Capture Client

Getting Started Guide

SONICWALL®

Contents

1

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 documents describes how to set up a Capture Client environment.

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

- Description
- Getting Started with Capture Client
- 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 360º 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.

Getting Started with Capture Client

This document outlines the key steps involved in getting your Capture Client subscription up and operational for your environment. At a high level, the following steps are recommended:

Topics:

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.
`Computer code`	Indicates sample code or text to be typed at a command line.

<Computer code italic>	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.
Italic	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.

2

Preparation

Before provisioning your Capture Client subscription, take the time to prepare for your deployment.

1. **Review system requirements**

   Capture Client is a comprehensive endpoint security solution that protects Windows, Linux, and macOS devices. It is administered from the SonicWallClient Management Console, a cloud service requiring only a web browser and an internet connection. To get maximum performance and protection, evaluate the detailed system requirements which are outlined in the *Capture Client 3.10 Release Notes*. The key parameters are:

   - Minimum hardware requirements
   - Supported operating systems
   - Installation notes

2. **Identify interoperability issues**

   Some software applications are known to have interoperability issues with Capture Client and SentinelOne. You can work around these issues by creating an exclusion and pushing it to the clients. Refer to Capture Client Inter-Operability With Third Party Applications for more information.

3. **Plan a pilot rollout**

   If you have a complex environment, with critical business operations and a diverse set of users, you should execute a pilot rollout, sampling one or two endpoints from various groups. This can help eliminate issues and reduce helpdesk tickets when rolling out to all users. Refer to Best Practices for a Pilot Exercise for more information.

4. **Verify your MSW account**

   Access to MySonicWall is required for many of the steps while setting up your Capture Client system. If you do not already have an MySonicWall account follow the steps in How Do I Create a MySonicWall Account? to set one up.

3

Activation

Once you have decided to provision Capture Client to your environment, you need to activate the subscription to get access via Capture Security Center and to setup the clients to be rolled out. Follow the procedures given below to activate the subscription:

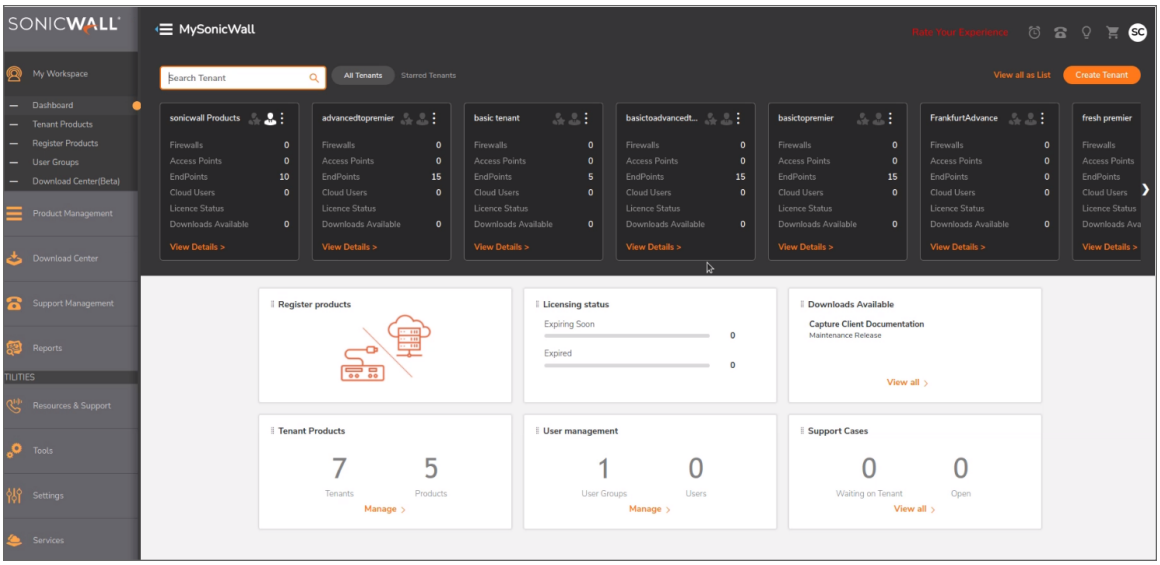
1. To create a tenant where your subscription is activated, refer to Creating Your Tenant .
2. To license or activate the Capture Client software in Licenses, refer to Activating the Capture Client .
3. To attach to a SonicOS firewall, refer to Attaching to a SonicOS Firewall.
4. To launch the management console, refer to Launching the Management Console.

Creating Your Tenant

To add a tenant in MSW:

1. Click on **Login with Capture Client Management account** and enter your MySonicWall credentials.
2. Click on **Login**.

3. Navigate to **My Workspace > Dashboard**.



4. To create a tenant, Click **Create Tenant**.
5. Enter a name in `New tenant` box and click the check mark next to the field.

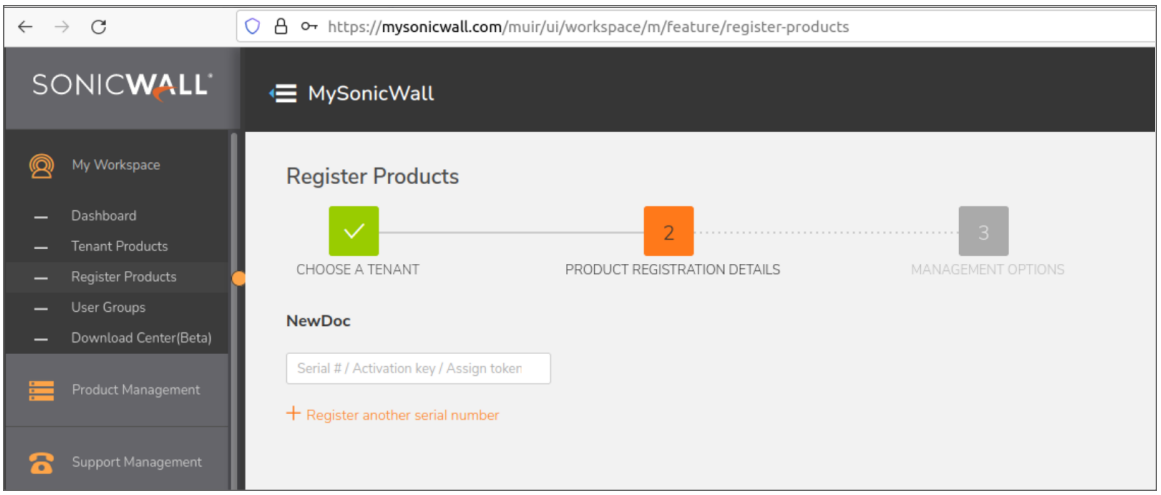
6. The User Group is added by default. You can add users to the tenant and assign permission to the users. Refer to the MSW online help if you need more detail.

