



Capture Client

Monitoring with Dashboard,  
Threats and Applications

Administration Guide

SONICWALL<sup>®</sup>

# Contents

<b>Overview</b>	<b>4</b>
Description	4
Navigation	5
Guide Conventions	7
<b>Dashboard</b>	<b>8</b>
About the Dashboard	8
Global Dashboard	9
Tenant Dashboard	10
<b>Alerts and Notifications</b>	<b>11</b>
Accessing Notifications	11
Viewing Alerts	12
<b>Threat Investigation</b>	<b>15</b>
Investigating Threats	15
Analyst Verdict	20
Downloading a Threat File	21
Detected Threats	21
Threats Mitigated	23
Performing a Rollback	23
Resolving Threats	24
Blacklisting Threats	24
Benign Threats	25
<b>Investigating and Responding to Active Clients</b>	<b>26</b>
View Clients	26
Monitoring and Managing the State of Devices	28
Reviewing Processes Running on a Device	30
Reviewing Policies Enforced on a Device	31
SentinelOne Pending Actions	31
<b>Investigating and Responding to Active Users</b>	<b>32</b>
<b>Enforce Trusted Certificates</b>	<b>33</b>
<b>Investigating and Responding to Risky Applications</b>	<b>35</b>

**SonicWall Support** ..... **39**  
About This Document ..... 40

# Overview

SonicWall® Capture Client provides a framework for managing and enforcing policy across endpoints in your IT infrastructure. It shows you the level of coverage you have and the gaps that need to be plugged.

This section provides general information about Capture Client and includes the following:

- [Description](#)
- [Navigation](#)
- [Guide Conventions](#)

## Description

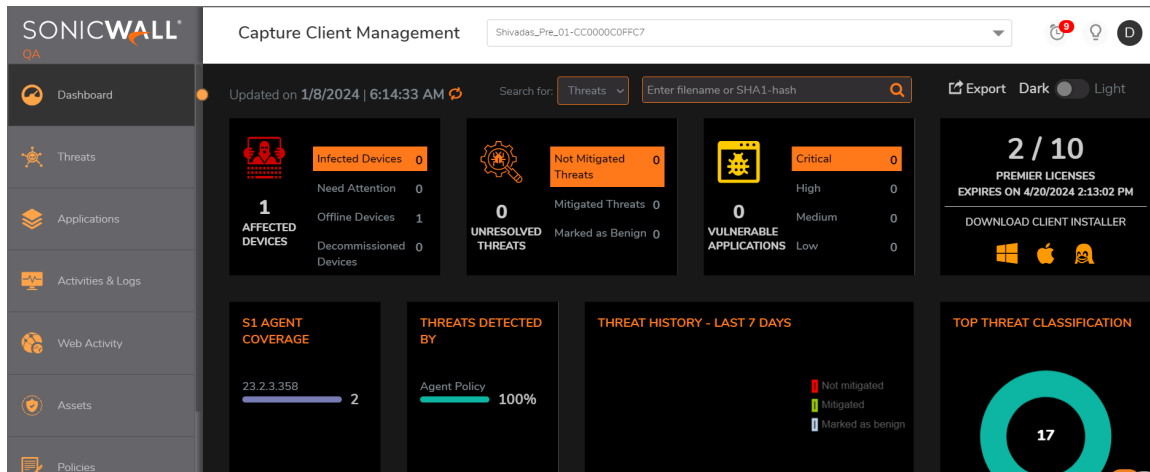
SonicWall Capture Client is a client offering that delivers multiple client protection capabilities. With a next-generation malware protection engine powered by SentinelOne, the SonicWall Capture Client delivers advanced threat protection with these key features:

- **Continuous behavioral monitoring** of the client that helps create a complete profile of file activity, application & process activity, and network activity. This protects against both file-based and fileless malware and delivers a 360° attack view with actionable intelligence relevant for investigations.
- **Multiple layered signatureless techniques** include techniques for protecting cloud intelligence, advanced static analysis and dynamic behavioral protection. They help protect against and remediate well known, little known, and even unknown malware, without regular scans or periodic updates. This maintains the highest level of protection at all times, without hampering user productivity.
- **Unique roll-back capabilities** support policies that not only remove the threat completely but also restore a targeted client to its original state, before the malware activity started. This removes the effort of manual restoration in the case of ransomware and similar attacks.
- **Cloud-based management console** reduces the footprint and overhead of management. It improves the deployability and enforceability of Endpoint Protection, irrespective of where the endpoint is.

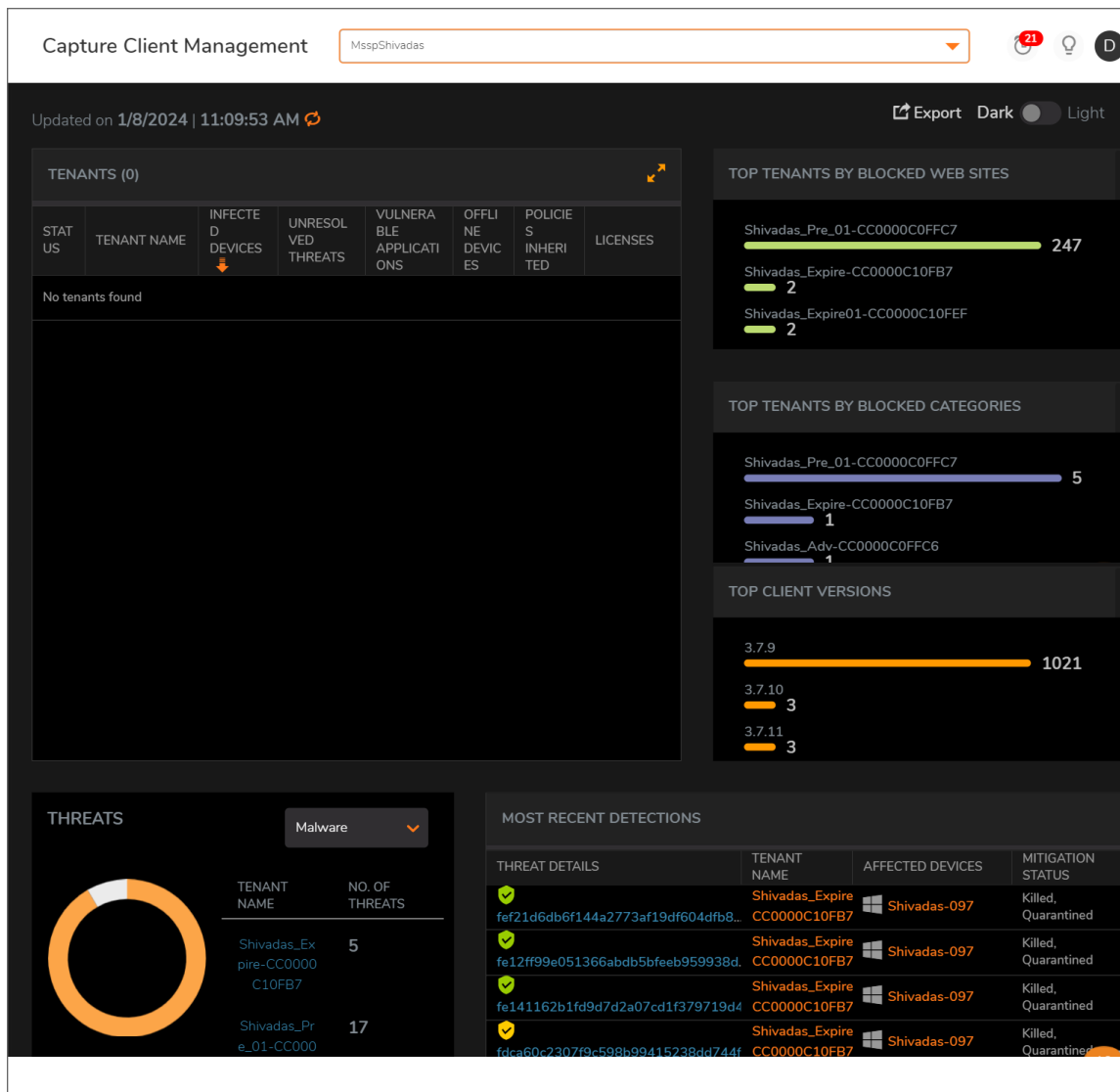
The size of your Capture Client tenancy is only limited by the number of endpoint licenses procured.

# Navigation

When logging in to Capture Client for the first time, the Dashboard is the default view. If one of your tenants is selected, you can get a quick summary of the number of affected devices, active threats and critical issues. You can also see a series of tiles showing the top items in each category.

