



Capture Client

Protecting Assets with Security Policies

Administration Guide

SONICWALL[®]

Contents

Overview	3
Description	3
Navigation	4
Guide Conventions	5
Scopes and Policies	7
Introducing Scope of Operations	7
Using Scope Selector	8
Policy Management	8
Inheritance	8
Policy Types	10
Replicating Policies	19
Group Ranking Policy	21
Creating Custom Policies for Device Groups	21
Device Control	22
Protection	23
Tenant Token	23
Installation for the New Clients	25
Migrating Clients Across Regions	27
Protecting Devices	29
Reviewing Registered Devices	30
List View	32
Unmanaged List View	33
Map	34
Active Users	35
Performing System Scan	36
Groups	38
Creating a Static User Group	39
Creating Static Device Groups	41
Creating Dynamic Device Groups	43
Creating Custom Rules for Dynamic Groups	46
SonicWall Support	48
About This Document	49

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 document describes how to set up the protection for your environment.

- [Scopes and Policies](#)
- [Protection](#)
- [Groups](#)

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

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

Description

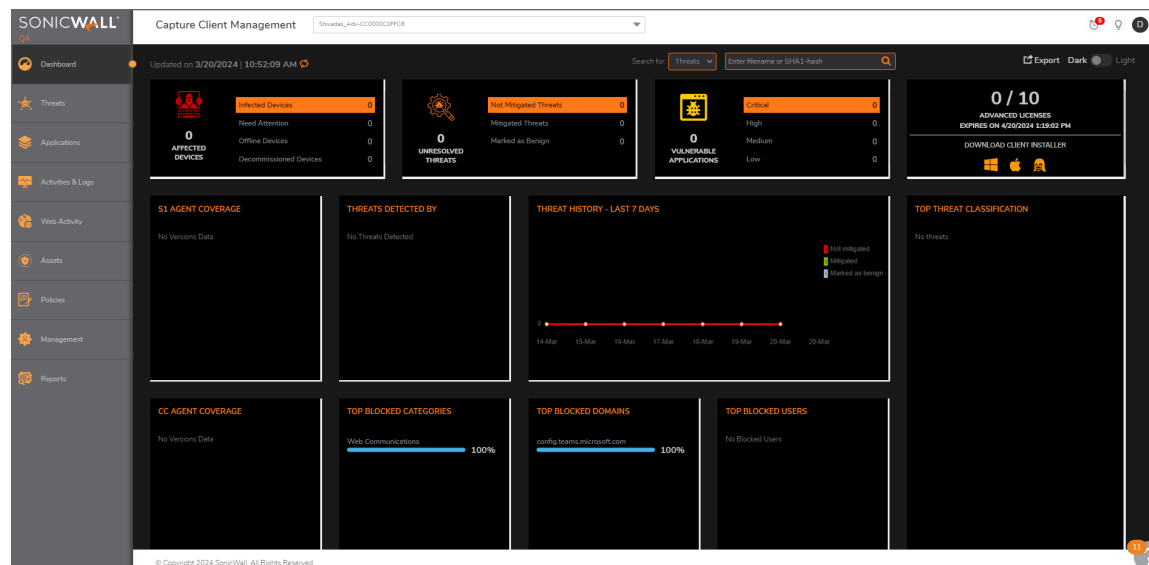
SonicWall Capture Client is a client offering that delivers multiple client protection capabilities. With a next-generation malware protection engine powered by SentinelOne, the SonicWall Capture Client delivers advanced threat protection with these key features:

- **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.

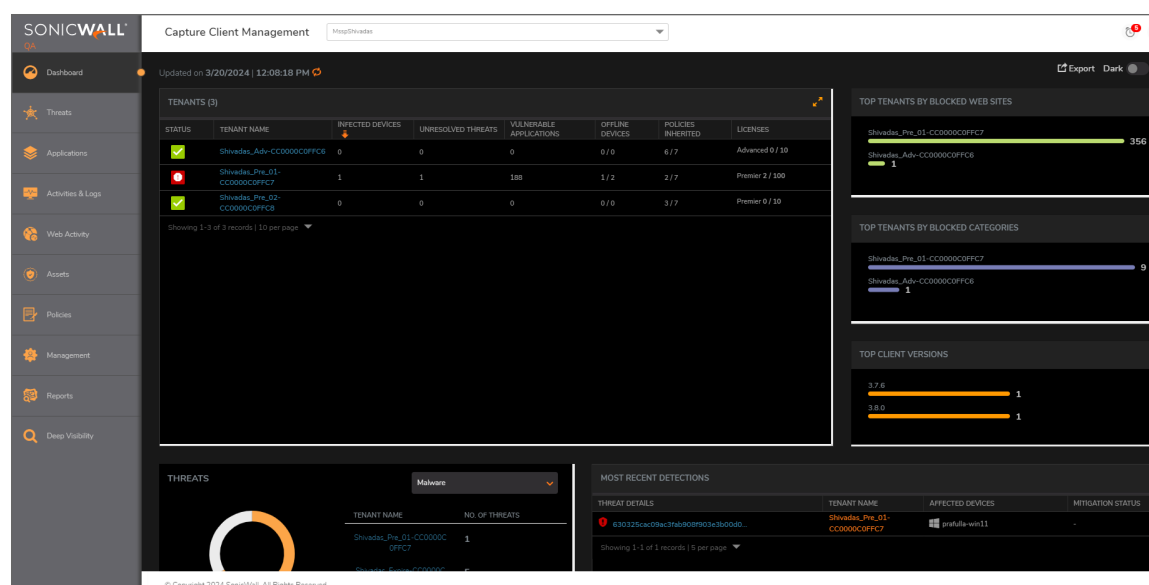
The size of your Capture Client tenancy is only limited by the number of endpoint licenses procured.

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 infected devices, active threats and critical issues. You can also see a series of tiles showing the top items in each category. By scrolling down on the Dashboard, you can see a summary of issues by group.

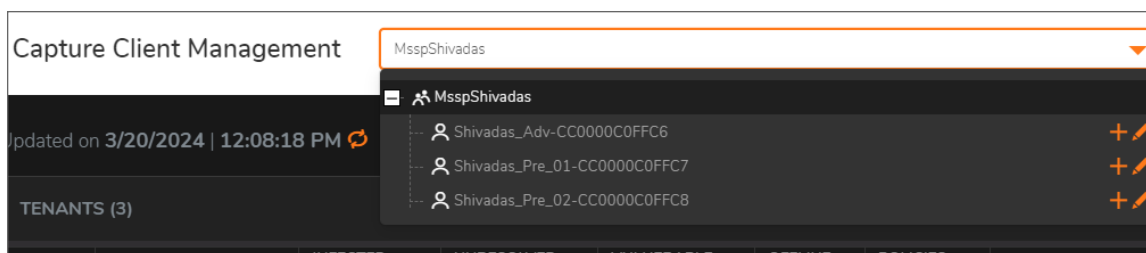


If the account is selected, the Dashboard information is summarized by tenants.



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
Bold Text	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.
Menu divider Menu item > Menu item	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><Computer code italic></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 <code>serialnumber=<your serial number></code> , replace the variable and brackets with the serial number from your device: <code>serialnumber=C0AEA0000011</code> .
<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.

Scopes and Policies

- [Introducing Scope of Operations](#)
- [Using Scope Selector](#)
- [Policy Management](#)

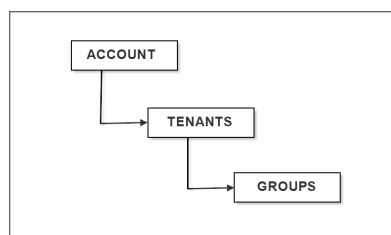
Introducing Scope of Operations

With Capture Client 3.8, a new concept of **Accounts** is being introduced. Accounts are containers of multiple tenants and can be used to define global policies to be applied across multiple tenants managed by the same organizations – as is typical of Managed Security Services Providers (MSSPs) or distributed enterprises that are split into multiple tenants for separate governance.

By default, all tenants will be created within a SonicWall-managed account, which will only have a default policy pre-configured but will not be updated. MSSPs and Distributed Enterprise customers can get their own accounts to better manage multiple tenants by submitting a request via Support.

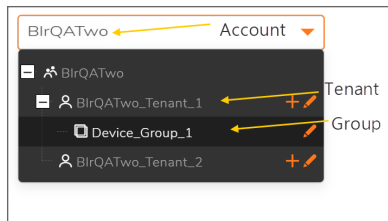
With this change, there is now a multi-tier hierarchy of “scope of operations” within Capture Client. By selecting a scope from the Scope selector, your operations are made specific to the **Account**, **Tenant**, or **Group**. See [Using Scope Selector](#). The available scopes are:

- **Account scope**
- **Tenant scope**
- **Group scope**



Using Scope Selector

By selecting a scope from the Scope selector, your operations are made specific to the selected scope. The available scopes are: **Account**, **Tenant** or **Group**.



Policy Management

- [Inheritance](#)
- [Policy Types](#)
- [Replicating Policies](#)

Inheritance

With this new hierarchy of scope, Capture Client 3.7 also introduces a concept of policy inheritance. *Inheritance* refers to the ability to configure a policy at a child scope to be automatically inherited from the policy of a parent scope. For example: If an MSSP has a baseline policy for Threat Protection, they can configure it at the Account level and enable inheritance for every new tenant they provision. If inheritance is enabled, any changes to the policy at the parent level are automatically propagated to child scopes.

Inheritance propagates from Accounts to Tenants and from Tenants to Groups. And if inheritance is enabled at the Tenant and Group level, the account policy is effectively applied to the Group level.

Policy Inheritance is applicable at an individual policy type and there are different rules for how inheritance works:

Policy Type	Inheritance Rules
Capture Client, Threat Protection, Trusted Certificates and Web Content Filtering	Inheritance can either be Enabled or Disabled. With inheritance enabled in a particular scope, the policy for that scope cannot be modified.
Blacklists & Exclusions	Inheritance is always enabled and cannot be disabled. But you also can create scope-specific configurations.