Activating the Capture Client

Once you create a tenant, you need to activate the subscription that provisions the instance in the cloud and gets you started:

1. Navigate to **My Workspace > Register Products**.
2. Select the tenant that you want to activate Capture Client in.

3. Enter the Capture Client **Activation key** and **Friendly Name**.



4. Click on the **Choose Management Options** link.
5. In the **Management Options** tab, select the Data Center from the drop down.

   ⓘ **NOTE:** When you select the data centre, the Capture Client instance is configured with SentinelOne and SonicWall Capture ATP servers from that geographic location.
6. Click **Done**.

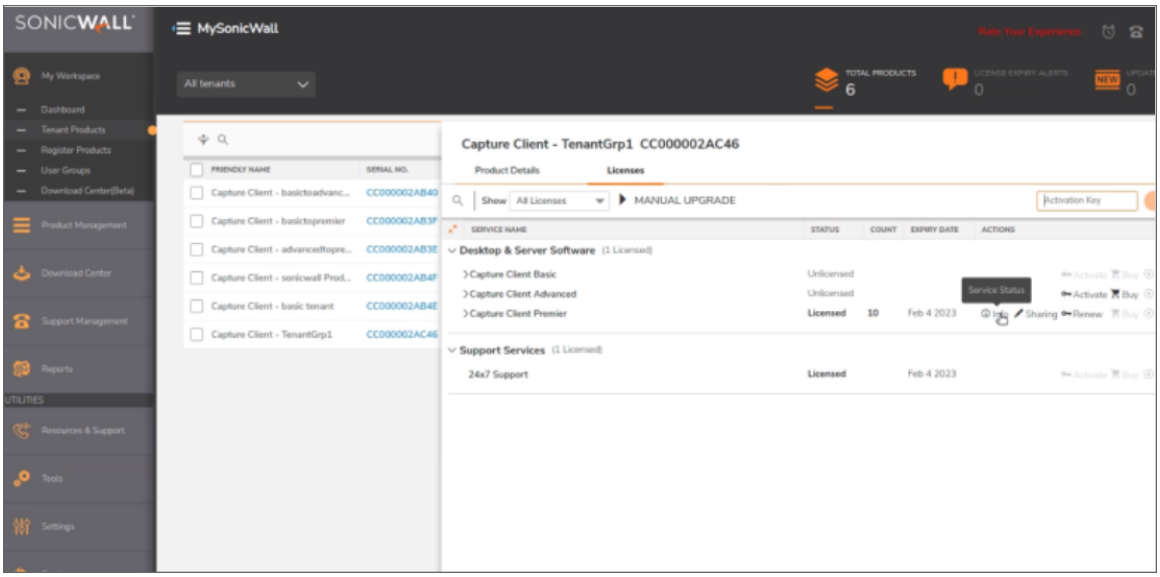
   Once complete, you are redirected to the **My Workspace -> Tenant Products** page, which shows the subscription you just activated.

Attaching to a SonicOS Firewall

Attaching your Capture Client subscription to a SonicOS firewall allows you to enable the Client Enforcement service on your firewall. Refer to the appropriate SonicOS Administration Guide for more details on how you can use enforcement to ensure compliance of endpoints on your network. With this you can also gain endpoint visibility and telemetry that can be used in policies.

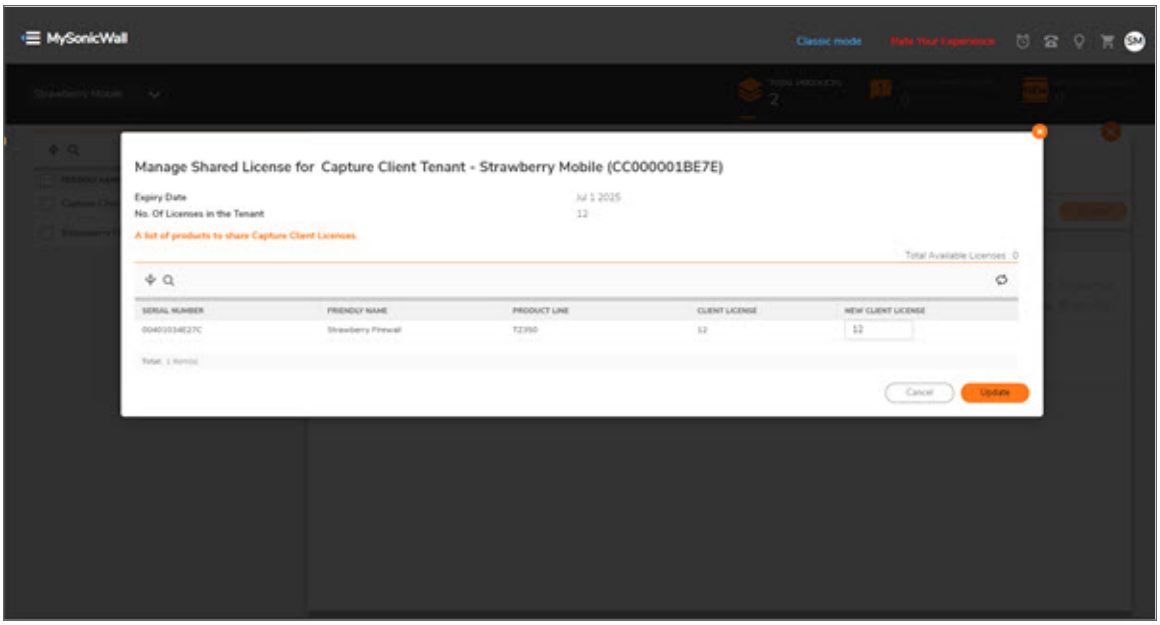
1. Navigate to **My Workspace > Tenant Products**.
2. Edit the Capture Client subscription.

3. Click on **Licenses** tab and click the button labeled **Sharing**.



4. On the popup window, distribute your license as required among the firewalls that you see.

   ⓘ | **NOTE:** Only firewalls registered with the same tenant can be attached to the subscription.