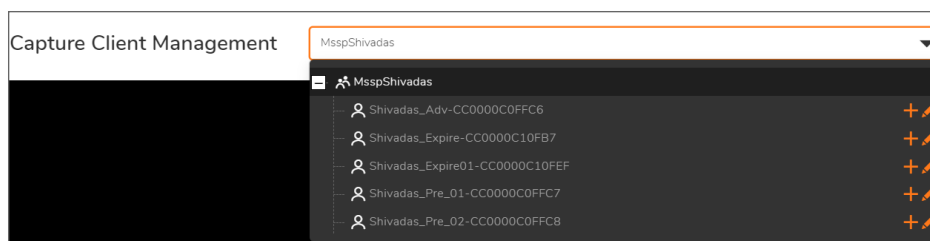


If the account is selected, the Dashboard information is summarized by tenants.



### To change to the account/tenant option:

1. Click the drop-down list, next to **Capture Client Management**, at the top of the page.



2. Select the account or tenant view that you want.

# Guide Conventions

The following conventions are used in this guide:

Convention	Use
<b>Bold Text</b>	Used in procedures to identify elements in the user interface like dialog boxes, windows, screen names, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
<b>Menu divider   Menu item &gt; Menu item</b>	Indicates a multiple step menu choice on the user interface. For example, System Setup   Users, Groups & Organizations > Users means find the menu or section divider System Setup first, select Users, Groups & Organizations, and then select Users.
<code>Computer code</code>	Indicates sample code or text to be typed at a command line.
<code>&lt;Computer code italic&gt;</code>	Represents a variable name when used in command line instructions within the angle brackets. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number>, replace the variable and brackets with the serial number from your device: serialnumber=C0AEA0000011.
<i>Italic</i>	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

# Dashboard

The well-designed Dashboard that Capture Client offers helps to monitor the performance metrics efficiently including the tenants, top tenants blocked web request, and so on. This section describes the following topics.

## Topics:

- [About the Dashboard](#)
- [Global Dashboard](#)
- [Tenant Dashboard](#)

## About the Dashboard





The Dashboard menu page is the landing page for the console and also the first place to monitor for alerts and threats.

Capture Client offers two different views:

- [Global Dashboard](#)
- [Tenant Dashboard](#)

When you log in for the first time, Global Dashboard is displayed. If you need to view the Tenant Dashboard, select the tenant from the drop-down list. For more information, see [Navigation](#).

The other options available in a dashboard include:

- Theme: Click  to select the Dark or the Light theme for your dashboard.
- Export: Click  to export the dashboard details to PDF format
- Help: Click  to view the online help for Capture Client.
- Notifications: Click  to view the notification center. For more details, see [Accessing Notifications](#).

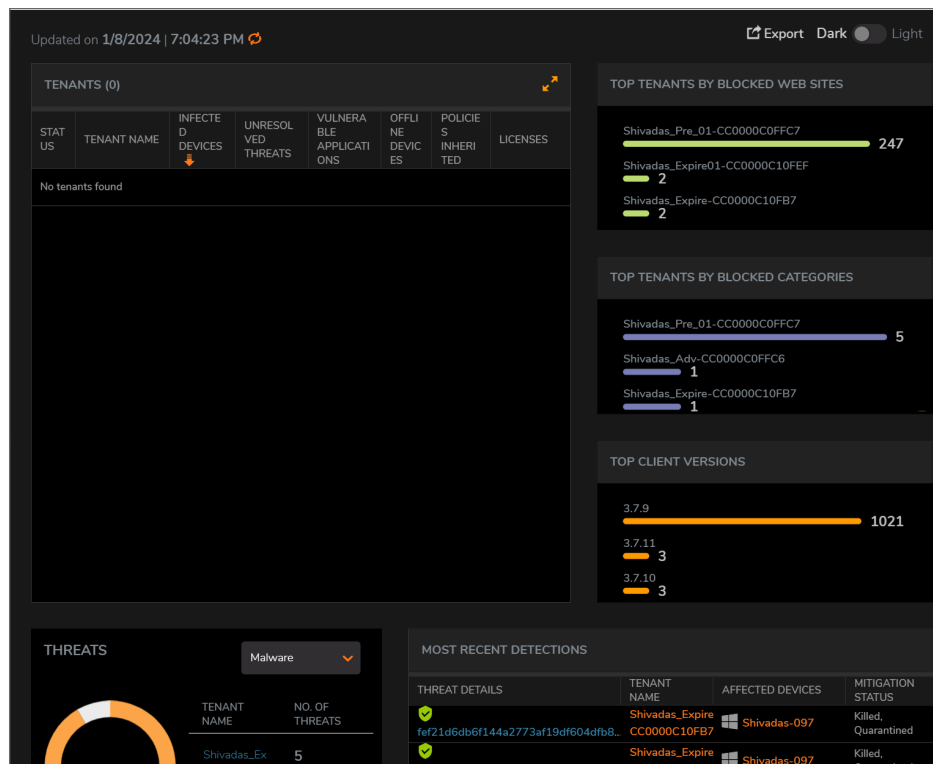


# Global Dashboard

The Global Dashboard shows you the details of critical information in the tiles given below:

- **Tenants:** This tile displays the names of tenants, Status, Infected Devices, Unresolved Threats, Vulnerable Applications, Offline Devices, Policies Inherited, and Licenses. Click on the name of tenant to navigate to the Tenant Dashboard. Click on the **Edit** option for any tenant to navigate to the **Tenants Settings** page to configure the settings for the respective tenant.
- Top Tenants by Blocked Websites
- Top Tenants by Blocked Categories
- Top Client Versions
- **Threats:** This tile displays the Tenant Names and the number of threats. You can filter the details by selecting the commands from the drop-down Click on the tenant name to navigate to the **Threats** page.
- **Most Recent Detections:** This tile displays the File ID of recent detections, Mitigation Status, Tenant Name, and the details of the Affected Devices. Click on the File ID to navigate to the **Threat Group** and **Threat Details**.

You can search for Threats and Devices, and further filter the data as required. You can also search by the file name for easy results.

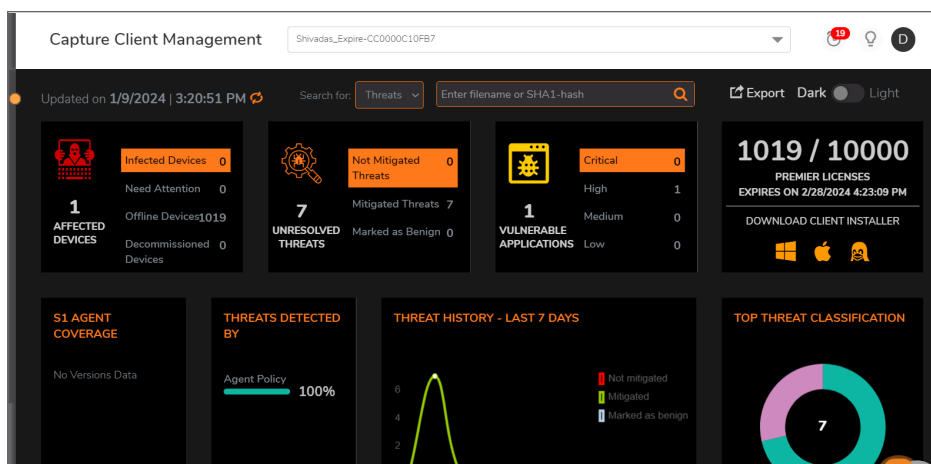


# Tenant Dashboard

The Tenant Dashboard shows you the details given below:

- **Affected Devices:** Displays the number of **Infected Devices**, **Need Attention**, **Offline Devices**, and **Decommissioned Devices**. Click on the respective link to navigate to the **Devices** page.
- **Unresolved Threats:** Displays the number of **Not Mitigated Threats**, **Mitigated Threats**, and **Marked as Benign**. Click on the respective link to navigate to the **Threats** page.
- **Vulnerable Applications:** Displays the **Critical**, **High**, **Medium**, and **Low** links to navigate to the **Applications** page.
- **Number of Licenses:** Displays the License Expiry date and the options to download the installer for different operating systems including Windows, macOS, and Linux.
- **S1 Agent Coverage:** Displays the details of SentinelOne agent coverage.
- **Threats Detected By:** Displays the details of the threats detected by Agent Policy and Full Disk Scan. Click on the type of command to navigate to the **Threats** page.
- **Threat History:** Displays the Threat History details of last 7 days including the threats not mitigated, mitigated, and marked as benign.
- **Top Threat Classification:** Displays the type of threats to navigate to the **Threats** page. Click on the link to navigate to the **Threats** page.
- **CC Agent Coverage:** Displays the Capture Client versions and the number of devices installed with these versions. Click on the link to navigate to the **Devices** page
- **Top Blocked Categories:** Displays the link to navigate to the **Web Activity** page.
- **Top Blocked Domains:** Displays the top blocked domain link to navigate to the **Web Activity** page.
- **Top Blocked Users:** Displays the user name to navigate to the **Users** page.