Policy Type	Inheritance Rules
Device Control	Inheritance can either be Enabled or Disabled. In either case, you can also add scope-specific rules. And the priority of rules will always be in the reverse order of inheritance – the inherited rules from the highest scope is at the bottom of the list.
Email and Notification Settings	Inheritance can either be Enabled or Disabled. For the new tenants, it will be always enabled by default. You can disable it later, if required.

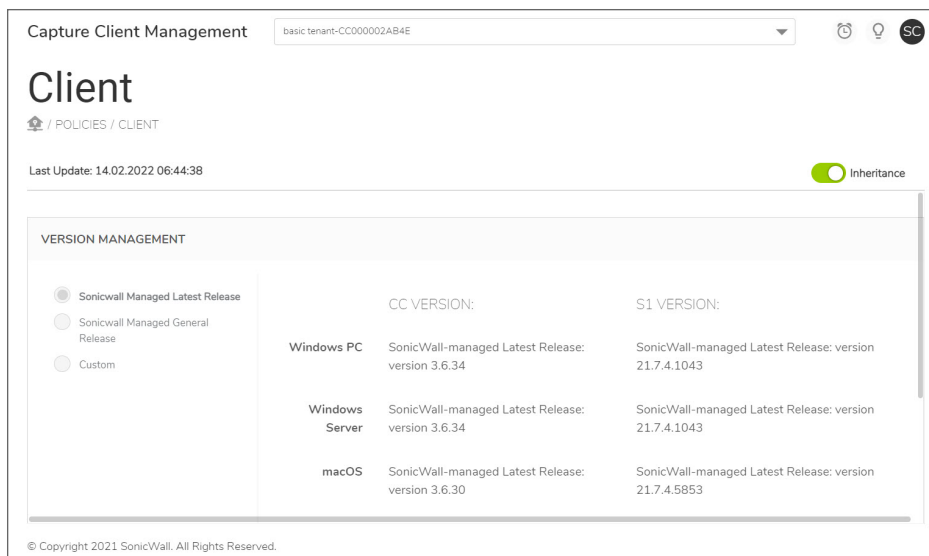
You can create several kinds of policies that can be effectively leveraged through inheritance. These include: **Client**, **Threat Protection**, **Trusted Certificates**, **Web Content Filtering**, **Blacklist**, **Exclusions**, **Device Control** and **Email and Notification Settings**. You can choose to either inherit policies or create custom policies for each tenant.

- ① **NOTE:** Blacklists and Exclusions are forced on tenants: You cannot disable inheritance of Blacklist and Exclusions items on to the tenants, instead you can add blacklist and exclusion items for tenants as required.
- ① **NOTE:** Even while you are inheriting the Email and Notification settings from the account scope, you can customize or edit the Email Address and Time Zone for a specific tenant.

The following is an example of creating a policy for Capture Client version management and enabling inheritance across selected tenants.

To create a Capture Client base policy and enable inheritance tenants:

1. Log into the Client Management Console and select the master account in the **Scope Selector** at the top of the page.
2. Navigate to **Policies > Capture Client**.
3. Configure the required Capture Client version management settings.
4. Click **Update** to save the base Capture Client policy.
5. From the **Scope Selector** at the top of the page, select any tenant that you want to inherit the parameters of this core Capture Client policy.
6. Navigate to **Policies > Client** and select the **Inheritance** option to green.



7. Provide confirmation.

Repeat steps 4 through 6 for other tenants if you wish to copy this Capture Client policy to other tenants too. If inheritance is enabled, any changes to the policy at the parent level are automatically propagated to child scopes.

Policy Types

The security policies define the conditions and constraints for connection.

The available security policies are:

- [Client Policies](#)
- [Threat Protection Policies](#)
- [Trusted Certificate Policies](#)
- [Web Content Filtering Policies](#)
- [Managing Blacklist](#)
- [Exclusions](#)
- [Device Control](#)

Client Policies

The Capture Client policy enables you to manage the Capture Client version on the endpoint devices .

To configure the Capture Client version management:

1. Log into the Capture Client Management Console and select the appropriate scope to configure the Client version management.

2. Navigate to **Policies > Capture Client**.
3. In the **VERSION MANAGEMENT** section, select one of the available options:
 - **Sonicwall Managed Latest Release**
 - **Sonicwall Managed General Release**

To let SonicWall manage the Capture Client version upgrades to the client machines, any latest available version/ latest general release version that SonicWall releases and promotes will be pushed to the client machines by automatically updating the Client Policy.
 - **Custom**

This option lets you control which version of the client gets installed on your devices by manually updating the required client version and compatible SentinelOne version in the Client policy.

You need to select the compatible SentinelOne version for the Capture Client version that you select in the CC VERSION section.
4. Configure the required Capture Client version management settings and click **Update** to save the Client policy.
5. In the **ADVANCED SETTINGS** section:
 - Either enable or disable the **Auto-Decommission** option. If enabled, set the time that a system can be offline before it is automatically decommissioned.
 - Either enable or disable the **Auto-Delete** option. If enabled, set the time that a system can be decommissioned before it is automatically removed from the network.

Threat Protection Policies

Threat Protection policy is one of the security policies that Capture Client offers. To view the Threat Protection policies, navigate to **Policies > Threat Protection**. The Threat Protection page lists the POLICY MODE OPTIONS, PROTECTION & CONTAINMENT OPTIONS, ENGINE SETTING, and ADVANCED SETTINGS.

To define the threat protection policy:

1. Navigate to **Policies > Threat Protection**.
2. If you want to configure a custom threat protection policy for a tenant, disable Inheritance.
3. In the **POLICY MODE OPTIONS** section:
 - a. Set the Policy Mode or mitigation mode for threats and suspicious activities. The available mitigation modes are: **Detect** (Alert Only), **Protect** (Kill & Quarantine), or **Capture ATP** (Auto Mitigate).

Detect—Detects a potential threat, suspicious activities and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.

Protect—Detects a potential threat, reports it to the management console, and immediately performs the configured Mitigation Action to mitigate the threat. To understand protection and options available for Protect mode, see step b.

Capture ATP—To let Capture ATP analyze suspicious activities and take necessary action based on the Capture ATP settings.

Capture ATP		
(Auto-mitigation) Protect		Detect (Alert Only)
Set the action to take if Capture ATP returns a Malicious Verdict : You have an option to enable the setting that ensures Capture Client to kill the process and block access to the file until a verdict is delivered.	When Protect is selected, the Mitigation Action is automatically set to Kill & Quarantine. This stops processes, encrypts the executable, and moves it to a confined path. If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action here is Quarantine.	Detects a potential threat and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.
<ul style="list-style-type: none"> • Mark as Threat — Automatically quarantines the file, marks it as a threat, and performs the corresponding mitigation action. • Detect (Alert only) 		
Set the action to take if Capture ATP returns a Not Malicious Verdict:		
<ul style="list-style-type: none"> • Detect (Alert only) • Mark as Benign 		

Capture ATP (Auto-mitigation) Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a Not Undetermined Verdict:	
<ul style="list-style-type: none"> • Detect (Alert only) • Mark as Threat • Contain 	

4. In the **PROTECTION & CONTAINMENT OPTIONS** section:

- Set the protection level. The available protection options are: Kill & quarantine, Remediate, or Rollback.

① **NOTE:** If you selected Detect for the Mitigation Mode, the Mitigation Action field is hidden since there are no actions for that option.
- Select **Disconnect from Network** If you want to automatically put a device in network quarantine when an active threat is detected. All of the agent's network connections will be blocked except to the management console. Devices will not be disconnected if a threat is detected pre-execution by the Reputation or Deep File Inspection engines, because the threat is not active.

5. In the **ENGINE SETTINGS** section:

Engine Type	Definition
Reputation	This engine uses the SentinelOne Cloud to make sure that no known malicious files are written to the disk or executed. This option cannot be disabled.
Documents, Scripts	This is a behavioral AI engine on Windows devices that focuses on all types of documents and scripts.
Lateral Movement	This is a behavioral AI engine on Windows devices that detects attacks that are initiated by remote devices.
Anti-Exploitation/Fileless	This is a behavioral AI engine focused on exploits and all fileless attack attempts, such as web-related and command line exploits.
Potentially unwanted applications	This is a static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.
Intrusion Detection	This is a behavioral AI engine on Windows devices focused on insider threats such as malicious activity through PowerShell or CMD.
DFI (Deep File Inspection)	This is a preventive static AI engine that scans for malicious files written to the disk.

DFI (Deep File Inspection) - Suspicious	This engine is a more aggressive static AI engine on Windows devices that scans for suspicious files written to the disk. When in Protect mode, this engine is preventive.
DBT (Dynamic Behavior Tracking) Executables	This is a behavioral AI engine that implements advanced machine learning tools. It detects malicious activities in real-time, when processes execute.

6. In the **ADVANCED SETTINGS** section, click **Manage Settings** and configure the following:

Device Configuration Options	Definition
Scan new agents	Enables a disk scan on the endpoint after installation. It runs a full disk scan using its Static AI engine, identifying any pre-existing malicious files and mitigating them based on the defined policy.
Anti Tamper	Does not allow end users or malware to manipulate, uninstall, or disable the client. Best practice is to keep this enabled.
Agent UI	Enables the SentinelOne client interface on the endpoint. This should be disabled by default as it is redundant with the Capture Client interface.
Snapshots	Sets Windows devices to keep Volume Shadow Copy Service (VSS) snapshots for rollback. If disabled, rollback is not available. Best practice is to keep this enabled.
Logging	Saves logs for troubleshooting and support. Best practice is to keep this enabled.

Trusted Certificate Policies

Trust Certificates is another agent Capture Client offers for protection. To view the Trusted Certificates policies, navigate to **Policies > Trusted Certificates**. The Trusted Certificates page shows trusted certificates parameters used in your environment.