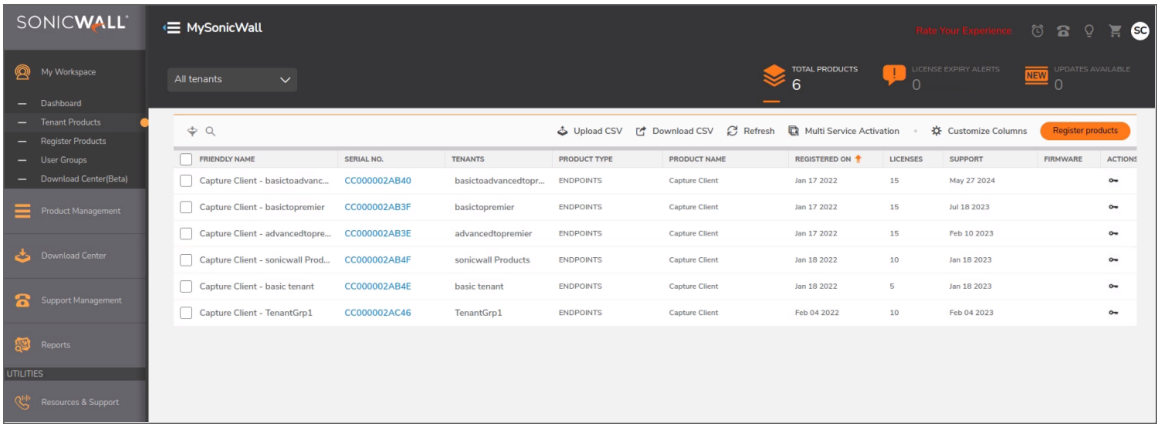


5. Click **Update** to complete the attachment and enable the Enforcement Service on the firewall.

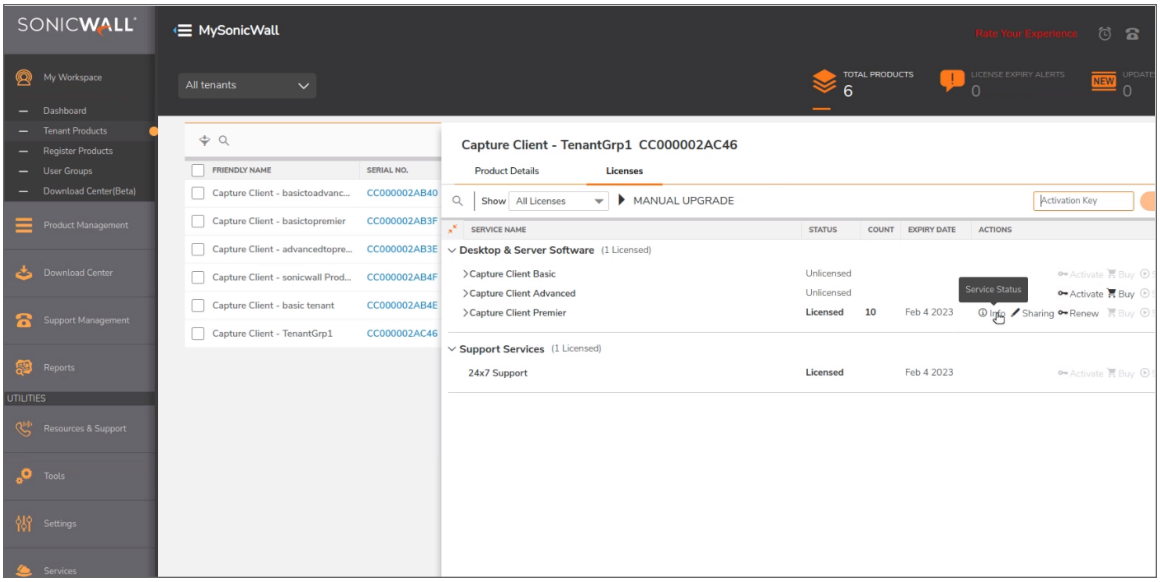
Launching the Management Console

To launch the Capture Security Center and get access to the Client Management Console, one can navigate to **cloud.sonicwall.com** and login with your MySonicWall credentials. Or, you can single-sign on to the console directly from MySonicWall as follows:

1. Navigate to **My Workspace -> Tenant Products**.

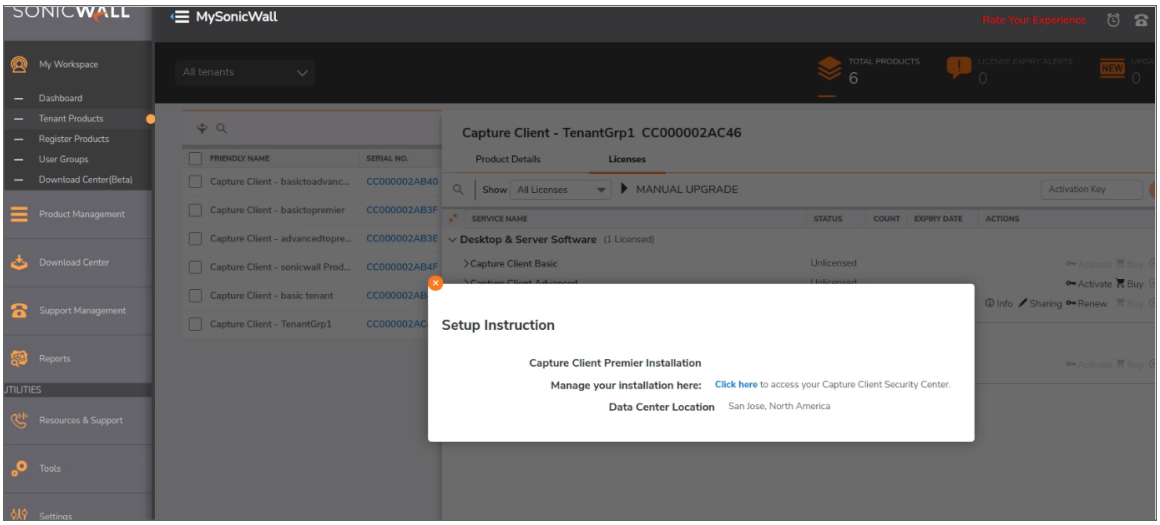


2. To edit the subscription you need to manage, click on the tenant serial number from the **All Tenants** option.
3. Click on the **Licenses** tab.