You can search for Threats and Devices, and further filter the data as required. You can also search by the file name for easy results.



# Alerts and Notifications


The Notifications feature allows administrators and users to see the status of any threats, events, or alerts and to set the rules for the kinds of notifications associated with these activities.

## Topics:

- [Accessing Notifications](#)
- [Viewing Alerts](#)

## Accessing Notifications

When you first log into the Capture Client, you can quickly see the number of notifications that are pending with some kind of acknowledgment.

Click  in the upper-right corner, to open the Notification Center.

NOTIFICATION CENTER

NEW

!

Suspicious activity detected: Malware-Mitigated(Cloud)

Suspicious Activity Detected

6 days ago

!

Suspicious activity detected: Trojan-Mitigated(Cloud)

Suspicious Activity Detected

6 days ago

!

Threat event remediated: Trojan-Mitigated(Cloud)

Threat Killed and Quarantined/Remediated

6 days ago

!

Threat event remediated: Malware-Mitigated(Cloud)

Threat Killed and Quarantined/Remediated

6 days ago

!

Threat event remediated: Malware-Mitigated(Cloud)

Threat Killed and Quarantined/Remediated

6 days ago

!

Threat event remediated: Malware-Mitigated(Cloud)

Threat Killed and Quarantined/Remediated

6 days ago

10

See all alerts

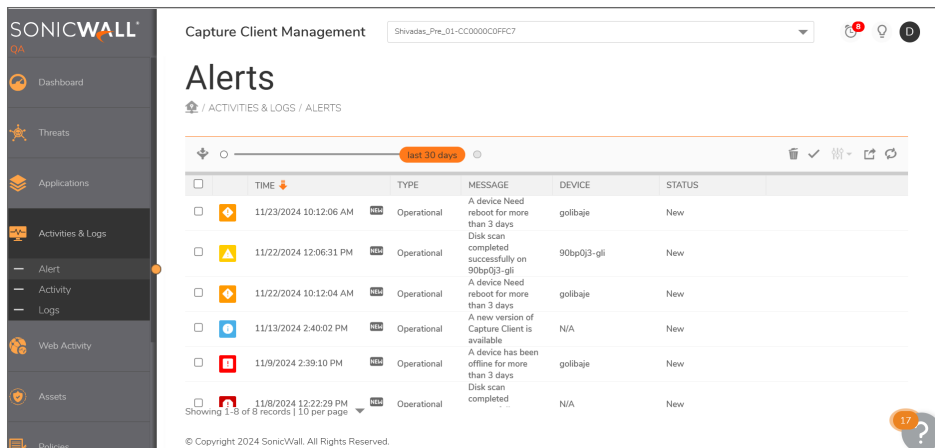
?

You can acknowledge or delete the notifications hovering the mouse to the icons on the right side of each notification.

Click **See all alerts** to view a full list of notifications. This is same as navigating to **ACTIVITIES & LOGS > Alerts**.

## Viewing Alerts

All alerts are listed in a table at **ACTIVITIES & LOGS > Alerts**. The table lists the alert severity, time it was detected, type of issue, message, and status. Once you mouse over a particular alert, you also have the options to **Mark it as read** or **Delete**.






The table below shows the level of severity an event is assigned by default. This is based on the category the event belongs to.

Type	Category/Description	Severity
Threat	Threat Detected	High
	Threat Killed and Quarantined/Remediated	Major
	Suspicious Activity Detected	High
	Suspicious Activity K&Q/Remediated	Major
Operational	Infected Device	Major
	Device is offline for more than 8 days	High
	Scan Started	Minor
	Scan Completed Successfully	Minor
	Scan Completed with Errors	Major
	Other Device Event	Low
	License Expiring Soon	Major
	License Expired	High
	Global Notification	Info
	Planned Maintenance	Low
	New Version Available	Info
	Incompatible versions	Major
	End of Support	High
	Invalid Release	High
	Other Console Event	Minor
	Found Application Vulnerability	High
	Report Ready to Download	Info

To refine your search for specific issues, click on the **Filter** icon. It expands and you can select a combination of parameters to filter against.

SEVERITY	TYPE	STATUS	CATEGORY
<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Threat	<input checked="" type="checkbox"/> New	<input checked="" type="checkbox"/> Threat Detected
<input checked="" type="checkbox"/> High	<input checked="" type="checkbox"/> Operational	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Threat Killed and Quarantined/Remediated
<input checked="" type="checkbox"/> Major			<input checked="" type="checkbox"/> Suspicious Activity Detected
<input checked="" type="checkbox"/> Minor			<input checked="" type="checkbox"/> Suspicious Activity K&Q/Remediated
<input checked="" type="checkbox"/> Low			<input checked="" type="checkbox"/> Infected Device
			<input checked="" type="checkbox"/> Threat on Multiple Devices
			<input checked="" type="checkbox"/> Application Vulnerabilities

You also have the options to:

- Mark the alerts: Select the alert and click  ▼ to categorize the alert as **Mark as New**, **Mark as Read**, or **Delete** it.
- Export as CSV: Click  to export and download the alerts to CSV file.
- Refresh data: Click  to refresh data.

# Threat Investigation

You can use Capture Client to reduce the effort when analyzing and responding to active threats. You can navigate to the list of threats by clicking **Threats**.

The Threat lifecycle in the Capture Client Management Console is designed to give you visibility and control. A threat is generated when the agent detects suspicious or malicious activity on the endpoint. The Agent can detect only, or also mitigate threats automatically, based on the Threat Protection Policy settings.

## Topics:

- [Investigating Threats](#)
- [Analyst Verdict](#)
- [Downloading a Threat File](#)
- [Detected Threats](#)
- [Threats Mitigated](#)
- [Performing a Rollback](#)
- [Resolving Threats](#)
- [Blacklisting Threats](#)
- [Benign Threats](#)

## Investigating Threats

You can navigate to the list of threats by clicking **Threats**. The **Threats** page shows all the threats detected in the reverse chronological order with the latest detection at the top of the first page.

Capture Client Management

Shivadas\_Expire-CC0000C10FB7

# Threats

/ THREATS

Threats

last month

Custom

	REPORTED TIME	THREAT DETAILS	DEVICE	CLASSIFICATION	AI CONFIDENC...	INCIDENT S
<input type="checkbox"/>	1/3/2024 11:23:31 AM	fe21d6db6f144a2773af19df604df...	Shivadas-097	Trojan	Malicious	Unresolved
<input type="checkbox"/>	1/3/2024 11:23:21 AM	fe12ff99e051366abdb5bfeeb9599...	Shivadas-097	Malware	Malicious	Unresolved
<input type="checkbox"/>	1/3/2024 11:23:20 AM	fe141162b1fd9d7d2a07cd1f37971...	Shivadas-097	Malware	Malicious	Unresolved
<input type="checkbox"/>	1/3/2024 11:23:20 AM	fdca60c2307f9c598b99415238dd...	Shivadas-097	Malware	Suspicious	Unresolved
<input type="checkbox"/>	1/3/2024 11:23:19 AM	fe2fab6a0eb675ad7ef702044ea0c...	Shivadas-097	Trojan	Suspicious	Unresolved
<input type="checkbox"/>	1/3/2024 11:23:18 AM	fc3a0143eb8a6440b09d795ad0f4...	Shivadas-097	Malware	Malicious	Unresolved

Showing 1-7 of 7 records | 10 per page

10

© Copyright 2023 SonicWall. All Rights Reserved.

You can view the status of the threat displayed in the tabular view. The colors of the icons (green, red and gray) represent different stages of the threat:

Icon	Meaning
	A mitigated or resolved threat.
	A threat is currently unresolved or suspicious.
	A threat has been detected and blocked.

### Filter Options

Click and select the check the boxes for the **Mitigation Status**, **Classification**, **Incident Status**, **AI Confidence Level**, **Analyst Verdict**, **Reboot Required**, **OS**, **Threats Detected By** options to filter on.