To define a Trusted Certificate policy:

1. Log into the Client Management Console and select the appropriate scope to define a trusted certificate policy.
2. Disable inheritance if enabled.
3. Add or remove certificates in the **NATIVE OS TRUST** by enabling or disabling the **Windows Certificate Store** and or **macOS Keychain** options.
By default, Windows Certificate Store and macOS Keychain options are enabled by default.
4. Define Firefox support in the **FIREFOX BROWSER TRUST** section, if needed. Select from the following:
 - **Trust certificates in Firefox certificate store**
 - **Configure Firefox to trust OS certificate store**
 - **None**

5. To add certificates to the **ENFORCED CERTIFICATES** section, click **Upload Certificates**, browse the file, and click **Upload**.
6. Enable the switch if you want to **Retain trust when Capture Client is uninstalled**.
7. Click **Update**.

Web Content Filtering Policies

The ability to perform web content filtering has been added to Capture Client's policy management. You can configure policies that allow or block access to various websites. This allows endpoint security and content filtering to be managed from the same management console, simplifying administration. The feature also includes web-activity reporting for easier monitoring.

To Configure Web Content Filtering policy:

1. Navigate to **Policies > Web Content Filtering**.
2. Select appropriate scope from the Scope selector.
3. Enable **Enable Web Content Filtering** option.
4. Select the web categories that you wish to block from the protected devices that are associated with the web content filtering policy.
5. To perform advanced settings, click **Manage advanced settings**.
6. Do the following in the **ADVANCED SETTINGS** section:
 - a. To choose to rely on SonicWall Firewall, enable **Enforce behind SonicWall Firewall**.
By default, the option is disabled, hence Web Content Filtering is based on the configured web content filtering policy.
 - b. For websites that are blocked as per the policy, define the type of block page used:
 - **Use default block page**
 - **Define a custom block page**
To use a custom block page, click **Edit custom block page** and upload an HTML file by dropping it in the **BLOCK PAGE EDITOR** window, or select a file manually, and then click **Save changes**.
7. You can perform the following **Custom Settings** to set up the following:
 - **Allowed web domains** – To only allow the URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field.
 - **Forbidden web domains** – To block URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field.
 - **Forbidden URL Keywords** – To block URLs that contain the keywords you specify, add the keywords in the `Forbidden URL Keywords` field.
 - **Allowed process paths** – To only allow the paths that you specify, add the path in the `Allowed process paths` field.

8. Enable/disable these options as needed:
 - **Block all unauthorized processes**
 - **Enable Block request by default when category cannot be determined**
 - **Show notification when accessing a malware site**
 - **Force SafeSearch on supported search engines**
 - **Filter requests to localhost**
9. Click **Update** to save your changes.

Managing Blacklist

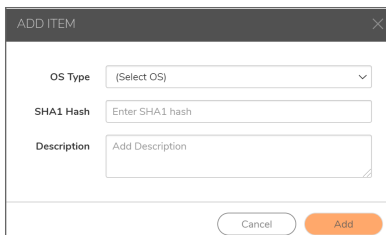
With the Blacklist feature you can choose to block known threats or unwanted files by curating a list of denied files.

- ❗ **NOTE:** The blacklist created at the Account scope is forced on the tenants and cannot be deleted. Although the blacklist for a tenant is inherited from the Account scope, you can still add items to the blacklist in addition to the ones that are inherited.

To set up the Blacklist:

1. Log into the Capture Client Management Console and select the appropriate scope to define blacklist at the selected scope.
2. Navigate to **Policies > Blacklist**.

❗ **NOTE:** When creating blacklists at the **Tenant** scope, the blacklists created at the account level are inherited by default. You can also create blacklist items for the tenant in addition to the ones that are inherited from the account.
3. Click **Create New**.



The screenshot shows a modal window titled "ADD ITEM" with a close button (X) in the top right corner. Inside the modal, there are three input fields: "OS Type" with a dropdown arrow, "SHA1 Hash" with a text input placeholder "Enter SHA1 hash", and "Description" with a text area placeholder "Add Description". At the bottom of the modal, there are two buttons: "Cancel" and "Add".

4. Select an operating system from the `OS Type` drop-down list.
5. Input a `SHA1 hash` for the file you wish to have blocked.
6. Add the `Description` in the field provided.
7. Click **Add**.

Exclusions

By using exclusions, you can whitelist various resources that Capture Client touches—both locally and remotely. This is particularly useful if you are experiencing false positives and you want to allow the resource or content to

access your device.

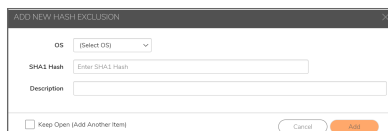
To navigate to Exclusions, select **Policies > Exclusions**. The screen is broken down into five tabs, which allows for more granular control of resources on your device:

- **Hashes**
- **Paths**
- **Signer Identity**
- **File Types**
- **Browsers**

Hashes

To add a Hash exclusion:

1. Navigate to **Policies > Exclusions**.
2. Select the **Hashes** tab.
3. Click **Create New**.



4. Enter the hash string in the `SHA1 Hash` field.
5. Choose the **OS** from the drop-down menu.
6. Add a `Description` in the field provided.
7. Click the Add button to save your exclusion.

Paths

You can exclude a specific location or file by defining a path on the device to a specific directory.

To exclude a path:

1. Navigate to **Policies > Exclusions**.
2. Select the **Path** tab.
3. Click **Create New**.
The **ADD NEW PATH EXCLUSION** dialog is displayed.
4. In the **OS** field, select an operating system from the drop-down list.
5. Enter the path to a directory or file in the `Path` field.
6. From the drop-down list in the **As** field, select one of the following: **File**, **Folder**, or **Folder and Subfolders**.

7. Select an Exclusion Mode. The options are defined below:

Exclusion Mode	Definition
Suppress Alerts	Does not display alerts on any of the processes.
Interoperability	Reduces the monitoring level of the processes, which may be needed for interoperability with some third party applications that may be running on your system (for example, CAD).
Interoperability—Extended	Reduces the monitoring level of the processes and their child processes.
Performance Focus	Disables monitoring of the processes associated with this path. You might select this option if monitoring these processes creates performance issues.
Performance Focus—Extended	Disables monitoring of the processes associated with a path and the child sub-processes. You might select this option if the parent and child processes together cause performance issues.

8. Click **Add**.

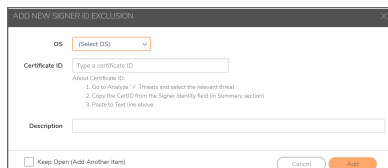
❶ **NOTE:** By clicking the **Keep Open** box, the ADD EXCLUSION window stays open after clicking Add. That way you can immediately define another exclusion if you want.

Signer Identity

You can exclude content from a particular publisher by using a Certificate ID.

To exclude a particular signer:

1. Navigate to **Threats** page and click on any threat to find the Signer Identity of the threat on SUMMARY section in the **Threat Details** page.
2. Copy the Signer Identity string.
3. Go to **Policies > Exclusions**.
4. Select the **Signer Identity** tab.
5. Click **Create New**.
6. Choose the **OS** from the drop-down menu.



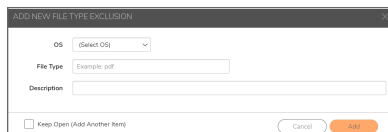
7. Paste the signer ID from Step 2 in the **Certificate ID** field.
8. Add a **Description**.
9. Click **Add**.

File Types

You can exclude specific file types from scanning.

To exclude particular file types:

1. Navigate to **Policies > Exclusions**.
2. Select the **File Types** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down list.



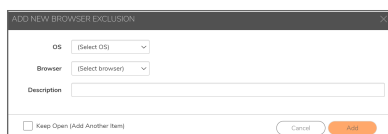
5. Enter the **File Type**.
6. Add a **Description**.
7. Click the **Add** button to save the exclusion.

Browsers

You can exclude a specific web browser from being checked for malicious content.

To exclude a specific browser:

1. Navigate to **Policies > Exclusions**.
2. Select the **Browsers** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down menu.



5. Select a **Browser** type from the drop-down list.
6. Add a **Description**.
7. Click **Add** to save the exclusion.

Replicating Policies

You can replicate custom policies (when it is not inherited or when inheritance is disabled) of any tenant and apply them to specified tenants. This feature helps you to apply a custom policy to multiple tenants easily.

To copy a policy from one tenant to other tenant:

1. Log into the Capture Client Management Console.
2. In the **Scope Selector**, select the tenant from which you wish to copy the policy.
3. Click **Policies** and select the policy that you wish to replicate.
4. Click **Copy to**.
5. Do the following In the **Copy To** page:
 - a. In the **All Tenants** section, select the tenants to which you wish to apply the selected policy.
① | **NOTE:** The tenants should not be inherited policies from its parent.

Copy To
🏠 / POLICIES / COPY TO

1 ✓ CLIENT POLICY 2 SELECT TENANT 3 SUMMARY

All Tenants

Search tenant... 🔍

<input type="checkbox"/>	TENANT NAME
<input type="checkbox"/>	Grannys Laundry-CC000001EEC1
<input type="checkbox"/>	RunningBird Vegetables-CC000001EEBF
<input type="checkbox"/>	SonicDemo Electronics-CC000001EE72
<input type="checkbox"/>	SWL Groceries-CC000001EEBD
<input type="checkbox"/>	Twisted Chocolates-CC000001EEC0

No tenants selected

Selected Tenants

Search tenant... 🔍

<input type="checkbox"/>	TENANT NAME
<input type="checkbox"/>	ACME inc-CC000001EE73
<input type="checkbox"/>	Coyote Meat & Fish-CC00000229FE

2 tenants added


Add ⇄ ⇄ Remove


Cancel View summary


- b. Click **Add** to add the tenants to the **Selected Tenants** list.
- c. Click **View summary**.


- d. Review the summary and click **Confirm**..

Copy To

 / POLICIES / COPY TO


CLIENT POLICY


SELECT TENANT


SUMMARY

Policy selected

Client Policy

Tenants/Groups selected

1 Tenants
[View details](#)

Policy copied from

SNWL Hardware Supplies-CC000001EE33

Back

Confirm

Group Ranking Policy




A device can be part of multiple groups depending on the rules associated with those groups. A device takes the policies of the group that is ranked higher than the other groups it belongs to. You have the ability to move group ranks higher and lower. In general, Dynamic groups are used for regular policy enforcement (for example: All Marketing Department users) and Static groups are used for exceptions (for example: Chief Marketing Office). So typically, Static groups would be ranked higher than Dynamic groups.