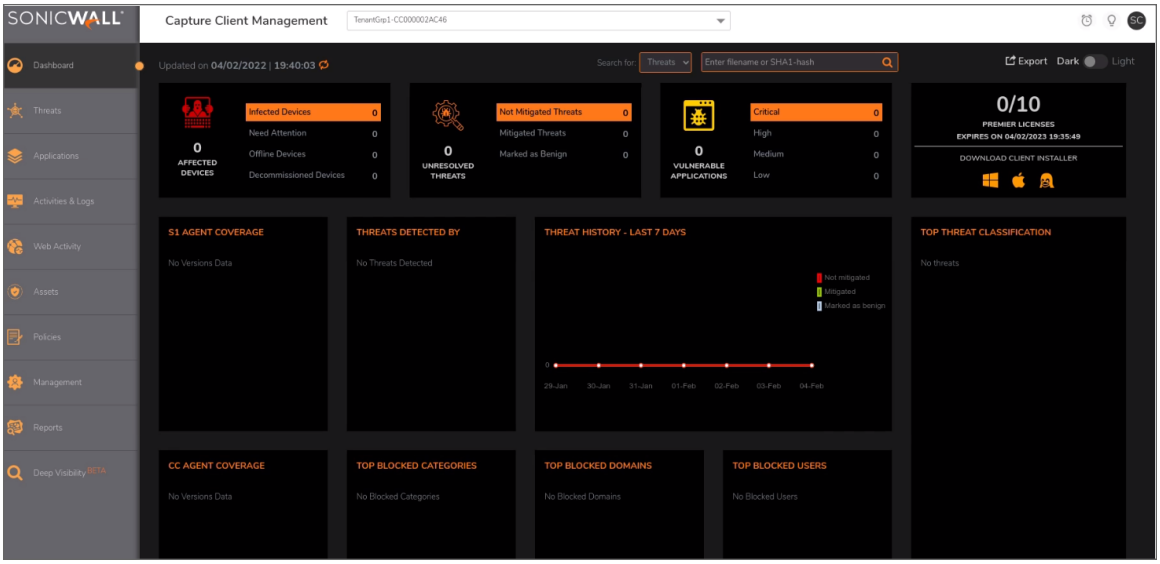


4. Click **Info**.

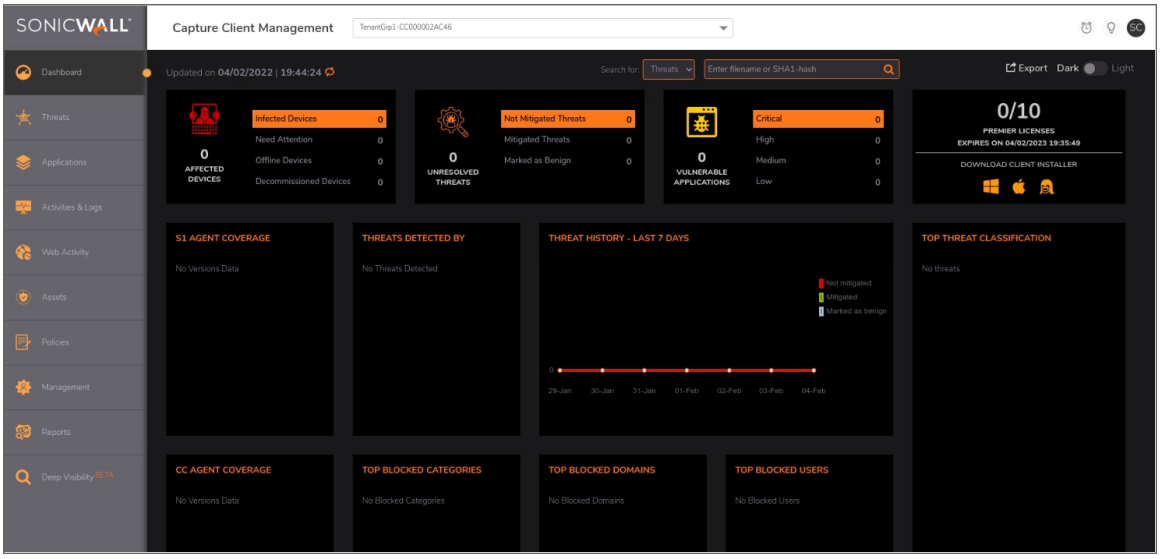
5. Click on the management link **Manage your installation here: Click here**, to launch the console in a new tab.



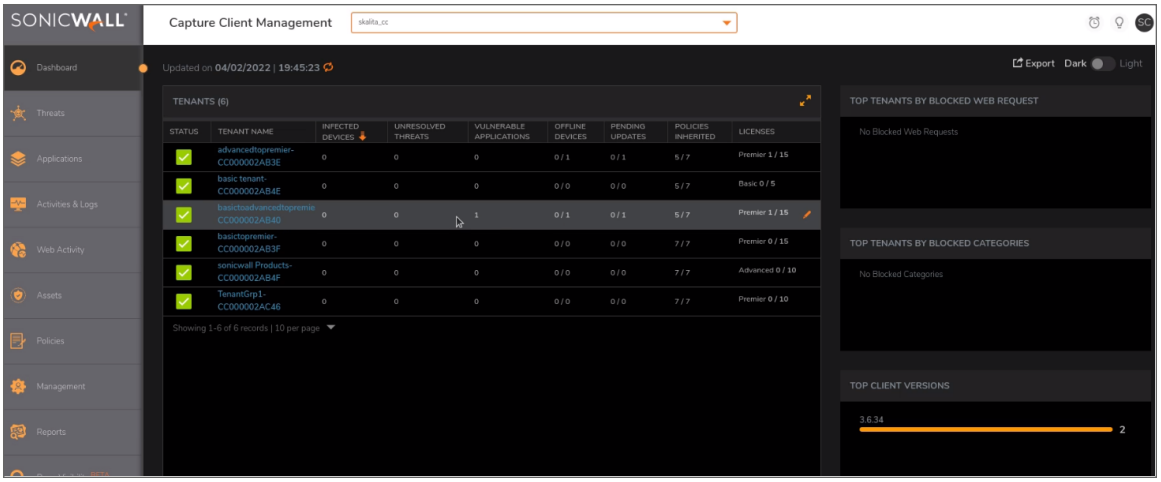
The landing page is the Dashboard to the tenant where you have activated the subscription.



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, actives 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.