/ THREATS

all

Custom

MITIGATION STATUS	CLASSIFICATION	INCIDENT STATUS	AI CONFIDENCE LEVEL	ANALYST VERDICT
<input type="checkbox"/> Not Mitigated 6	<input type="checkbox"/> Benign 0	<input type="checkbox"/> Resolved 43	<input type="checkbox"/> Malicious 46	<input type="checkbox"/> True Positive 31
<input type="checkbox"/> Mitigated 34	<input type="checkbox"/> Cryptominer 0	<input type="checkbox"/> Unresolved 3	<input type="checkbox"/> Suspicious 0	<input type="checkbox"/> Suspicious 0
<input type="checkbox"/> Marked as Benign 6	<input type="checkbox"/> Ransomware 0	<input type="checkbox"/> In Progress 0	<input type="checkbox"/> N/A 0	<input type="checkbox"/> False Positive 6
	<input type="checkbox"/> Malware 13			<input type="checkbox"/> Undefined 9
	<input type="checkbox"/> Trojan 27			
	<input type="checkbox"/> Virus 0			
	<input type="checkbox"/> Exploit 0			





- Use **Mitigation Status** to filter the threats based on the options Not Mitigated, Mitigated, and Marked as Benign.



- Use **Classification** to filter the threats based on the software.
- Use **Incident Status** to filter the threats based on the options Resolved, Unresolved, and In Progress.
- Use **AI Confidence Level** to filter the threats based on the options Malicious, Suspicious, and N/A.  
 ⓘ | **NOTE:** The users cannot change the AI Confidence Level that is generated by AI.
- Use the **Analyst Verdict** options to investigate more on the threats and reach a conclusion on them. For more details, see [Analyst Verdict](#).
- To find threats that require a reboot to complete mitigation, use the **Reboot Required** filter options Yes or No.  
 ⓘ | **NOTE:** Certain mitigation actions (for example, the deletion of corrupted system files) may not be able to complete due to permission or OS deadlocks. In such situations, a reboot may be required to complete the action and this is indicated on the management console.
- Use the **OS** options to filter by the Operating System.
- Use the **Threats Detected By** options to filter the threats based on the options Full Disk Scan, Agent Policy, Local Agent Command, Deep Visibility Command, Management Console API, and On-Demand Scan.


## Other Options

At the top of the page, you also have the following options to:

- Search: Click  and enter the file details in the search string.
- Detailed view: Click  to expand the options in the table. Click it again to return to the simple view.
- Time Filters: Move the orange cursor and select the required time anywhere from **Last 5 Minutes** to **All**. You can also click **Custom** and select the start date and end date.
- Export: Click  to export the threat list in CSV format
- Taking appropriate actions for threats: Select the threats from the list and click  to take appropriate actions. You can take any of the following:
  - Kill Threat
  - Unquarantine
  - Quarantine
  - Connect Network
  - Disconnect Network
  - Mark as Threat
  - Add to Blacklist
  - Add to Exclusions

- Analyst Verdict
- Mark as Unresolved
- Mark as Resolved
- Mark as In Progress
- Mark as Benign

① | **NOTE:** These options are displayed depending upon the status of the threat.








① | **NOTE:** To take action for single threat items, you can also click  pertaining to each threat to view the options.

Double-click on any of the File Details, Device, Classification, or Mitigation actions to view the detailed information on the **Threat List** page.

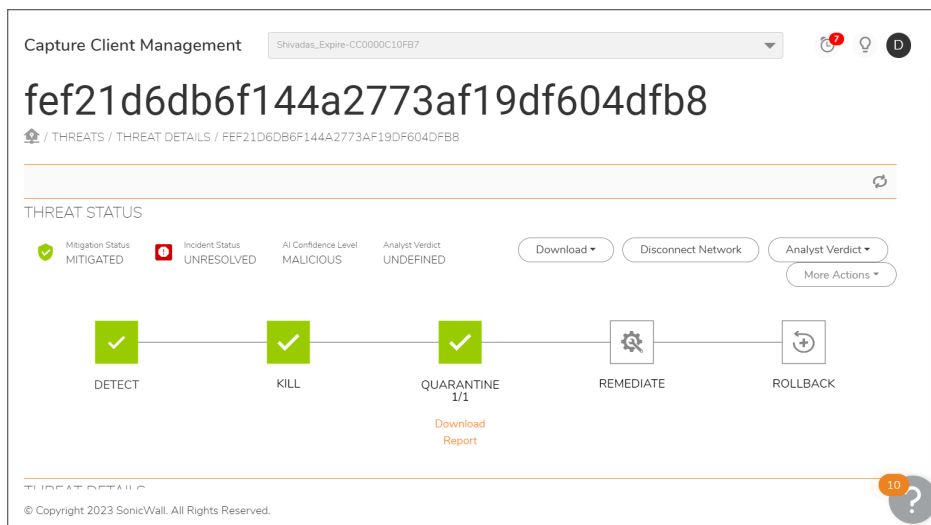
Capture Client Management Tenant2-CC0000AA0417 94 SK

## Threat List for fe2fab6a0eb675ad7ef702044e...

🏠 / THREATS / THREAT LIST / FE2FAB6A0EB675AD7EF702044EA0CA07.EXE

REPORTED TIME	THREAT DETAILS	DEVICE	ACTIONS
6/21/2021 2:49:47 PM	 fe2fab6a0eb675ad7ef702044ea0ca07.exe	Win10-64bit-Sangeeta	
6/21/2021 2:42:10 PM	 fe2fab6a0eb675ad7ef702044ea0ca07.exe	Win10-64bit-Sangeeta	
3/31/2021 6:41:40 PM	 fe2fab6a0eb675ad7ef702044ea0ca07	Win10-Malware	Killed, Quarantined
3/31/2021 6:41:30 PM	 fe2fab6a0eb675ad7ef702044ea0ca07	Win10-Malware	Killed, Quarantined
3/31/2021 6:40:41 PM	 fe2fab6a0eb675ad7ef702044ea0ca07	Win10-Malware	Killed, Quarantined
3/31/2021 5:03:47 PM	 fe2fab6a0eb675ad7ef702044ea0ca07	Win10-Malware	Killed, Quarantined
3/31/2021 5:03:47 PM	 fe2fab6a0eb675ad7ef702044ea0ca07	Win10-Malware	Killed, Quarantined

On the Threat List page, double click on the threat again to view the **Threat Details** page.



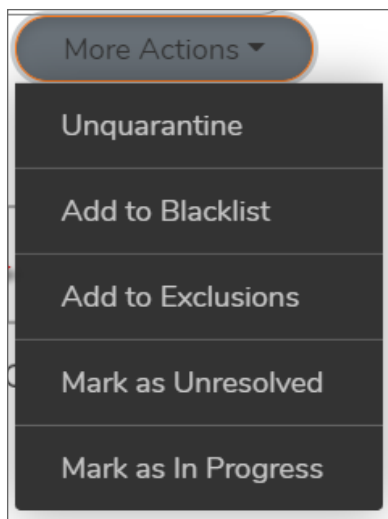
When you expand the threat, you have access to additional actions.

Click on **Download** drop-down tab and select the required format (pdf, json, or csv) to download the threat report. Alternatively, click on the file name in the File Info section to view the download threat file option. To download threat file, see [Downloading a Threat File](#).

Click on **Disconnect Network** to disconnect the device from the network.

Click on **Analyst Verdict** drop-down to take the security team's decisions. For more information, see [Analyst Verdict](#).

Select the **More Actions** drop-down list, which provides other actions you can take on the threat.



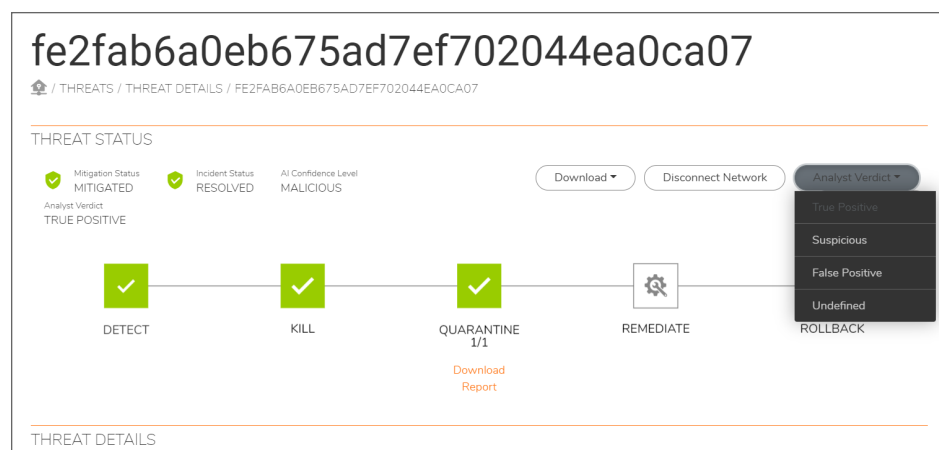
You also have other options to analyze the details of threats by scrolling down to the **File Info** and **Summary** sections:

- Click on the **View events** hyperlink to view the capture ATP events.
- Click on the **VirusTotal** hyperlink to determine if the threat was seen by anyone else. For more information, see [Detected Threats](#).
- Click on the hyperlink pertaining to **Seen on network** to view the details and number of instances the threat was seen on the network.
- Click **Open Policy** to navigate to the **Threat Protection** page.