Creating Custom Policies for Device Groups

A newly created device group inherits the policies that are associated with the tenant under which the group is created; any changes to the policy at the tenant level are automatically propagated to the groups. You can also customize the policies associated with the group as required.

To customize the group policies:

1. Log into the Capture Client Management Console.
2. In the **Scope Selector**, select the appropriate tenant, and navigate to **Assets > Groups**.
3. Click the link displayed in **POLICY ASSIGNED** column for the group.

<input type="checkbox"/>	RANK	NAME	TYPE	CATEGORY	POLICY ASSIGNED	
<input type="checkbox"/>	#1	Test_group	Devices (0)	Dynamic	5/7 policies inherited from tenant	  
<input type="checkbox"/>	#2	Group 3	Devices (0)	Dynamic	0/7 policies inherited from tenant	
<input type="checkbox"/>	#3	Group 2	Users (0)	Static	0/7 policies inherited from tenant	
<input type="checkbox"/>	#4	te	Devices (0)	Dynamic	5/7 policies inherited from tenant	
<input type="checkbox"/>	#5	smp	Devices (0)	Dynamic	5/7 policies inherited from tenant	

- Update the policy as required and click **Update**.

Device Control

Capture Client allows you to control what USB devices can be connected to or are blocked from connecting to an endpoint. This feature can be used on both Windows and Mac devices.

Capture Client features a device control option that allows you to prevent data exfiltration and the malware threats from spreading via USB devices. USB devices are still a big source of malware threats spreading through an environment, and they are often used by insiders to steal sensitive data from an organization.

IMPORTANT: Device Control is only available via the Capture Client Advanced License and is supported with SentinelOne 2.8 Windows Agents and 2.7 macOS Agents.

Device Control lets you manage which external devices can be used with endpoints in your organization. It can be used at both the tenant level and at the policy level; each device control list is independent of the other. The policy device control takes precedence over the global device control. Use Device Control to:

- Block those external devices that are not required so data leaks are limited.
- Strictly control allowed devices to prevent malicious content from entering your network through external devices.

Protection

Endpoints are where data is created and where it is accessed from, so every endpoint connected to a network—whether it is a PC, a tablet, or a smartphone—is a point of vulnerability. With one compromised endpoint, an entire infrastructure can be compromised. The priority then is to get the endpoint protected and monitored by Capture Client.

Topics:

- [Tenant Token](#)
- [Migrating Clients Across Regions](#)
- [Protecting Devices](#)
- [Reviewing Registered Devices](#)
- [Active Users](#)
- [Performing System Scan](#)

Tenant Token

Tenant Token is required for installation or migration of clients effective Capture Client 3.8.0 release for Windows and macOS. For more information, refer to [Migrating Clients Across Regions](#).

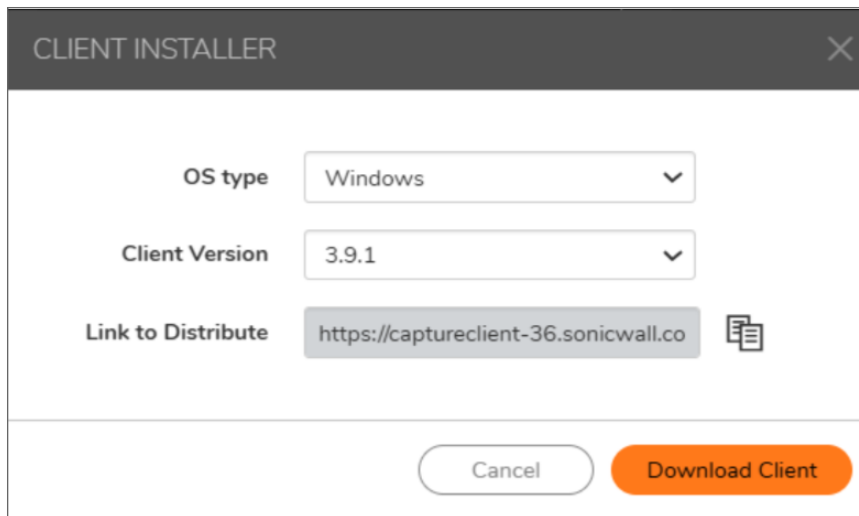
When an existing customer downloads the installer for the latest version, the notifications prompts them to copy the Tenant Token. Customers can copy and download the Tenant Token before proceeding with the installation process.

You can find the tenant token easily from the **Management settings** as described below.

To find the tenant token:

1. Navigate to **Management > Tenant Settings**. The **Basic Settings** page is displayed by default.
2. Scroll down to view the tenant details including Tenant ID, Name and Tenant Token.

2. The **Client Installer** page is displayed.



CLIENT INSTALLER

OS type Windows

Client Version 3.9.1

Link to Distribute <https://captureclient-36.sonicwall.co>

Cancel Download Client

3. Click on **Download Client** and **Save**.

The configuration file gets downloaded in Zip format, that also includes the tenant token, that is automatically picked during the installation process.

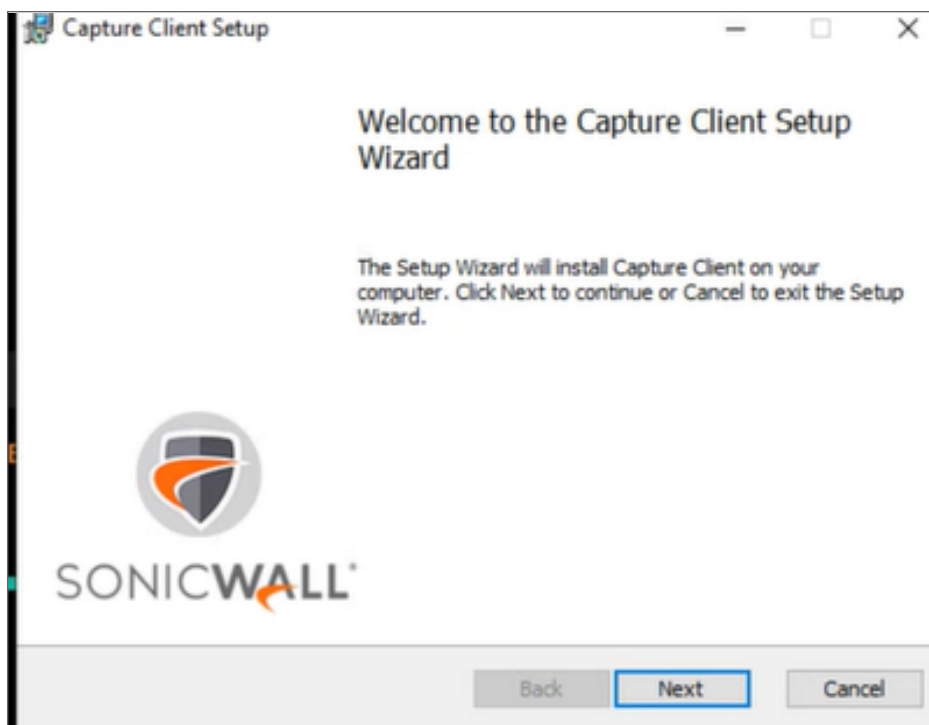
Installation for the New Clients

The new clients can run Capture Client with the help of a target tenant token.

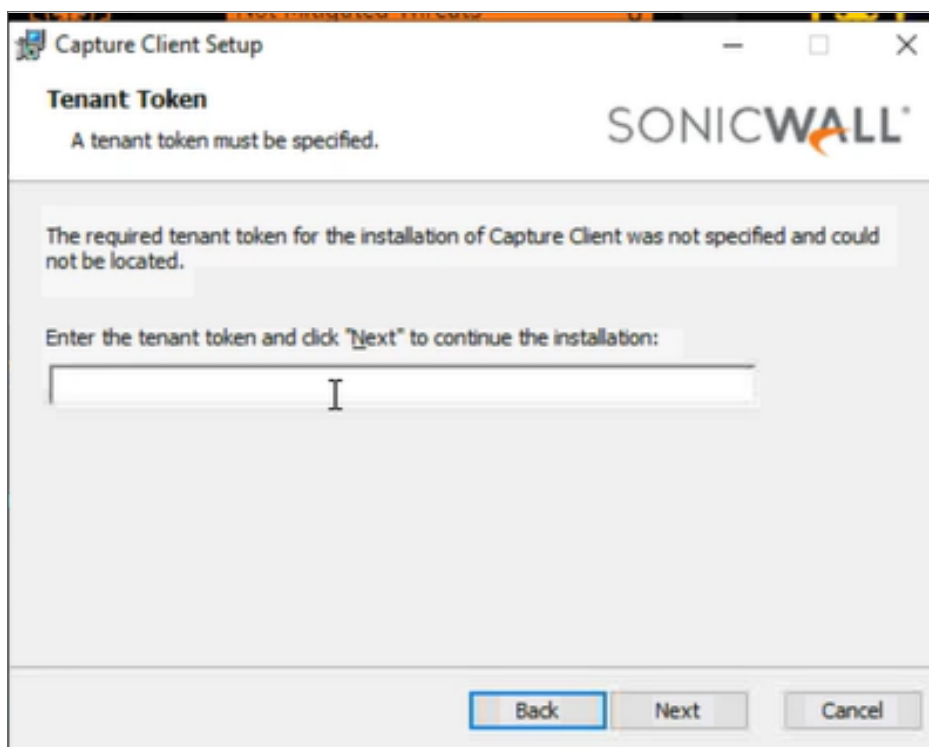
For pre-configured client installation, the Dashboard provides access to the Download links that can be used to download the clients for each OS type with choices for versions. We always recommend installing the latest General Release version. You can also copy the link to distribute the client via custom installation scripts or third-party platforms like software deployment tools and Remote Monitoring & Management tools.