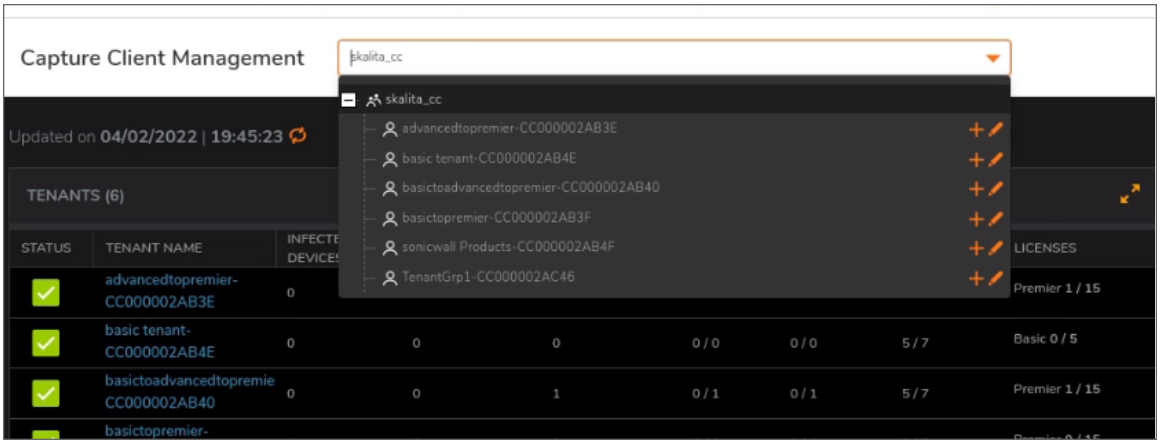


If the account is selected, the Dashboard information is summarized by tenants.



To change to the account/tenant option:

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

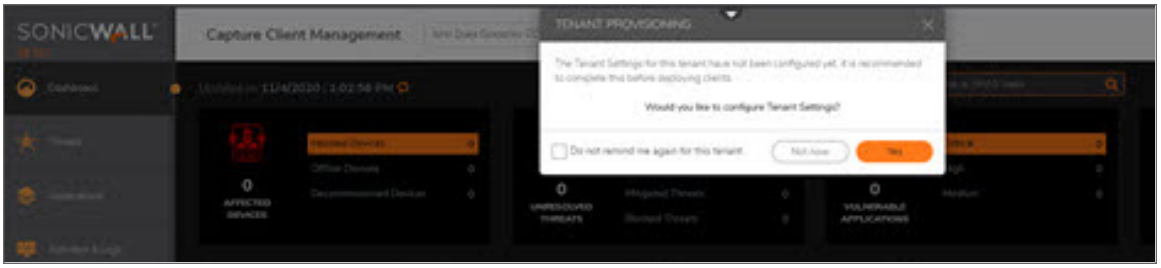


2. Select the account or tenant view that you want.

4

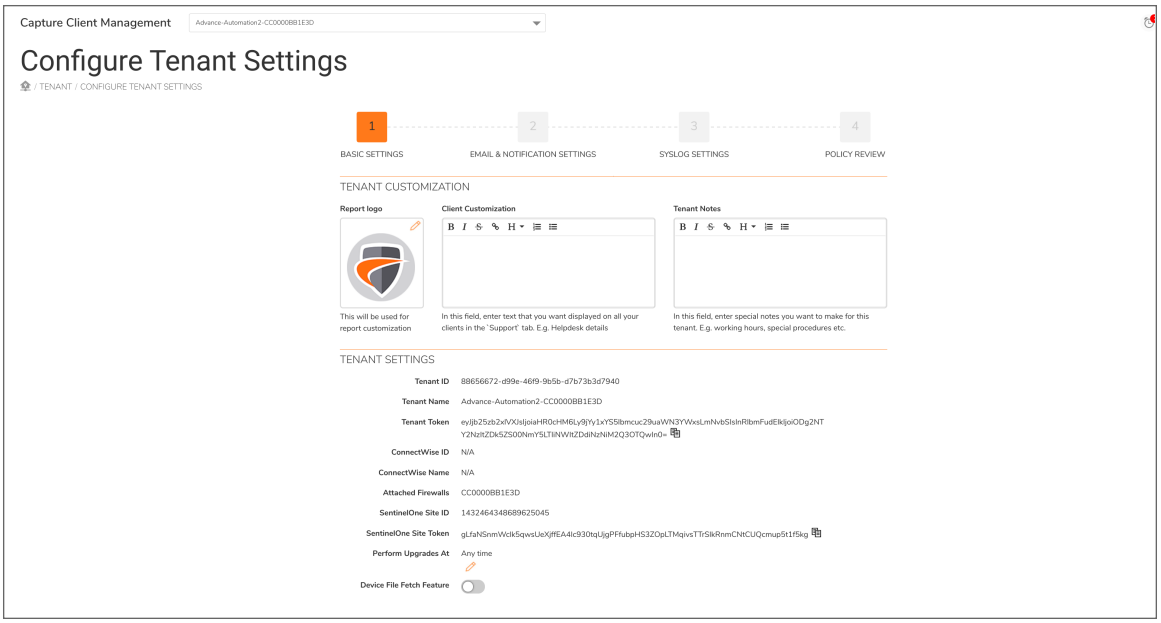
Configuration

When you navigate to a new tenant for the first time in the management console, an automatic popup shows asking if you would like to configure the Tenant settings before you get started.



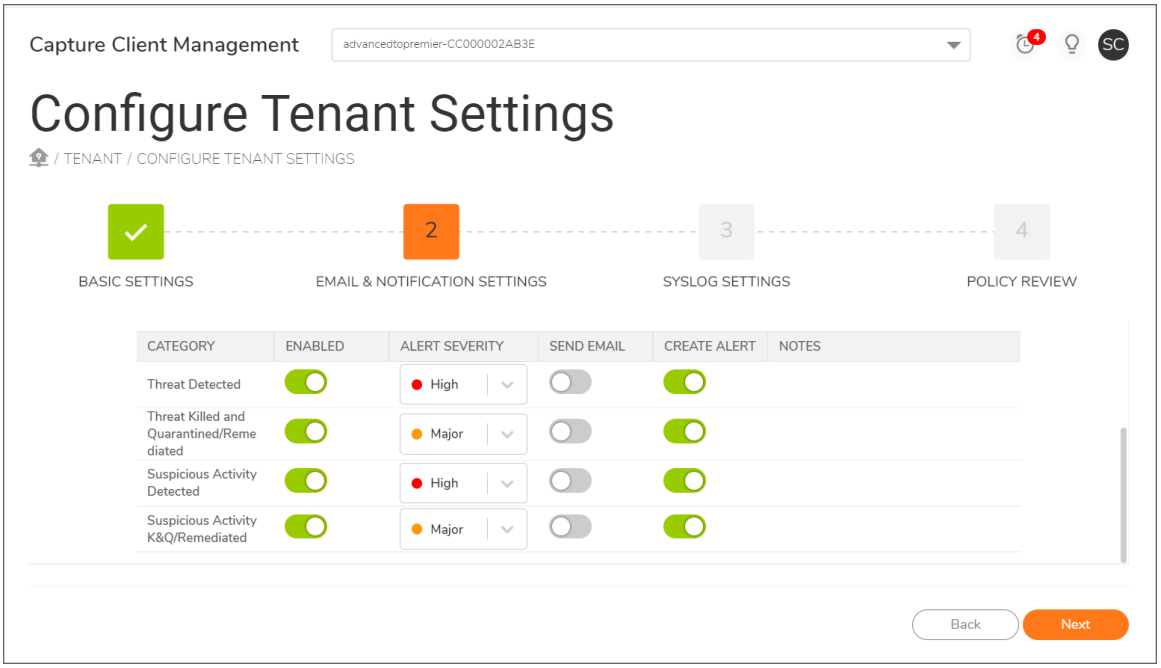
You can choose to dismiss this or get started. If you dismiss it, you can revisit these settings any time by either editing the tenant from the **Scope Selector** at the top or by navigating to **Management > Tenant Settings** in the specific Tenant scope.