Click **Go Back** to navigate to the **Threat Lists** page.

## Analyst Verdict

The Analyst Verdict feature serves as a place to record the security team's decisions - True Positive, False Positive, or Suspicious.



Analysts can investigate threats for hours or even days to reach a conclusion. A recorded verdict for each threat gives you more visibility about what occurs in your environment: to view the number of True positives, False positives, and the threats that you are not sure about (suspicious). Thus Analyst Verdict helps the team work more efficient. This feature also makes the threats easily searchable for future reference. For example, when you find a suspicious threat entering your environment, click on the link in the Network History of the threat. You can find if the same threat was seen in your network a month ago and a teammate marked it as True Positive. You can mark the same threat True positive without further investigations, or you can add it to the Blacklist as required.

When you run a mitigation action on one or more items, you are prompted to set the Analyst Verdict.

Each threat starts as **Undefined**.

If you set the Analyst Verdict to **True Positive** or **Suspicious**, it does not trigger any changes. If you set the Analyst Verdict to **False Positive**, the Threat Status changes to **Marked as Benign**.

❗ | **NOTE:** It DOES NOT automatically create exclusions or blacklist items.

If you create an exclusion for threats (**Threat Actions > Add to Exclusions**), the Analyst Verdict automatically changes to **False Positive**.

If you add threats to the blacklist (**Threat Actions > Add to Blacklist**), the Analyst Verdict automatically changes to **True Positive**.

When there is lack of sufficient evidence to establish a threat as either malicious or non-malicious (False Positive), you can update an Analyst Verdict to Suspicious.

To change a threat's Incident Status to Resolved, it must have an Analyst Verdict set.

You can change the Analyst Verdict at any time if you get new information or regret your decision.

## Downloading a Threat File

You can download the threat files in ZIP format from the **Threat Details** page.

### *To download a threat file:*

1. Click on the threat to expand it and see details on the **Threat Details** section.
2. Click on **Download** drop-down tab in the **Threat Status** section and select **Threat File**.
3. Enter and confirm the **Password** to protect the ZIP file archive that contains the threat.
4. Click **Download**. The Download window is displayed after a few seconds.  
Clicking on the threat file option allows the affected machine to upload the threat file to CMC and then download it to the local machine that requested the threat file. This may take a few seconds.
5. Save the threat file. You can check the logs from the **Activities** page.

## Detected Threats

You can select individual threats for details of that threat and actions taken by SonicWall Capture Client. You can also see the current status of the threat and in some instances, you are given a list of options for further actions, including **Mark as In Progress**, **Mark as Resolved**, **Add to Exclusions**, and **Add to blacklist** and so on.

If you click on a threat that was only detected, it shows a page as given below. Under the Actions section, you can see that the Threat has only been detected. It shows that the reason for non-prevention of the threat is because the policy is set to **Detect (Alert only)** threats. It does not **Protect (Kill & Quarantine)**.

# Noi dung chi tiet

[Home](#) / [THREATS](#) / [THREAT DETAILS](#) / [NOI DUNG CHI TIET](#)

---

## THREAT STATUS

Mitigation Status

NOT MITIGATED

Incident Status

RESOLVED

AI Confidence Level

MALICIOUS

Download ▾

Disconnect Network

Analyst Verdict ▾

Threat Actions ▾

Analyst Verdict

TRUE POSITIVE

DETECT

KILL

QUARANTINE

REMEDiate

ROLLBACK

---

## THREAT DETAILS

- By looking at **File Info** section, you can see the file name, path, and the device on which it was detected, as well as device details such as IP address and time of detection and alerting.
- The Threat Indicators section displays the reasons for the engine to detect the incident. Indicators are generated based on analysis of the threat. The indicators display the behaviors the engine detected as malicious or suspicious. These include:
  - Abnormalities
  - Boot Configuration Update
  - Discovery
  - Evasion
  - Exploitation
  - Execution
  - General
  - Hiding/Stealthiness
  - Impersonation
  - InfoStealer
  - Injection
  - Lateral Movement
  - Malware
  - Packer
  - Persistence
  - Post Exploitation
  - Privilege Escalation
  - Process Injection

- Ransomware
- Reconnaissance
- To determine if this threat was seen by anyone else, you can click on the **VirusTotal** link in the summary section to open a browser window with a search against the **VirusTotal** database for the SHA1 Hash of the file.
  - Check the signing authority for the file. If it is a legitimate organization and is verified, this may be a false positive. But some threats steal legitimate certificates for signing malware code.
  - The detection engine reflects which engine enabled via the policy actually detected this threat.
- If you deem that the threat is real, you can immediately kill and quarantine the threat using the Kill link located in the **More Actions** section.
- If you are not sure and would like to investigate further, you can contain the threat from spreading to other endpoints or from causing network-based impact (like exfiltration of data). You can also logically disconnect the endpoint from the network by clicking on the **Disconnect Network** button. This ensures that the endpoint can talk to the Capture Client Management Console but not to any other destination. You can reset this action by clicking on the button again which is now labeled **Reconnect to Network**.
- If the file looks like a legitimate file to your organization (custom app/script), then you can mark it as benign by clicking on **More Actions** and selecting **Mark as benign**.
- If the file is determined as malicious, you can also select **More Actions > Add to Blacklist** to mark it as a legitimate threat across the organization. In this case the Analyst Verdict is set as **True Positive**. This reduces the need to do any analysis on this threat if it is seen again.
- If you create an exclusion for threats (**More Actions > Add to Exclusions**), the Analyst Verdict automatically changes to **False Positive** and the Status is set to **Marked as Benign**.

## Threats Mitigated

If you click on a threat that was mitigated, you see that the threat was detected, alerted on, killed (stop execution) and quarantined (prevent further execution temporarily). Since the threat was mitigated, one can be confident that this was a real threat. However, to validate this, you can follow the same investigation steps as provided in [Detected Threats](#).

If you have confirmed that the threat is real, then it is good practice to remediate (delete or remove) the threat from the endpoint. This can be done by clicking on the **Remediate** under the **Actions** section.

## Performing a Rollback

Even if a threat has been re-mitigated, you cannot be sure that there are no remnants that may impact performance (for example, registry keys, temp files, system changes, and so forth). The best way to avoid issues is to roll the system back to its last known good state. This is made possible using the **Rollback** function available with Capture Client.

- ① | **IMPORTANT:** Before performing rollback on Windows endpoints, you need to configure Volume Shadow Copy Service (VSS). To configure VSS on Windows computers for Capture Client rollback feature to work, see [SonicWall Support Knowledge Base](#).

The **Rollback** function is only available on Windows endpoints and relies on the Virtual Shadow Copy Service (VSS) available in the Windows operating system. It is enabled by default and used to create the system recovery image. The **Rollback** function is only available for customers who procure the **Capture Client Advanced** license for their endpoints.

- ① | **NOTE:** The Rollback feature is currently only available for Windows systems.

The time it takes for a rollback to complete depends on the size of the shadow copy, but for a large disk, it should only take a few minutes.

Once the rollback is complete, the **Actions** section shows that the rollback was completed successfully.



## Resolving Threats

After you have taken necessary action with any threat, it is important to mark it as **Resolved**. This ensures that no other user has to investigate the threat and the end-user systems are released from their Infected state, thereby not seeing any alerts for infections on the client console. To resolve then threat, click **More Actions > Resolve Threat**.

- ① | **NOTE:** Marking an issue as resolved does not ensure that the system is not infected. Make sure that you have taken the appropriate action to investigate and resolve the threat before you mark it resolved.

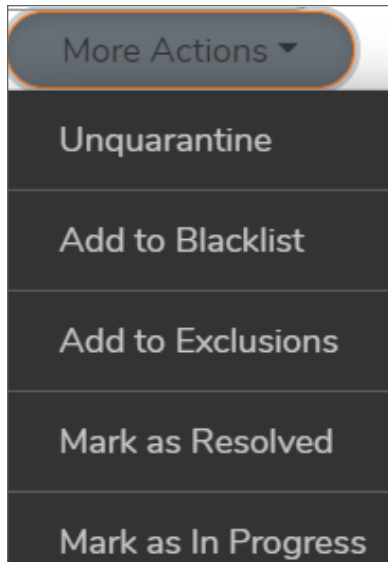
## Blacklisting Threats

After you have taken necessary action on any known threat, you can blacklist the threat. Threats similar to the blacklisted one will also blacklisted.

### ***To blacklist a known threat:***

1. Click on a threat from the **Threat Details** page.
2. Click **More Actions** drop-down box, click **Add to blacklist**.





