKAGES	UPGR/	DE POLI	CY S	SITE INFO	o g
Q	Sei	ect filters											
*		Q Search							Load Fil	ter 🗸	Save F	Filter	
Ø		Recently Used	•	1 Item selected			2 Endpoints 50 F	Results	✓ Colum	ns 🗸 🖻	Expor	t 🗸	
<>	C	Agent Actions	+	Endpoint Tags		Account	≎ 🕴 Site	0	Last Log	gged In Use	r ç	: 0	rç
5	C	Endpoint Actions	+	N/A		SentinelOne	CC000002AF17-S	15W	N/A			A	v
~		Response	+	Disconnect from Network		SantinalOna	CC0000024E17-S	1514/	Chandan			~	c
lu.		Agent Upgrade	+	Reconnect to Network		Sentimerone	CC00002AF17-5	1344	Chanta			C	5
Ø		Shortcuts		Remote Shell									
_		Full Disk Scan		Clear Remote Shell Session									
\$8		Troubleshooting		Run Script									
	-	Configuration	•		_				chandan-P	с		>	c

3. 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.

← →	C 🛆 🔒 sonicwall.sentinelone.ne	et/sentinels/de	vices?page=1&filter-	0				0	*	
(l)	Remote Shell							▼ Minim	ize	>
0	PS C:\Windows\TEMP> PS C:\Windows\TEMP> whoami chandan-pc\sentinelrshuser PS C:\Windows\TEMP> taskli						Last logged in user			
0	Image Name		ession Name	Session#	Mem Usage	_	• COMMENTO			
*	System Idle Process	0.8	ervices	0	24 K	Terminate				
~	System	4 8	ervices		3,980 K	reminance				
	smss.exe	264 3	ervices		1,272 K					
5 1	csrss.exe	302 8	ervices		9,199 K					
-	wininit.exe	370 8	MEVICES		4,340 K					
	viploren eve	410 0	ionsole		10,230 h					
(a)	services exe	484 0	lonsore		19 744 8					
	lsass.eve	504 8	arvices		17.380 K					
	lem.exe	512 8	arvices		11.384 K					
5 /	sychost eve	620 8	lervices		24.836 K					
	sychost.exe	700 5	ervices		21.244 K					
	sychost.exe	784 5	lervices		40,288 K					
h. 1	sychost.exe	844 \$	ervices		39,588 K					
	sychost.exe	892 8	ervices		52,820 K					
~	sychost.exe	924 8	ervices		94,680 K					
<u> </u>	sychost.exe	1056 8	ervices		54,288 K					
	spoolsv.exe	1168 \$	ervices		17,392 K					
	sychost.exe	1212 8	ervices		31,204 K					
2	sychost.exe	1348 \$	ervices		30,084 K					
-	sychost.exe	1408 s	ervices		32,900 K					
~	SentinelServiceHost.exe	1448 \$	ervices		28,128 K					
140 M	SentinelAcent eve	1604 9	terri cer		174.868 8					

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

6

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.

7

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.

(i) **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