When you choose to edit the Tenant settings it launches the **Configure Tenant Settings** wizard:



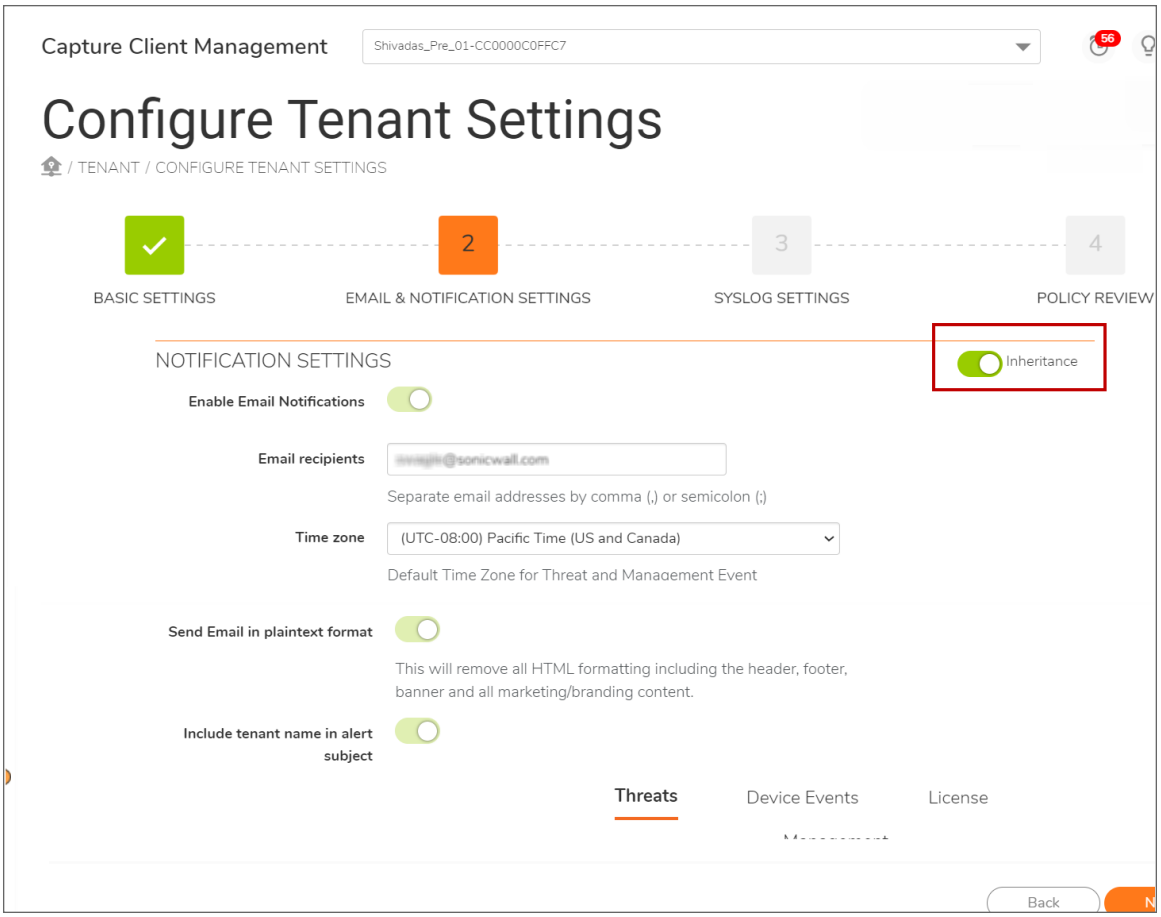
1. ***To set TENANT CUSTOMIZATION:***
    a. In the **Report Logo** section, click the **Edit** icon.
    b. Click **Choose File**.
    c. Select the logo file and click **Open**.
    Make sure that the image is 128x128 pixels in size for best results. Images of other sizes are scaled.
    d. To include a custom note in the Capture Client interface, enter appropriate text in the **Client Customization** box.
2. ***To define TENANT SETTINGS:***
    a. To schedule device upgrades, in the TENANT SETTINGS section click the **Edit** icon next to **Perform Upgrades At**.
    b. Set the schedule as required.
    c. Click Save.
    d. To enabling device file fetch, click the **Device File Fetch Feature** button.
    e. Click **Next**.

3. ***To enable the email settings for notification:***



a. Enable **Enable Email Settings** toggle button.

ⓘ **NOTE:** By default, the email notification settings will be inherited from the account scope for the new tenants. For the existing tenants, you can enable or disable the email and notifications settings into inherit from the account scope. Even when the **Inheritance** option is enabled, you can update the email recipient list and timezone for the Tenant.



b. Type the email addresses of the email recipients in the field provided. Separate email addresses by a comma (,) or semicolon (;).

c. Select the default **Time Zone** from the drop-down list.

d. If you want to include the tenant name in the subject line of the alert, enable that option. This option is only available to administrators of multiple tenant sites.

ⓘ **IMPORTANT:** From step 3d to 7f, you can update the settings only if the **Inheritance** is disabled for the Tenant. If enabled, it will be inherited from the Account scope.

e. Enable the **Send Email in plaintext format** toggle button, if intended to send email without including the header, footer, banner and all marketing/branding content.