3. Click **Confirm**.

## Benign Threats

In the event that Capture Client reports a false positive, you are able to mark the file as benign. This instructs the endpoint client to ignore the process when it occurs again.

To mark an event as benign, go to **More Actions** in the **Status** pane and select **Mark as benign**.

# Investigating and Responding to Active Clients

This workflow shows administrators how to investigate the state of the devices, view details of the devices and details of the users using the endpoint. For threat events, refer to [Threat Investigation](#).

To view the list of endpoints and take any actions, navigate to **Assets > Devices**.

## View Clients

To view the list of devices managed by this instance of SonicWall Capture Client, navigate to **Assets > Devices**.

Capture Client Management

Shivadas\_Expire-CC0000C10FB7

### Devices

ASSETS / DEVICES

List View World Map

NAME	STATUS	COMMISSIONED	NETWORK STATUS	PENDING ACTIONS	PENDING THREAT REBOOT	LAST AC
Win10_dome0		Yes	Unavailable	N/A	N/A	2 months
Win10_dome1		Yes	Unavailable	N/A	N/A	2 months
Win10_dome10		Yes	Unavailable	N/A	N/A	2 months
Win10_dome100		Yes	Unavailable	N/A	N/A	2 months

Total: 25 elements

Last Update: 1/16/2024 8:37:09 AM


Showing 1-25 of 1019 records | 25 per page

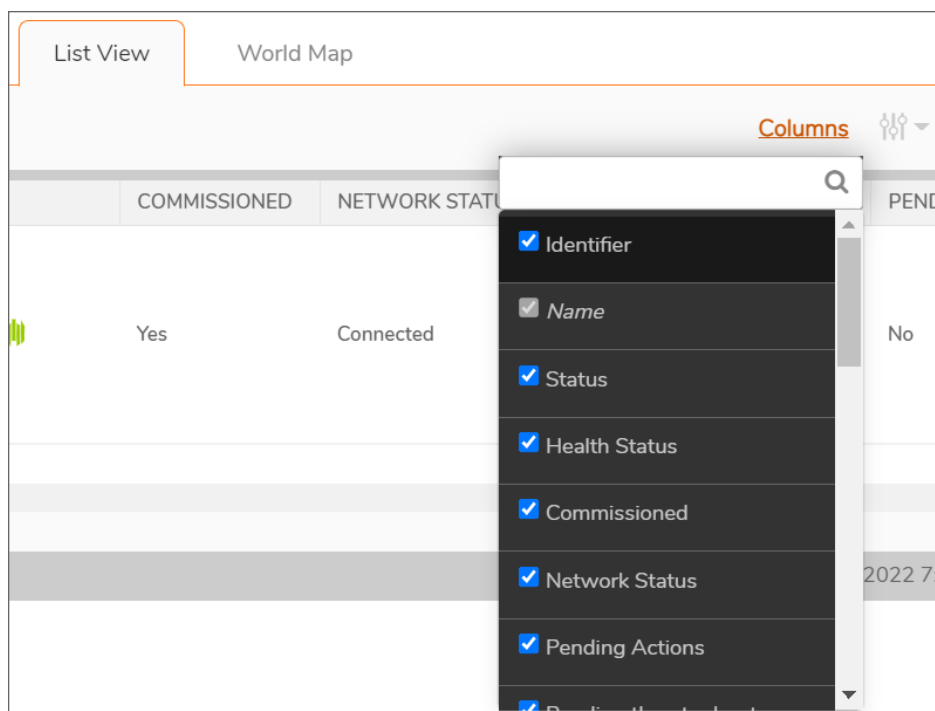
Page 1 / 41




At the top of the page, you have the options to:

- Filter the list: Click and select the check the boxes for the **Capture Client, SentinelOne, Health Status, Commissioned, Network Status, Pending Actions, Pending Threat Reboot, Operational**

**State, Vulnerability Status, Type, OS, Network Protection, Update Requested, SentinelOne Pending Upgrade, Scan Status, Disk Encryption**, or by entering the **Client Version, SentinelOne** version or the **Location** options in the respective search boxes to filter on.

- Search: Click  and enter the search string.
- Columns: Click **Columns** to select and view the required columns. You can customize the options to display the required columns including Identifier (shows as an identifier or 'tag' assigned to the endpoint), Name (Endpoint name), Status (shows the current state of any updates performed), Health Status (shows as Healthy or Infected. An endpoint shows as infected if it has at least one active threat.), Commissioned, Network Status (Is **Disconnect from Network** enabled or disabled), Pending Actions, Pending threat reboot (Yes or No), Operational State (If an endpoint was disabled by the customer or by SentinelOne it shows **Disabled**. Otherwise it shows **Not disabled**.), Vulnerability Status, Tenant, Last Active (when the Agent last connected to the Management), Current User, Local IP, Console Visible IP (External IP address of the Agent), Location, Domain (Network domain that the endpoint belongs to), Type (Installer type - file used to install the Agent), OS, Network Protection, Client Version, SentinelOne Version, SentinelOne Pending Upgrade, Scan Status (when the last scan was completed), Disk Encryption (On or Off), and Group.

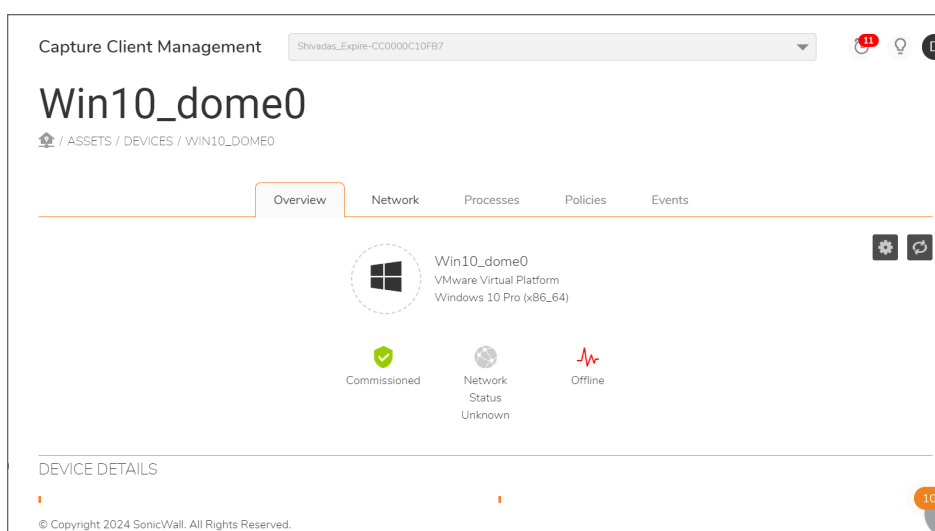


- Export as CSV: Click  to export and download the devices details to CSV file.
- Refresh data: Click  to refresh data.
- Taking appropriate actions for devices: Select the device from the list and click  to take appropriate actions. You can take any of the following:

- Initiate Scan
- Uninstall
- Decommission
- Delete
- Disconnect from Network
- Refresh Active Directory Info

## Monitoring and Managing the State of Devices

On clicking any of the devices, the **Overview** tab shows details of the device including the machine name, IP address, the operating system (OS) in which it is running, the licenses that are attached to this device and the users logged into this device the last time.






To collect information for troubleshooting or to manage state of the device, click  and select:

- **View Threats**
- **Update Policy** to update the Endpoint Policy assigned to the user.
- **Upgrade Client**
- **Refresh Active Directory Info**
- **Send Logs**
- **Enable Debug Logs**
- **Archive Logs**
- **Initiate Scan**

- **Send TSR** (to pull specific data from the endpoint for investigation purposes)
- **Disconnect Network**
- **Decommission** to decommission Capture Client and remove it from console
- **Uninstall Client** to uninstall Capture Client from the endpoint
- **Show Authorization Password**
- **Shutdown Device**
- **Reboot Device**
- **Reset Authorization Password**

The key data points to be observed here are the three icons in the **Overview** tab that represent the state of the endpoint. The green colored icons represent a healthy state while gray icon indicates that there is a problem with that device.