To install the client:

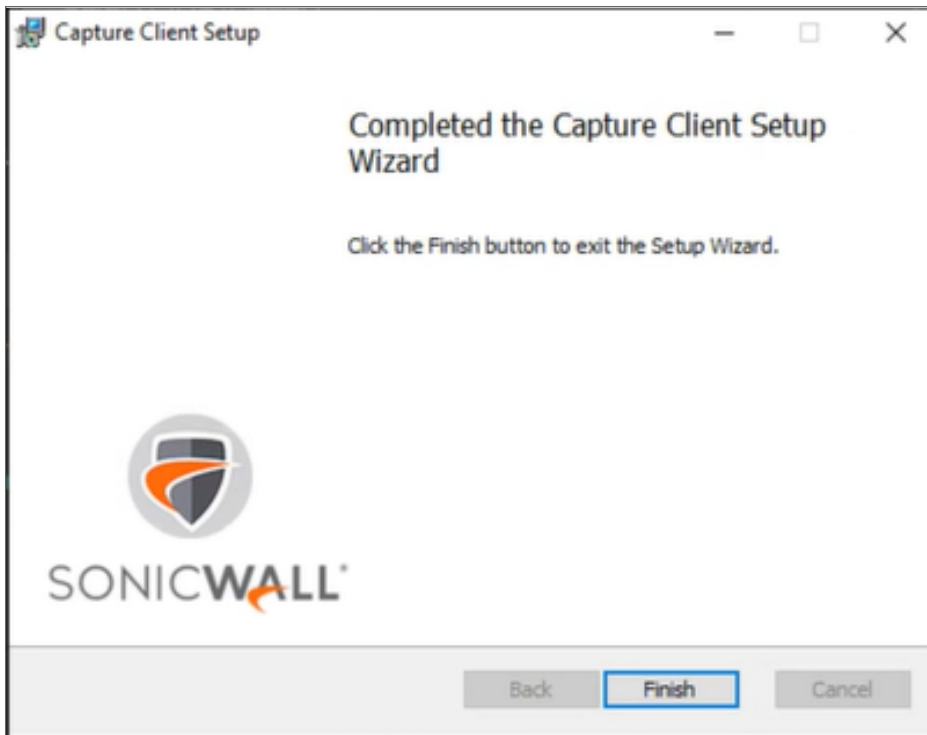
1. For the Pre-Configured Client installation, click on the **Download Client** link.
Alternatively, to install Capture Client on the blocked page, click **Install Capture Client** on the blocked page and click on the **Download Client** button.
NOTE: Blocked page installation is only available on Windows and macOS. A blocked page installation cannot be performed on devices running other operating systems. For more information, refer to the Capture Client Getting Started Guide on [technical-documentation](#).
2. After the installer file is downloaded, click **Run** to confirm you want to run the setup wizard.
3. Click **Next** to run the Capture Client Setup Wizard. The **Client Installer** window is displayed.



4. Accept the End User Licence Agreements and click **Next**. The Tenant Token window is displayed.



5. The **Tenant Token** is automatically picked from the installer file. Click **Next**. Wait till the installation is successful. If the installation is successful, click **Finish**. A small icon is loaded on your desktop tray and the endpoint dashboard displays.



① | **NOTE:** For more information on Tenant Token, refer to [Tenant Token](#).

① | **NOTE:** You can also do installation via command line interface. For more information, refer to the Capture Client Getting Started Guide on [technical-documentation](#).


Migrating Clients Across Regions

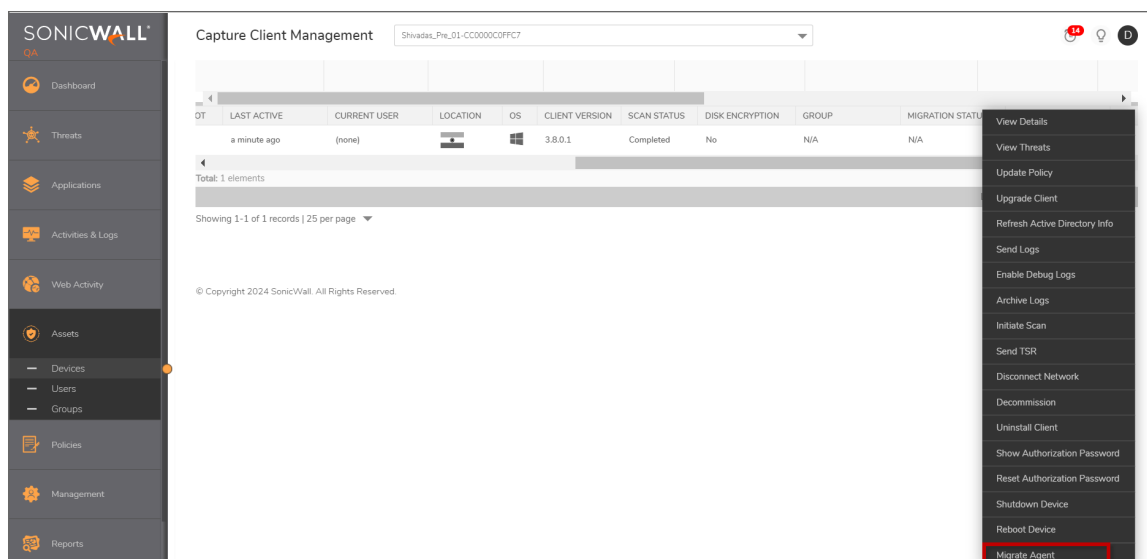
SonicWall partners using Capture Client, can seamlessly transfer or re-register the existing clients to a tenant in another data center (at different region) from the Management console, using the destination tenant token. This helps the existing clients to migrate across consoles (North America, Europe, MDR) without uninstalling and reinstalling Capture Client .

① | **IMPORTANT:** The migration feature works only on Capture Client 3.8.0 or the later versions. So, the Tenant Token option is not displayed for the older versions.

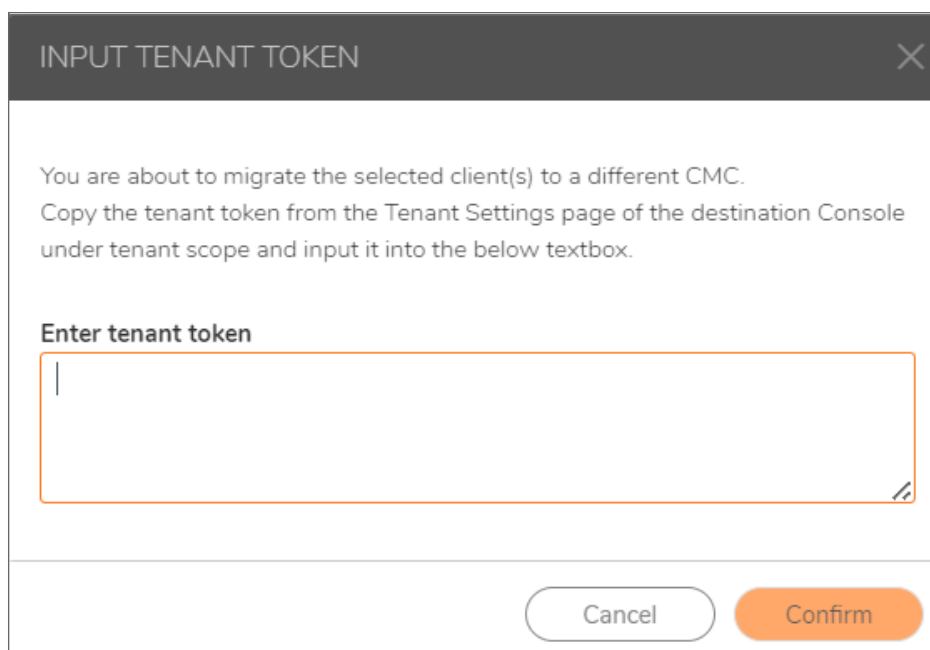
The migrate agent feature helps the existing customers who have tenants in one region to migrate their endpoints to another region.

To migrate agents for the existing clients:

1. Navigate to **Assets > Devices**.
2. From the **List View** tab, select the device for which you want to migrate the agents.
3. Click on the gear icon  on the right side. The actions that you can take on that particular endpoint are displayed.



4. Click on **Migrate Agent**. The **Input Tenant Token** Window is displayed.

The 'INPUT TENANT TOKEN' dialog box is shown. It has a title bar with a close button (X). The main text reads: 'You are about to migrate the selected client(s) to a different CMC. Copy the tenant token from the Tenant Settings page of the destination Console under tenant scope and input it into the below textbox.' Below this is a label 'Enter tenant token' followed by a large text input field. At the bottom right of the dialog are two buttons: 'Cancel' and 'Confirm'.

5. Enter the Tenant Token. This is the target tenant token for the new tenant on the destination console.

① | **NOTE:** To get the tenant token, navigate to **Management > Tenant Settings**. For more information, refer to [Tenant Token](#).

6. Click **Confirm**. The tenant is automatically migrated to the destination tenant on the destination console.

Protecting Devices

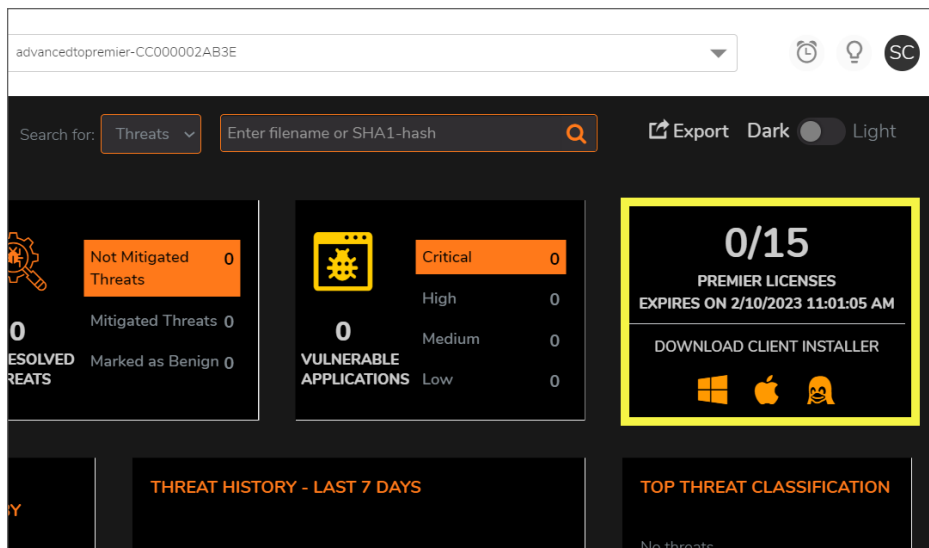
The individual devices can log into the Client Management Console and download the protection.