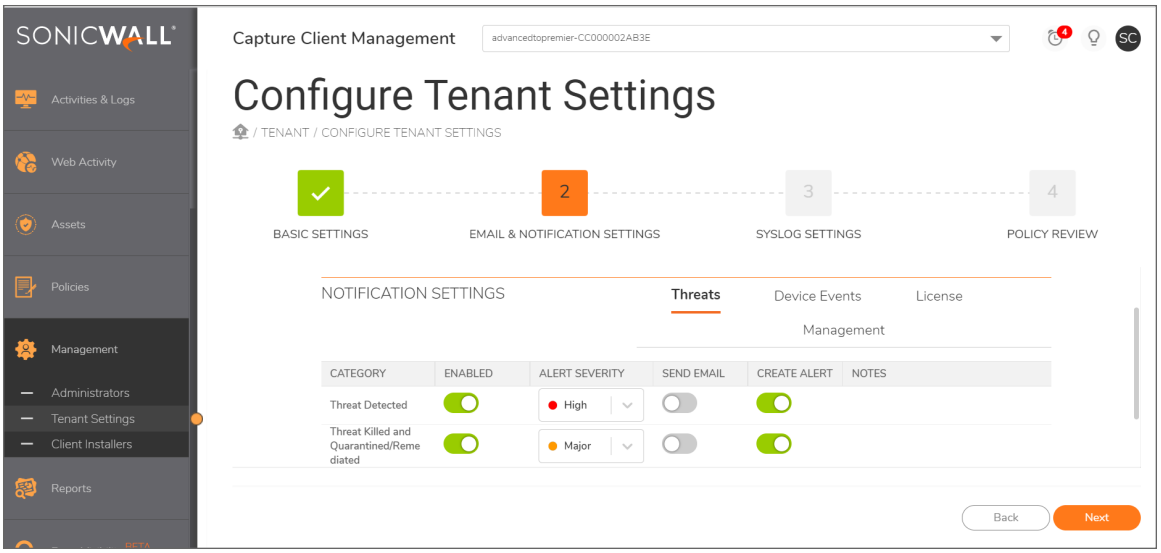
f. Set up the **Notification Settings** for the following: **Threats**, **Device Events**, **License**, and **Management**.

4. ***To setup notifications for threats:***

a. Under the **NOTIFICATION SETTINGS** heading, select the **Threats** tab.

b. Slide the switch under **ENABLED** section to green for each type of threat you want to be notified about. The options include:

- Threat Detected
- Threat Killed and Quarantined/Remediated
- Suspicious Activity Detected
- Suspicious Activity K&Q/Remediated



c. Slide the switch under **SEND EMAIL** section to green for each type of threat for which you want to send email.

d. Slide the switch under **CREATE ALERT** section to green for each type of threat for which you want to create an alert.

e. Under the **ALERT SEVERITY** section select the severity level of the threats from the drop-down list. The options are:

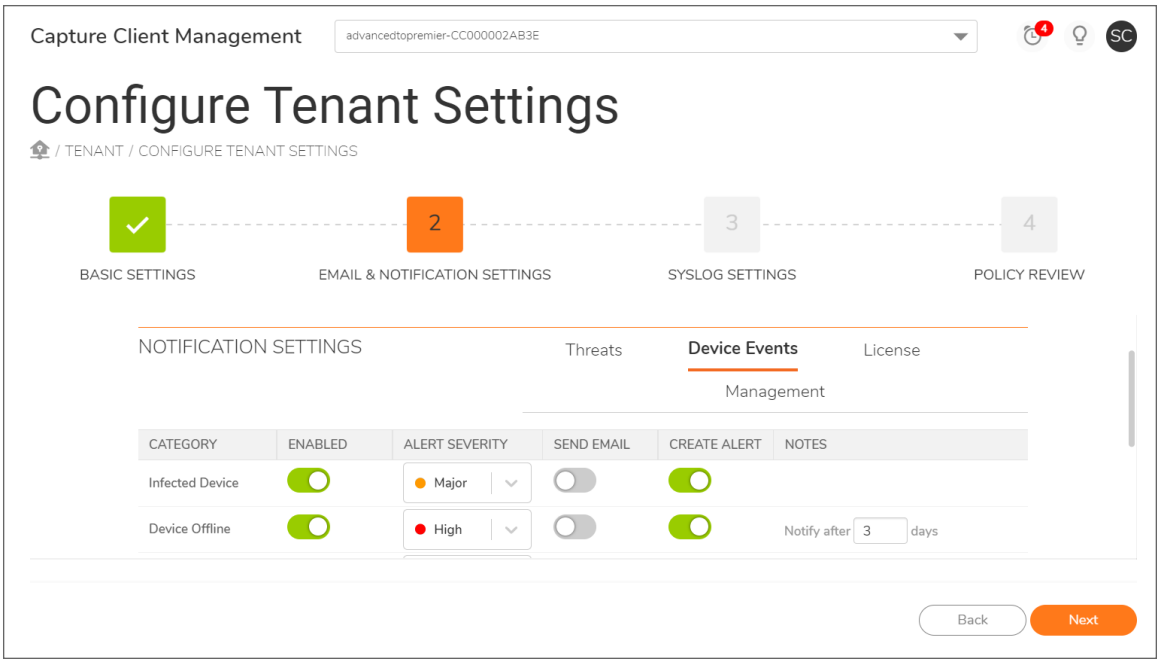
- **Critical** (dark red)
- **High** (bright red)
- **Major** (orange)
- **Minor** (yellow)
- **Low** (light yellow)
- **Normal** (green)
- **Info** (blue)

5. ***To setup notifications for device events:***

a. Under the **NOTIFICATION SETTINGS** heading, select the **Device Events** tab.

b. Slide the switch under **ENABLED** section to green for each type of device event you want to be notified about. The options include:

- Infected Device
- Device Offline
- Scan Started
- Scan Completed Successfully
- Scan Completed with Errors
- Other Devices Event
- Found Application Vulnerability
- Need Reboot



c. Slide the switch under **SEND EMAIL** section to green for each type of device event you want to send email.

d. Slide the switch under **CREATE ALERT** section to green for each type of device event you want to create an alert.

e. Under the **ALERT SEVERITY** section select the severity level of the device events from the drop-down list. The options are:

- **Critical** (dark red)
- **High** (bright red)
- **Major** (orange)
- **Minor** (yellow)
- **Low** (light yellow)

- **Normal** (green)
- **Info** (blue)

f. Under the Notes section set the **Notify After**(days) by incrementing or decrementing the count and the **Minimum Severity** of the device events from the drop down list. The options are:

- **Critical** (dark red)
- **High** (bright red)
- **Major** (orange)
- **Minor** (yellow)
- **Low** (light yellow)
- **Normal** (green)
- **Info** (blue)