Icon	Meaning
	<p>Green if network is connected.</p> <p>Red if network is disconnected.</p> <p>Grey if network status is unavailable.</p> <p>Orange if network is reconnecting.</p>
	<p>Green if SentinelOne agent is online.</p> <p>Grey if SentinelOne agent is Offline.</p> <p>Yellow if SentinelOne is in 'Pending upgrade' or 'Pending uninstall' state.</p> <p>Red if SentinelOne has a pending action. For more details, refer to <a href="#">SentinelOne Pending Actions</a>.</p>
	<p>Green if Capture Client on the endpoint is online.</p> <p>Grey if Capture Client on the endpoint is offline.</p>

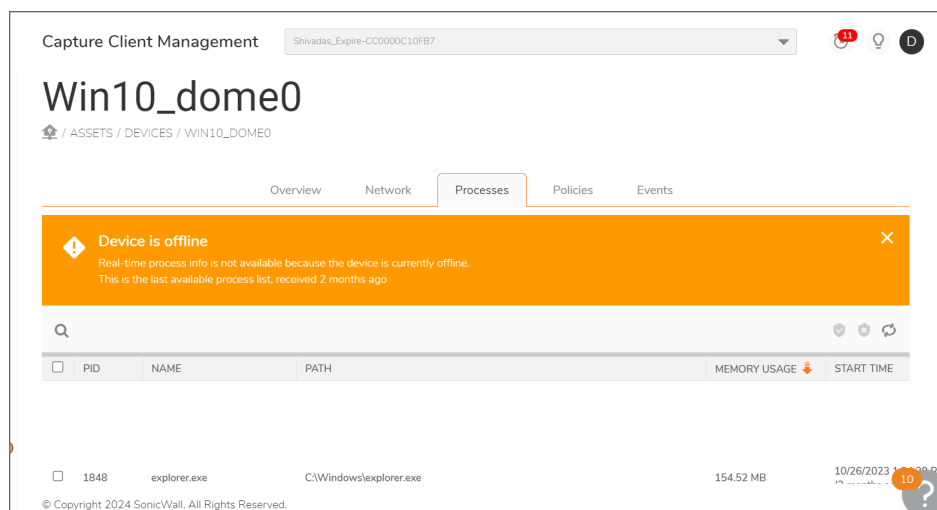
- **Activated**—This state means that the device on which Capture Client is running is connected to the network and can access the network.
  - **Possible Problem**—The Capture Client or any of its modules needs an upgrade to the most current version. The device is unavailable when the icon is red and pending connecting information when gray.
  - **Resolution**—Navigate to **Policies > Client** for the package and roll out the latest version of the package.
- **Online**—This state means that this device is up and running and is communicating with the Cloud Management Console.
  - ① | **NOTE:** Even if the device is offline, the device is still protected.
  - **Possible Problem**—The endpoint is disconnected from the network and cannot communicate with the Client Management Console. If you see the icon in red, the device cannot communicate


with either Cloud Management Console or SentinelOne.

- **Resolution**—Validate with the user that the endpoint is up and running and online. If yes, then check for any firewalls or network connectivity issues that may be impacting connectivity to the console. Check the Logs folder in the Capture Client installation folder for the endpoint for any connectivity errors. If no error is identified, attempt a reboot of the system to restore it to a good state.

## Reviewing Processes Running on a Device

Capture Client also obtains the list of processes running on an endpoint at any given time. Knowing what processes are running can be useful in malware incident investigations. It also helps you to know if a dubious application or process is being run on the endpoint. Navigate to **Assets > Devices** to see the entire list of processes running on that endpoint. Select a device and click on the **Process** tab. You can also search for specific processes by name or filter the list if you are looking for a specific process.



You can easily build bulk exclusions from the **Processes** tab of any device. Simply select the process or set of processes and then click . This icon is to **Adds paths to exclusions**. You can even search for processes belonging to a specific application or vendor (for example, Apple or Adobe) and exclude all their applications.

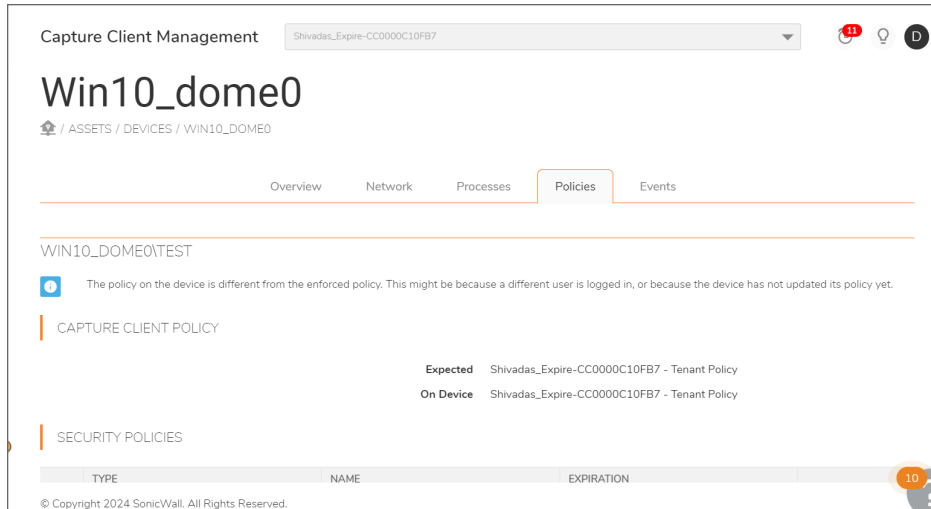
You can also de-list processes on the **Processes** tab (remove them from the Exclusions list). Those processes that are already excluded are identified by a gray checked shield at the end of the name. Select all those

processes that you want to de-list, and click . This icon **Removes paths from exclusions**.

Click  to refresh data.

# Reviewing Policies Enforced on a Device

Click on **Assets > Devices**. Double-click on the desired device in the table to see the device detail. Select the **Policies** tab to view the policies assigned to the user who was logged into this device. This can be helpful in investigating if a policy issue may be causing problems with a specific endpoint. From this section, you can also navigate to editing the Capture Client policy or the child Threat Protection and Trusted Certificates policies.



Scroll down and click on the **Details** button to view the **Policy Priority** window. You can manually modify the policies assigned to a particular user. Refer to [Capture Client Policies](#) for more information.

## SentinelOne Pending Actions

SentinelOne device icon is displayed in red, if there is some pending action required for SentinelOne to become fully functional.

This includes any of the following:

- Agent Suppressed (macOS only) - An agent upgrade might be required.
- Unprotected (macOS only) - Enable the anti-tampering for the agent, or make sure that the agent's local configuration is appropriate.
- Incompatible OS (macOS only) - An agent upgrade might be required.
- Attention Needed (Windows only) - Reboot the endpoint manually.
- Missing Permissions - Make sure that the user permissions on the endpoint computer allows SentinelOne agent installation.
- Reboot required.

# Investigating and Responding to Active Users

Capture Client also captures which users are logged into the managed devices and allows for applying policies to users and user groups (and not just clients) in case they have more than one device. To manage users and group policies, you can either navigate to **Assets > Users**. The landing page displays a list of all the users who have registered managed devices with the Capture Client Console.

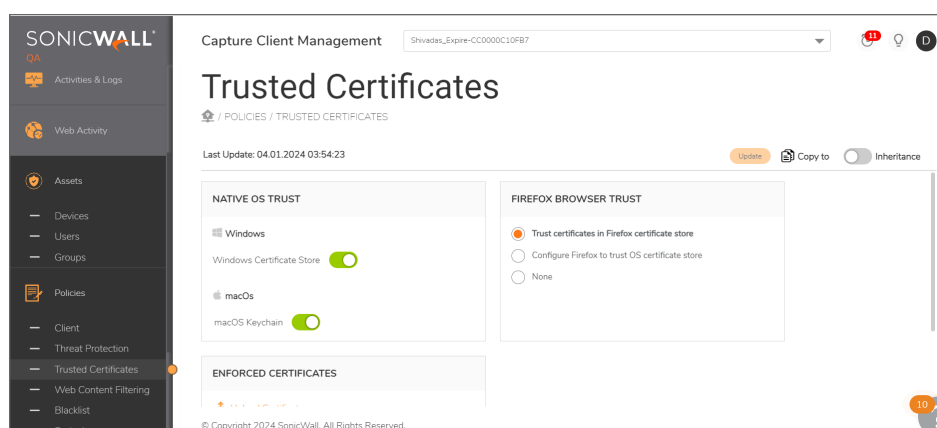
Clicking on any user entry opens an overview page that shows the user's profile information as well as devices registered to that user.

Click on the **Policies** tab to see what policies have been assigned to this user. This page also allows for manual modification of policies assigned to this user. Refer to [Capture Client Policies](#) for more information.



# Enforce Trusted Certificates

Trusted Certificate summarizes how many SSL certificates are in use and being enforced.



① | **NOTE:** You can also configure trusted certificate policies by navigating to **Policies > Trusted Certificates**.


The **Trusted Certificates** page displays the **Native OS Trust** settings:

- Windows - Displays the toggle button for the Windows Certificate Store.
- macOS - Displays the toggle button for the macOS Keychain.

You can view the **Firefox Browser Trust** options:

- Trusted Certificates in Firefox Trusted Store.
- Configure FireFox To Trust OS certificate store.
- None

Click **Upload Certificates** under the **Enforced Certificates** option to upload a certificate.