To set up device protection:

1. Navigate to the Client Management Console and log in with the appropriate credentials provided by your system administrator.
2. Select the appropriate tenant in the **Scope Selector** to add devices to the selected tenant.
3. On the **Dashboard** page, click an appropriate icon to download the required Capture Client installer. Installers are available for:

- **Windows**
- **macOS**
- **Linux**

① | **NOTE:** The Linux installer is available only for Capture Client version 3.0.x or later.



4. Select the appropriate **OS type** from the dropdown.
5. Click on the required **Download Client Installer**. The **Client Installer** pop-up window is displayed.

CLIENT INSTALLER

OS type: macOS

Client Version: 3.9.1

Link to Distribute: <https://captureclient-36.sonicwall.co>

Buttons: Cancel, Download Client

① **NOTE:** Only Capture Client 3.8.0 or future versions need to enter the tenant token. For more information, refer to [Migrating Clients Across Regions](#).

6. Copy the link from **Link to Distribute** box.
You can send this 'HTML link to download Client Installer' to users to download the client installer from any browser.
7. Click **Download Client**. This downloads the ZIP file containing the client installer and tenant token file.
8. Run the setup file and confirm you want the program to install the client agent on the device. If the installation is successful, a small icon is loaded on your desktop tray and the endpoint dashboard displays.

Reviewing Registered Devices

To see all the active clients (devices) associated with a configuration, navigate to **Assets > Devices**.

SONICWALL

Capture Client Management

Devices

Assets / DEVICES

View: List View | Unmanaged List View | Map

CAPTURE CLIENT	SENTINELONE	COMMISSIONED	NETWORK STATUS	PENDING ACTIONS	PENDING THREAT REBOOT	LOCATION	OS
<input checked="" type="checkbox"/> Online <input checked="" type="checkbox"/> Offline	<input checked="" type="checkbox"/> Online <input checked="" type="checkbox"/> Offline	<input checked="" type="checkbox"/> Commissioned <input type="checkbox"/> Pending Uninstall <input type="checkbox"/> Decommissioned	<input checked="" type="checkbox"/> Connected <input type="checkbox"/> Disconnected <input checked="" type="checkbox"/> Connecting <input type="checkbox"/> Disconnecting <input checked="" type="checkbox"/> Unavailable	<input type="checkbox"/> Attention needed <input type="checkbox"/> Missing Permissions <input type="checkbox"/> Incompatible OS <input type="checkbox"/> Unprotected <input type="checkbox"/> Agent Suppressed	<input checked="" type="checkbox"/> Yes <input checked="" type="checkbox"/> No		<input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Windows <input checked="" type="checkbox"/> Linux

Table with 1 row and 8 columns: CAPTURE CLIENT, SENTINELONE, COMMISSIONED, NETWORK STATUS, PENDING ACTIONS, PENDING THREAT REBOOT, LOCATION, OS.

Showing 1-1 of 1 records | 25 per page

To view the geographical locations of the devices, click **Map** tab on the **Assets > Devices** page.

A search function is provided at the top of the table so you can more easily find a specific device. Enter the search string in the field and the table immediately shows the results.

To see more details about the device, click on the device name.

The Alerts section displays events that need to be addressed; If there is any active threat in the device, a link to the threat is provided to investigate and respond.

OverviewNetworkProcessesApplicationsPoliciesEvents

Win10TechPubs02

VMware Virtual Platform

Windows 10 Pro (x86_64)

Commissioned

Activated

Online

ALERTS

The device requires a reboot to activate all policy engines.

DEVICE DETAILS

DEVICE INFO

CAPTURE CLIENT

Device Name

Win10TechPubs02

Device ID

C13A164D-22E6-C868-5886-3C28370F3F3C

Model

VMware Virtual Platform

Processor Type

x86_64

Device Type

Desktop

OS Version

Windows 10 Pro 10.0.19041.388

Last Active

less than a minute ago

Network Protection

SonicWall firewall not detected

Public IP Address

103.19.168.100

Console Visible IP Address

10.194.69.12

Local IP Address(es)

10.194.69.12

Ethernet0

127.0.0.1

Loopback Pseudo-Interface 1

MAC Address(es)

00-50-56-8B-63-DC

Ethernet0

Domain

WORKGROUP

Capture Client Version

3.5.13.3513

Install Token

E56C8448-18E5-433D-883E-884D8A1F0679

Authorization Password

Show

License Type

Capture Client Advanced

License Expiration

3/5/2030 3:47:36 PM (Expires in 9 years)

SentinelOne Agent Version

4.1.5.97

Disk Encryption

Off

Scan Status

In Progress (started 10/15/2020 1:22:17 PM)

Device Health


Healthy

Icon	Meaning
	Commissioned—Capture Client is installed and running on the device
	Red if Capture Client is not running on device.
	Green if network is connected.
	Red if network is disconnected.
	Grey if network status is unavailable.
	Orange if network is reconnecting.
	Purple if SentinelOne agent is online.
	Red if SentinelOne agent is Offline.
	Green if Capture Client on the endpoint is online.
	Red if Capture Client on the endpoint is offline.

List View

The **List View** tab on the **Assets > Devices** page, includes the following information for each devices being monitored:

- Identifier
- Name
- Status
- Commissioned
- Network Status
- Pending Actions
- Pending Threat Reboot
- Last Active
- Current User
- Location
- OS
- Client Version
- Scan Status
- Group
- Migration Status
- Migration Time Stamp

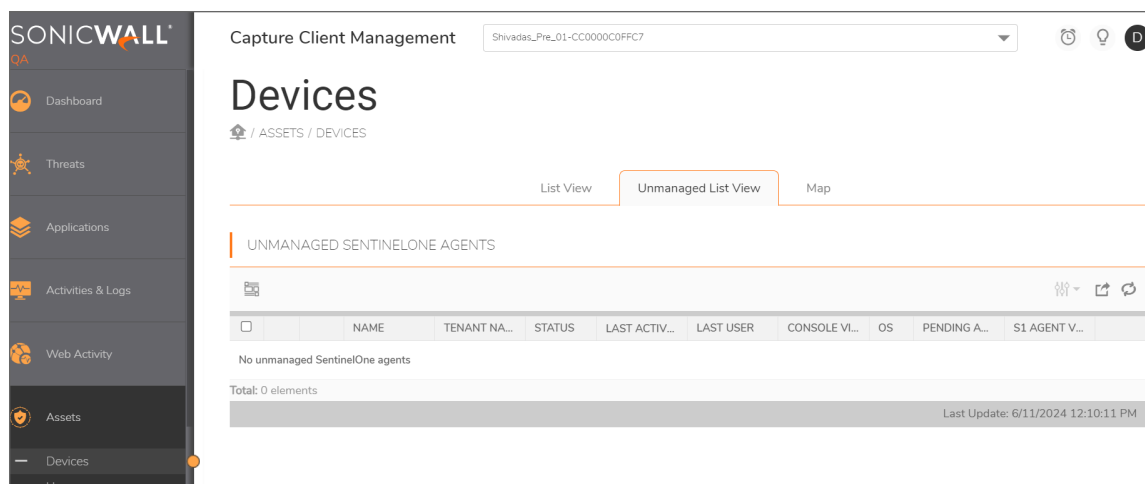
The options icon (gear icon - ) is visible on the right hand side, when you mouse over a particular device. The Options icon activates a drop-down list of actions you can take on that particular endpoint.

Option	Description
View Details	Expands the devices so that all the details about it are visible.
View threats	Lists threats in that device if any.
Update Policy	Updates the Capture Client policy on the device.
Upgrade Client	Provides option to upgrade the Capture Client version and threat protection client on the endpoint as per the Capture Client policy associated with the device or any available later versions of Capture Client. Make sure to review the system requirements for endpoint before performing a client version upgrade.
Refresh Active Directory Info	Refreshes the Active Directory information.
Send Logs	Requests that the logs from that client be sent for analysis.
Enable Debug Logs	Enables the debug logs on that client device.

Option	Description
Archive Logs	Archives and removes the debug or regular log files.
Initiate Scan	Initiates a scan of that client device.
Send TSR	Requests a Tech Support Report from that device.
Disconnect Network	Blocks the connection between the client device and the network.
Decommission	Decommissions the device and removes it from management console. When the device comes online subsequently, it registers again and shows up on the console.
Uninstall Client	Uninstalls Capture Client from the device.
Show Authorization Password	Displays a password that can be sent to the end user so the user can uninstall the client on their device.
Reset Authorization Password	Resets the uninstall password for a device.
Shutdown Device	Shuts down the client device.
Reboot Device	Reboots the device
Migrate Agent	Migrates the clients to a separate CMC. For more information, refer to Migrating Clients Across Regions


Unmanaged List View

The **Unmanaged List View** tab on the **Assets > Devices** page helps to view the list of unmanaged SentinelOne agents.



It includes the following information for each devices being monitored:

- Name
- Tenant Name
- Status
- Last Active
- Last User
- Console Visible IP
- OS
- Pending Actions
- S1 Agent Version

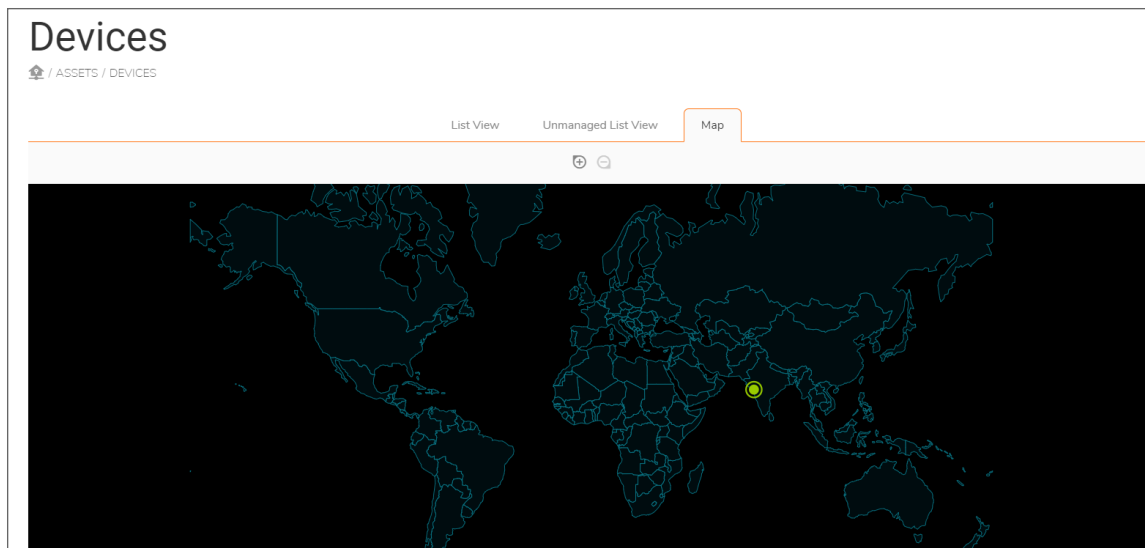
The options icon (gear icon - ) is visible on the right hand side, when you mouse over a particular device. The Options icon activates a drop-down list of actions you can take on that particular endpoint.

Option	Description
Decommission	Decommissions the device and removes it from management console. When the device comes online subsequently, it registers again and shows up on the console.
Uninstall Client	Uninstalls Capture Client from the device.
Show Authorization Password	Displays a password that can be sent to the end user so the user can uninstall the client on their device.
Initiate Scan	An initiate scan command is sent to the client.

You can also download export the list of unmanaged devices clicking on .

Map

The **Map** tab on the **Assets > Devices** page, helps to view the geographical locations of the devices.



Hover the mouse over the countries and click on the green icon to view devices and their details.

DEVICES NEAR MANOR, IN

MANOR

	NAME	STATUS	LAST ACTIVE	CONSOLE VISIBLE IP	OS
	ShivadaRestoreUtility003		3 minutes ago	49.249.49.243	
	sonicwall-virtual-machine		9 days ago	49.249.49.243	

Close

Active Users

To see all the active users associated with a configuration, navigate to **Assets > Users**.

Users				
ASSETS / USERS				
<div> <div></div> <div></div> <div></div> </div>				
	USERNAME	FULL NAME	DEVICE(S)	GROUP(S)
▶	CAPTURECLIENTQAAdministrator	CAPTURECLIENTQAAdministrator	Win10-Georgy.captureclientqa.local	No groups
▶	CAPTURECLIENTQAsonicwall	CAPTURECLIENTQAsonicwall	Win10-Georgy.captureclientqa.local	User_grp_2
▶	WIN10-32-GEORGYsonicwall	WIN10-32-GEORGYsonicwall	Win10-32-Georgy	No groups
▶	WIN10-GEORGYsonicwall	WIN10-GEORGYsonicwall	Win10-Georgy.captureclientqa.local	User_Group_1
▶	WIN10TECHPUBS02admin	WIN10TECHPUBS02admin	Win10TechPub02	No groups

A search function is provided at the top of the table so you can more easily find a specific user. Enter the search string in the field and the table immediately shows the results.

The simple view (default) of the **Users** list includes the following information for each user being monitored:

- User name
- Full Name
- Device(s)
- Group(s)

To see more detail about a user, click on the arrowhead on the left to expand the selection and see more details.

Performing System Scan

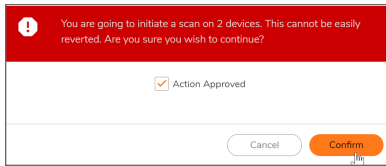
To perform the system scan on a device or a group of devices:

1. Hover over any device, click the gear icon that appears, and select **Initiate Scan**.
Initiate scan command is sent to the device. Skip the remaining steps.
2. To perform the system scan on a group of devices, do one of the following:
 - Navigate to **Assets > Devices**, select the devices on which you want to perform a scan, click the gear icon , and then click **Initiate Scan**.
 - To perform system scan on all the devices associated with a tenant, navigate to **Assets > Devices**, click the gear icon , and then click **Initiate Scan**.

Devices									
ASSETS / DEVICES									
<div> <div></div> <div></div> <div></div> </div>									
<div> <div>List View</div> <div>World Map</div> </div>									
	NAME	STATUS	LAST ACTIVE	CURRENT USER	CONSOLE VISIBLE IP	LOC...	OS	CLIENT VERSION	
▶	Win10TechPub02	✔️ 🟢	less than a minute ago	(none)	10.184.69.12		Windows	3.5.13	⚙️
▶	Win10-Georgy.captureclientqa.local	✔️ 🟢	less than a minute ago	CAPTURECLIENTQAsonicwall	10.5.156.12		Windows	3.5.14	⚙️
▶	Win10-32-Georgy	❌ 🟡	a day ago	WIN10-32-GEORGYsonicwall	10.5.155.237		Windows	3.5.13	⚙️
Total: 3 elements									

3. Select **Action Approved** and click **Confirm** in the below prompt.

NOTE: After you confirm, you cannot cancel scan for all the devices at once and should be done individually.



After the system scan is initiated on a group of devices, the scan status of each of the devices is independent of each other. It is recommended that you disable disk-scan notifications before initiating group scan for a group with a large number of devices to avoid email spamming.

Groups

In some cases, you may want to associate a policy to a group of users or devices rather than an individual or an entire organization. Capture Client makes the distinction between static groups (which contains a static list of devices or users) and dynamic groups (where devices are added or removed based on rules). For example, you may want a policy applied to all incoming traffic going to your sales team and no one else in your organization. If you want to apply a policy to particular group, you first have to create a group.

A newly created device group inherits the policies that are associated with the tenant under which the group is created; any changes to the policy at the tenant level are automatically propagated to the groups. You can then disable inheritance and customize the policies as required. For information on creating custom policies for groups, see [Creating Custom Policies for Device Groups](#).

To see all the active groups associated with a configuration, navigate to **Assets > Groups**. Groups are broadly classified into two types: **DYNAMIC GROUPS** and **STATIC GROUPS**.

- **DYNAMIC GROUPS** are groups where devices are added or removed automatically based on policy rules.
- **STATIC GROUPS** lists are static assignments managed by an administrator manually and not by any rule dynamically. Static groups are further classified as Static Device Groups and Static User Groups.
 - **Static Device Groups**—Groups created by selecting devices
 - **Static User Groups**—Groups created by selecting users

Topics:

- [Creating a Static User Group](#)
- [Creating Static Device Groups](#)
- [Creating Dynamic Device Groups](#)
- [Creating Custom Rules for Dynamic Groups](#)

Creating a Static User Group

To create a new static user group:

1. Log into the Capture Client Management Console.
2. In the **Scope Selector**, select the appropriate tenant in which you wish to create a static user group.
3. Navigate to **Assets > Groups**.
4. Click **+** at the upper-right corner of table.
5. Type the **Group Name** in the field provided.

Create New Group

HOME / ASSETS / GROUPS / CREATE NEW GROUP

1 GROUP DETAILS 2 ADD DEVICES/ RULES 3 SUMMARY 4 POLICY REVIEW

Group Name: Test

Group Type: Device Group, User Group (selected)

Group Category: Dynamic, Static (selected)

Static groups are based on manual selection. Agents in a static group that match the filters of a dynamic group are automatically moved to the dynamic group.

Cancel Next

6. Select **Static** as **Group Category** and **User Group** as **Group Type**.
7. Click **Next**.
8. Select users from **All users** section and click **Add**.

Create New Group

ASSETS / GROUPS / CREATE NEW GROUP

✓

GROUP DETAILS

2

ADD DEVICES/ RULES

3

SUMMARY

4

POLICY REVIEW

All users

Search device or user...

USER NAME

☒ Win10TechPubs02
WIN10TECHPUBS02admin

☐ Win10-32-Georgy
WIN10-32-GEORGYYasnicwall

☐ Win10-
George.captureclient@qa.local
CAPTURECLIENTQAAdministrator

Add ➡

⬅ Remove

1 users selected

Selected users

Search device or user...

USER NAME

No Users

No users selected

Back

Next

9. Review **Selected users** section to verify the users that you want to be part of the user group.
To remove users from the list, select user(s) and then click **Remove**.
10. Click **Next**.
11. Review the summary of the user group being created.
You can click Edit to go back to the last screen and modify users of the group.

Create New Group

ASSETS / GROUPS / CREATE NEW GROUP

✓

GROUP DETAILS

✓

ADD DEVICES/ RULES

3

SUMMARY

4

POLICY REVIEW

Group Name

Test

Group Type

User Group

Group Category

Static

Selected Users

Win10TechPubs02

WIN10TECHPUBS02admin

✕

Edit

Back

Confirm

12. Click **Confirm**.
13. Click **Done** or click **Take me to policies** to review the policies inherited from the tenant and customize policies if required.

Create New Group
 / ASSETS / GROUPS / CREATE NEW GROUP

GROUP DETAILS ADD DEVICES/ RULES SUMMARY 4 POLICY REVIEW

All the policies are inherited from "BlrQATwo_Tenant_1".
 You can choose to review the policies immediately.
[Take me to policies](#)

The group "Test" has been created successfully.
 You can create new groups to apply custom policies.
[Create new Group](#)

Done

Creating Static Device Groups

To create a new static device group:

1. Log into the Capture Client Management Console.
2. In the **Scope Selector**, select the appropriate tenant in which you wish to create a static device group.
3. Navigate to **Assets > Groups**.
4. Click **+** at the upper-right corner of table.
5. Type the **Group Name** in the field provided.