Click  to view the details of the certificates uploaded in the **Certificate Information** window. You can view the information such as Name, Serial Number, Issuer, Subject, Public Key, Finger Print, and Validity details.

CAPTURE-QA-BLR.COM

CERTIFICATE INFORMATION

Name	capture-qa-blr.com
Serial number	A95E42F17AD206DD
Issuer	capture-qa-blr.com (qa) blr, ka, AU
Subject	capture-qa-blr.com (qa) blr, ka, AU
Public Key	RSA, 4096 bits
Fingerprint	SHA-256: 78 9B C1 1B 66 E4 93 31 6E A2 01 50 69 50 B7 AF 23 B5 07 BA 50 8E B6 8A 03 30 98 68 77 DB 26 1E

VALIDITY

Not valid before	Mon May 21 2018 23:56:54 GMT+0530 (India Standard Time)
Not valid after	Sun May 21 2023 23:56:54 GMT+0530 (India Standard Time)

Close

Click on the **Inheritance** toggle button if required. For more information on Inheritance, refer to the section *Inheritance* in the [Protecting Assets with Security Policies Guide](#).

Click **Update** to save and update the settings or the changes done, to the endpoint.





# Investigating and Responding to Risky Applications

Unpatched applications can be vulnerable to exploits and expose your entire IT infrastructure. Capture Client investigates and manages the risk associated with the apps (across all devices associated with a tenant) that do not have the latest patches.

- ① **NOTE:** Endpoint applications are scanned automatically on a weekly basis on every Wednesdays at 11 PM. The manual rescan can be done from SentinelOne console, if you have a Capture Client Premier license. Otherwise you need to contact the support team for assistance.

The Dashboard displays the number of vulnerable apps across all devices associated with a tenant.

At the top of the page, you have the options to

- Filter the list: Click  and select the check the boxes for the **Risk Level, Type, OS, or Device Type** options to filter on.
- Search: Click  and enter the search string.
- Download Files: Click  to download the Endpoint and CVE (Common Vulnerability and Exposure Identifier) lists.
- Refresh data: Click  to refresh data.

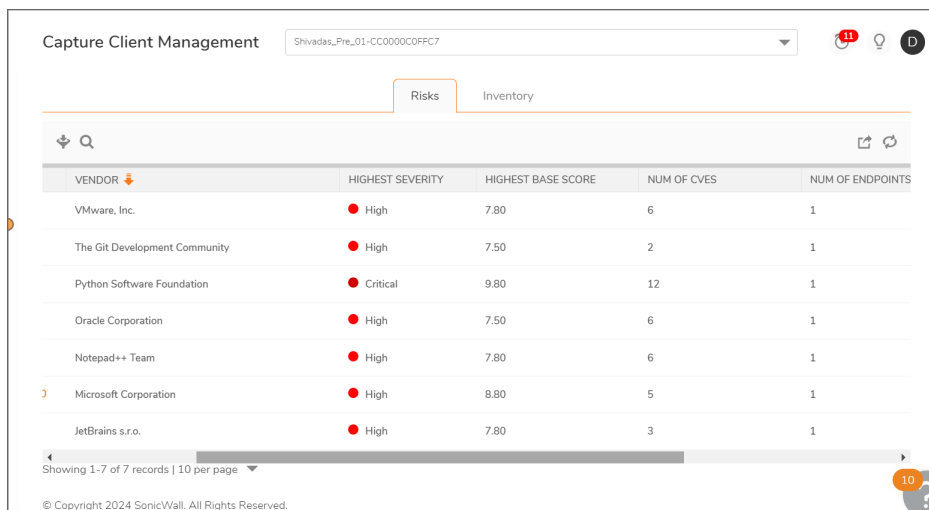
## ***To investigate and respond to vulnerable applications:***

1. Click **Applications** to view the list of vulnerable applications.  
The table on the **Applications** page lists the unpatched applications and displays the highest severity based on the highest base score for each. The values for the highest severity scores are Critical, High, Medium, and Low.  
You can sort the applications based on their risk level by clicking the **upward/downward** arrow next to **Highest Severity** in the header row.

- ① **NOTE:** The risk levels are categorized according to the Highest Severity Scoring System as given below:

Risk Level	Color	Highest Severity Score
Critical	Dark Red	9.0 to 10.0
High	Bright Red	7.0 to 8.9
Medium	Orange	4.0 to 6.9
Low	Yellow	0.1 to 3.9
No known risk	Green	The application poses no risk to the endpoint.

- You can choose to filter the vulnerable apps with **Highest Severity**, or **Device Type** to attend to the vulnerable apps on your priority.



The screenshot shows the 'Capture Client Management' interface with a search bar and a table of vulnerable applications. The table has columns for Vendor, Highest Severity, Highest Base Score, Num of CVEs, and Num of Endpoints. The 'Risks' tab is selected, and the table displays 7 records. A pagination bar at the bottom indicates 'Showing 1-7 of 7 records | 10 per page'.

VENDOR	HIGHEST SEVERITY	HIGHEST BASE SCORE	NUM OF CVEs	NUM OF ENDPOINTS
VMware, Inc.	High	7.80	6	1
The Git Development Community	High	7.50	2	1
Python Software Foundation	Critical	9.80	12	1
Oracle Corporation	High	7.50	6	1
Notepad++ Team	High	7.80	6	1
Microsoft Corporation	High	8.80	5	1
JetBrains s.r.o.	High	7.80	3	1

Showing 1-7 of 7 records | 10 per page

© Copyright 2024 SonicWall. All Rights Reserved.

- Use filter options to list the applications based on **Highest Severity** or **Device Type**.

Risks

**HIGHEST SEVERITY**

☒ Critical (9.0 - 10.0)

☒ High (7.0 - 8.9)

☒ Medium (4.0 - 6.9)

☒ Low (0.1 - 3.9)

**DEVICE TYPE**

☒ Desktop

☒ Laptop

☒ Server

- For more information about vulnerabilities in each application, click on each application to see details.

Capture Client Management
Shivadas\_Pre\_01-CC0000C0FFC7

## Applications

🏠 / APPLICATIONS

Risks
Inventory

◀
PyCharm Community Edition 2020.3.3
|
Vendor JetBrains s.r.o.
|
First Detected Jan 10, 2024
|
Highest NVD Base Score 7.80
|
Severity HIGH

Endpoints

CVEs

+

🔗 🔄

DEVICE	OS VERSION	TYPE	DOMAIN	APPLICATION DETECT...	DAYS FROM DETECTION	LAST SL
CCDEV-VTB160	Windows 10 Pro 19045	desktop	CCAUTO	Jan 10, 2024	6 days	Jan 11, 2

Showing 1-1 of 1 records | 10 per page

10
?


© Copyright 2024 SonicWall. All Rights Reserved.

- Click on the **Endpoint** tab to view the detailed description of the **Device**, **OS Version**, **Type**, **Domain**, **Application Detection Date**, **Days from Detection**, **Last Successful Scan**, and **Last Scan Result**.
- Click on the **CVEs** tab to view the Common Vulnerabilities and Exposure details including the **CVE ID**, **Severity**, **NVD Base Score** (the highest National Vulnerability Database score), **Published Date**, **Description**, and the **CVE Links**.


For more information the application view details are explained in the table given below.






Item	Description
Application Name	Name of the application that has vulnerability


Vendor	Application Vendor
Highest Severity	Based on the Base score. The values are Critical, High, Medium, and Low.
Highest NVD Base Score	Highest National Vulnerability Database (NVD) score for this application.
Number of CVEs	The number of CVEs that were detected on this application
Number of Endpoints	The number of endpoints the application has installed.
Application Detection Date	When the Agent detected this application on the endpoint.
Days from Detection	The number of days this application is on the endpoint from the time the Agent detected it.

5. You can also download the Endpoints and CVE lists clicking on .
6. Click on the Inventory tab to view the details such as Name, Vendor, Number of Versions, and the Number of Endpoints.

## Applications

 / APPLICATIONS

Risks Inventory			
<div>     </div>			
NAME 	VENDOR	NUMBER OF VERSIONS	NUMBER OF ENDPOINTS
7-Zip	Igor Pavlov	1	1
Autolt	Autolt Team	1	1
Azure Data Studio	Microsoft Corporation	1	1
Capture Client	SonicWall	1	1
Dependency Agent	Microsoft Corporation	1	1

Showing 1-10 of 28 records | 10 per page
Page 1 / 3


© Copyright 2024 SonicWall. All Rights Reserved.

# 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
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

# About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Capture Client Monitoring with Dashboard, Threats and Applications Administration Guide  
Updated - December 2024  
232-005518-00 Rev H

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