Create New Group
 / ASSETS / GROUPS / CREATE NEW GROUP

1 GROUP DETAILS 2 ADD DEVICES/ RULES 3 SUMMARY 4 POLICY REVIEW

Group Name

Group Type

Device Group User Group

Group Category

Dynamic Static

Static groups are based on manual selection. Agents in a static group that match the filters of a dynamic group are automatically moved to the dynamic group.

Cancel Next

6. Select **Group Category** as **Static** and **Group Type** as **Device Group** .
7. Click **Next**.

8. Select devices from **All devices** section and click **Add**.

Capture Client Management basic tenant-CC000002AB4E

Create New Group

ASSETS / GROUPS / CREATE NEW GROUP

1 GROUP DETAILS 2 ADD DEVICES/ RULES 3 SUMMARY 4 POLICY REVIEW

Rule 1

(select criterion) (select operation) reference value X ✓ +

Back Next

9. Review **Selected devices** section to verify the devices that you want to be part of the device group. To remove users from the list, select user(s) and then click **Remove**.
10. Click **Next**.
11. Review the summary of the user group being created. You can click **Edit** to go back to the last screen and modify users of the group, if anything is incorrect.

1 GROUP DETAILS 2 ADD DEVICES/ RULES 3 SUMMARY 4 POLICY REVIEW

Group Name Device_Group_1

Group Type Device group

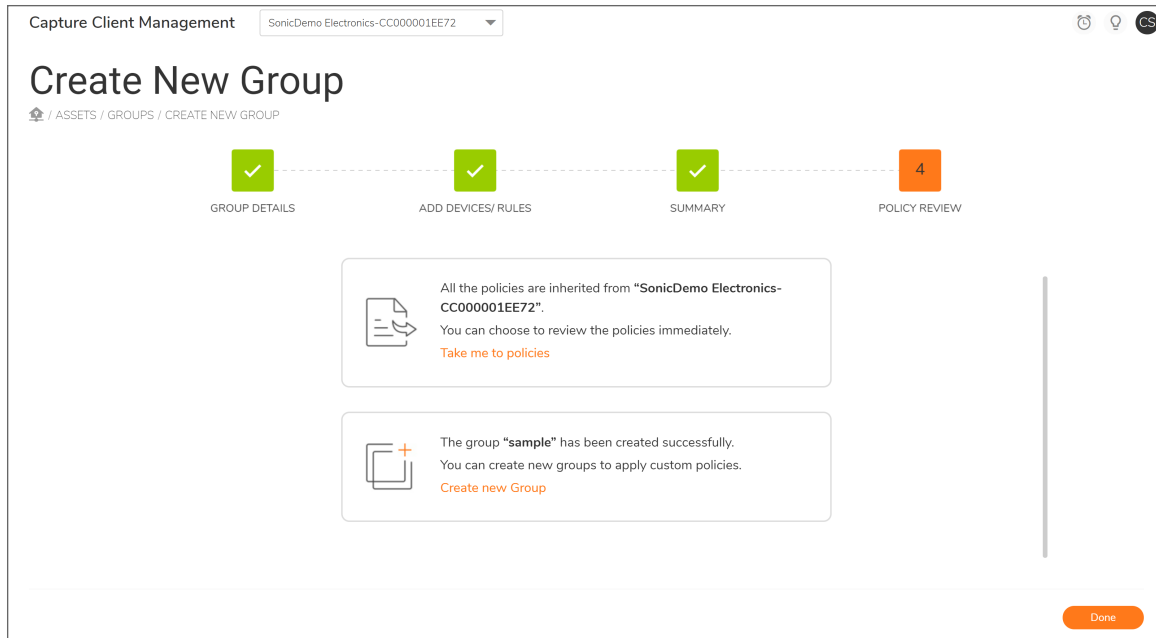
Group Category Static

Selected Devices

Win10-Georgy.captureclientqa.local Edit

Back Confirm

12. Click **Confirm**.
- To review the policies associated with the group, click **Take me to policies** . You can also configure the custom policies for the group, see [Creating Custom Policies for Device Groups](#). Otherwise go to step 13.



13. Click **Done**.

Creating Dynamic Device Groups

To create a new static device group:

1. Log into the Capture Client Management Console.
2. In the **Scope Selector**, select the appropriate tenant in which you want to create a group.
3. Navigate to **Assets > Groups**.
4. Click **+** at the upper-right corner of table.
5. Type the `Group Name` in the field provided.

Create New Group

🏠 / ASSETS / GROUPS / CREATE NEW GROUP

1

2

3

4

GROUP DETAILS

ADD DEVICES/ RULES

SUMMARY

POLICY REVIEW

Group Name

Group Type

Device Group

User Group

Group Category

Dynamic

Static

Dynamic groups are based on filters. Agents that match criteria of the filters are automatically added to the group.

Cancel
Next

6. Select **Group Category** as **Dynamic** and **Group Type** as **Device Group** .
 7. Click **Next**.
 8. In the **ADD DEVICES/RULES** page, you can add rule (s) for the device group being created.
- 📘 | **NOTE:** You can add multiple rules for a group if needed.

These are the criteria available for creation of a rule:

- Device ID
- Device Name
- Device Type
- Hardware Model
- Processor Type
- OS Name
- OS Type
- OS Version
- Public IP
- Console Visible IP
- Local IP
- MAC Address
- Capture Client Version
- Computer Distinguished Name
- Last User Distinguished Name
- ActiveDirectory Group for Computer

- ActiveDirectory Group for Computer
- Current Country
- Current City

Create New Group

ASSETS / GROUPS / CREATE NEW GROUP

✓

GROUP DETAILS

2

ADD DEVICES/ RULES

3

SUMMARY

4

POLICY REVIEW

All devices

Search device...

DEVICE NAME

☒ Win10-32-Georgy
 ☐ Win10-Georgycaptureclientga.local
 ☒ Win10TechPubs02

2 devices selected

Selected devices

Search device...

DEVICE NAME

No Devices

No devices selected

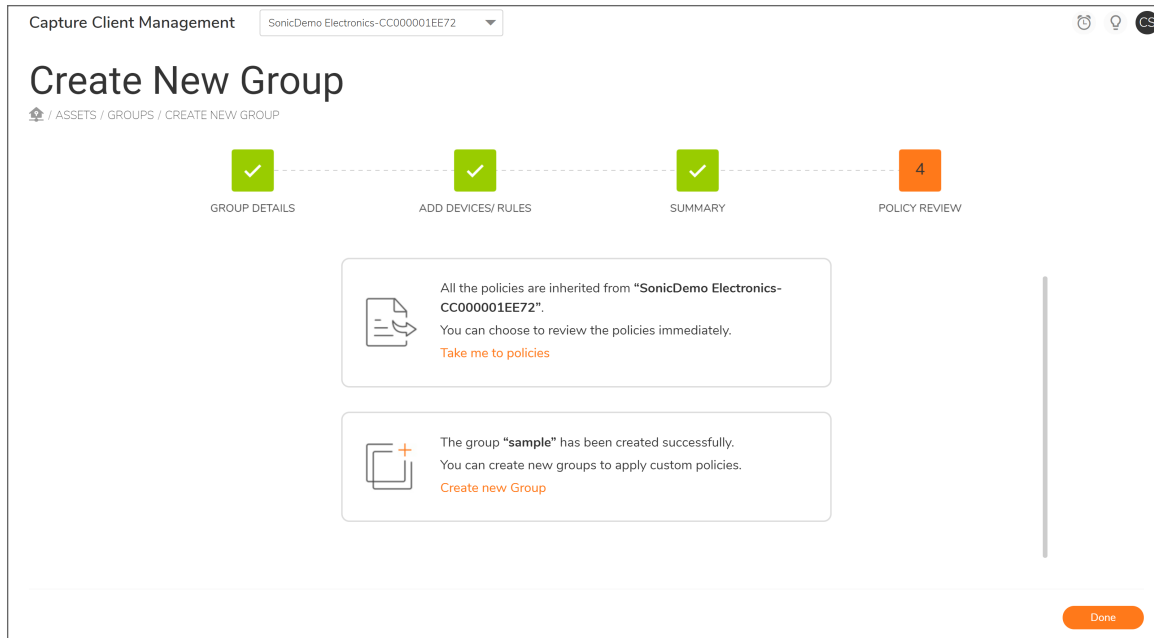
Add →

← Remove

Back

Next

- Review the summary of the device group being created and select the **Assignment Mode**.
You have options to Edit, Remove, or Add rules on this page.
- click Confirm.
To review the policies associated with the group, click **Take me to policies** . You can also configure the custom policies for the group, see [Creating Custom Policies for Device Groups](#). Otherwise go to step 11.



11. Click **Done**.

Creating Custom Rules for Dynamic Groups

When creating Dynamic Groups, the custom rules were enhanced to add the operating system version, including Windows Server versions, and the Capture Client version. You can also use operators to set the version levels to be greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=) the full OS version. With this capability, you can create flexible rules specific to operating system levels.

To set custom rules:

1. Navigate to **Assets > Groups**.
2. Click **+** to add a Dynamic Group.
3. Create the group by providing a **Group Name**.
4. Select **Group Category** as **Dynamic** and **Group Type** as **Device Group**.
5. Click **Next**.
6. Choose the **criterion** and then select the **operation** for the rule.

① | **NOTE:** Active Directory Integration with Capture Client 3.0 and above you can to create custom rules for Active Directory User Group and Active Directory Device Group.

Create New Group

ASSETS / GROUPS / CREATE NEW GROUP

✓

2

3

4

GROUP DETAILSADD DEVICES/ RULESSUMMARYPOLICY REVIEW

Rule 1

OS Version

(select criterion)
Device ID
Device Name
Device Type
Hardware Model
Processor Type
OS Type
OS Name
OS Version
Public IP
Console Visible IP
Local IP
MAC Address
Capture Client Version
Computer Distinguished Name
Last User Distinguished Name
ActiveDirectory Group for Computer
ActiveDirectory Group for User
Current country
Current city

=

reference value

X

✓

+

7. Add a `reference value` and click the right check mark.
8. Click **+**, next to the newly created rule to add more rules, and click **Next**.

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 Protecting Assets with Security Policies Administration Guide

Updated - December 2024

232-005517-00 Rev F

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