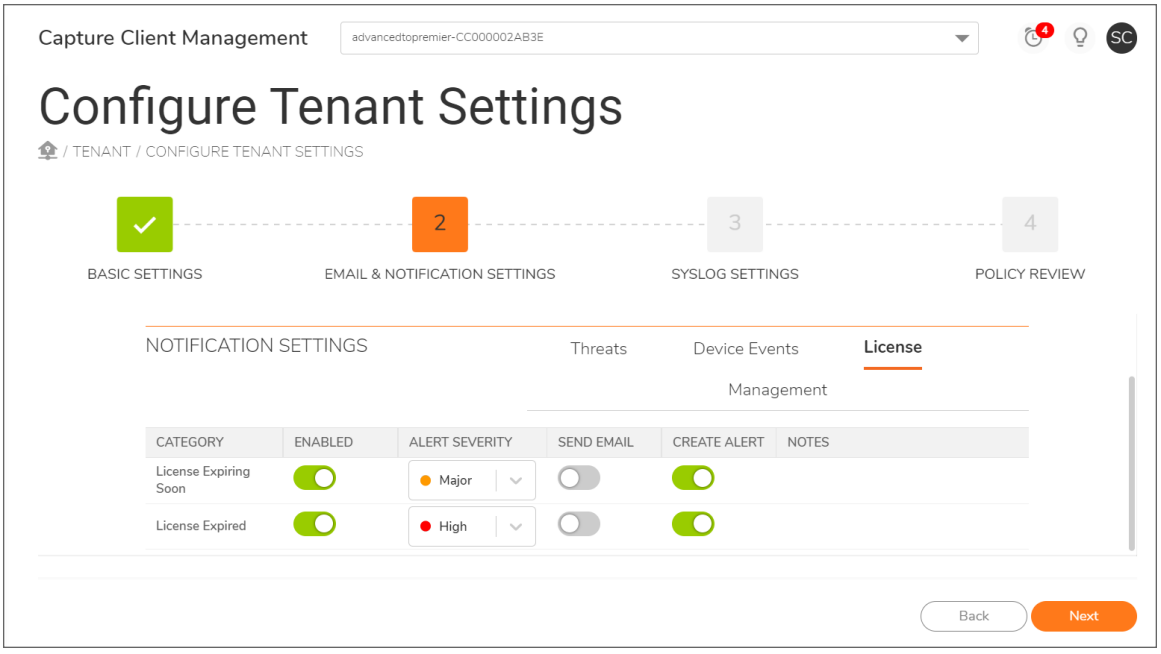
ⓘ **NOTE:** Alert Severity is a notification alert level which will show in the email notification whereas Minimum Severity is a threshold value. An email notification will be sent for all events with Alert Severity level higher than this threshold(Minimum Severity). This feature is only applicable to "Other Device Events".

6. ***To setup notifications for licensing:***

a. Under the **NOTIFICATION SETTINGS** heading, select the **License** tab.

b. Slide the switch under **ENABLED** section to green for each type of license you want to be notified about. The options include:

- License Expiring Soon
- License Expired



c. Slide the switch under **SEND EMAIL** section to green for each type of license you want to send email.

d. Slide the switch under **CREATE ALERT** section to green for each type of license you want to create an alert.

e. Under the **ALERT SEVERITY** section select the severity level of the license from the drop-down list. The options are:

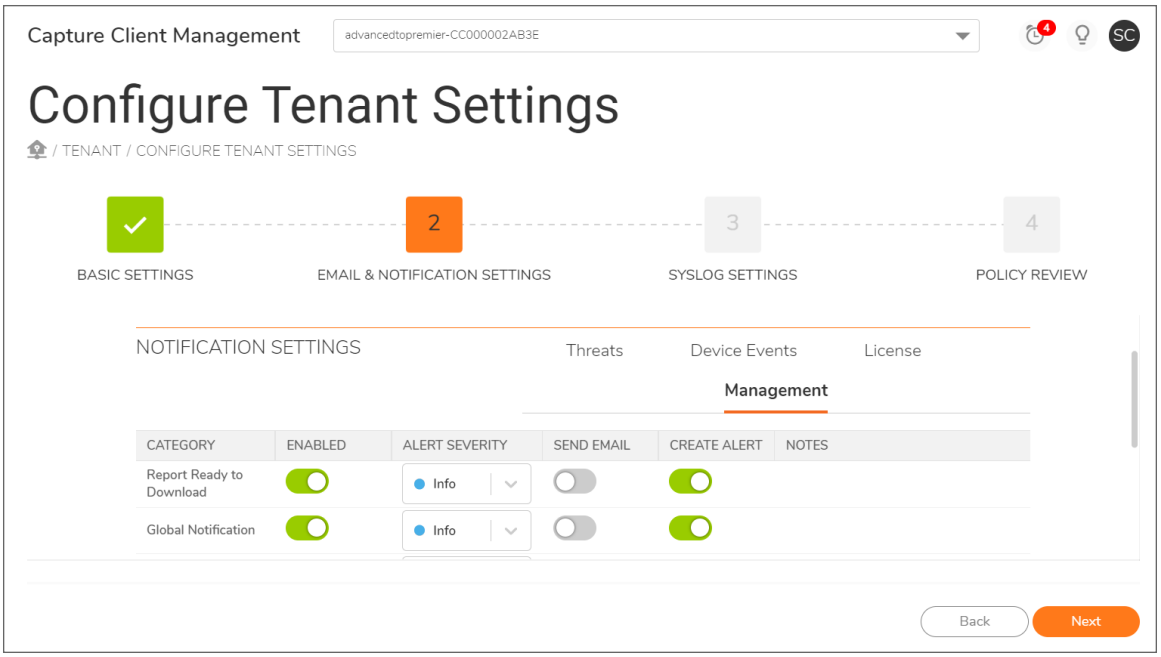
- **Critical** (dark red)
- **High** (bright red)
- **Major** (orange)
- **Minor** (yellow)
- **Low** (light yellow)
- **Normal** (green)
- **Info** (blue)

7. ***To setup notifications for licensing:***

a. Under the **NOTIFICATION SETTINGS** heading, select the **Management** tab.

b. Slide the switch under **ENABLED** section to green for each type of management activity you want to be notified about. The options include:

- Global Notification
- Planned Maintenance
- New Version Available
- Incompatible versions
- End of Support
- Invalid Release
- Other Console Event
- Report Ready to Download



c. Slide the switch under **SEND EMAIL** section to green for each type of management activity you want to send email.

d. Slide the switch under **CREATE ALERT** section to green for each type of management activity you want to create an alert.

e. Under the **ALERT SEVERITY** section select the severity level of the management activity from the drop-down list. The options are:

- **Critical** (dark red)
- **High** (bright red)
- **Major** (orange)
- **Minor** (yellow)
- **Low** (light yellow)
- **Normal** (green)
- **Info** (blue)

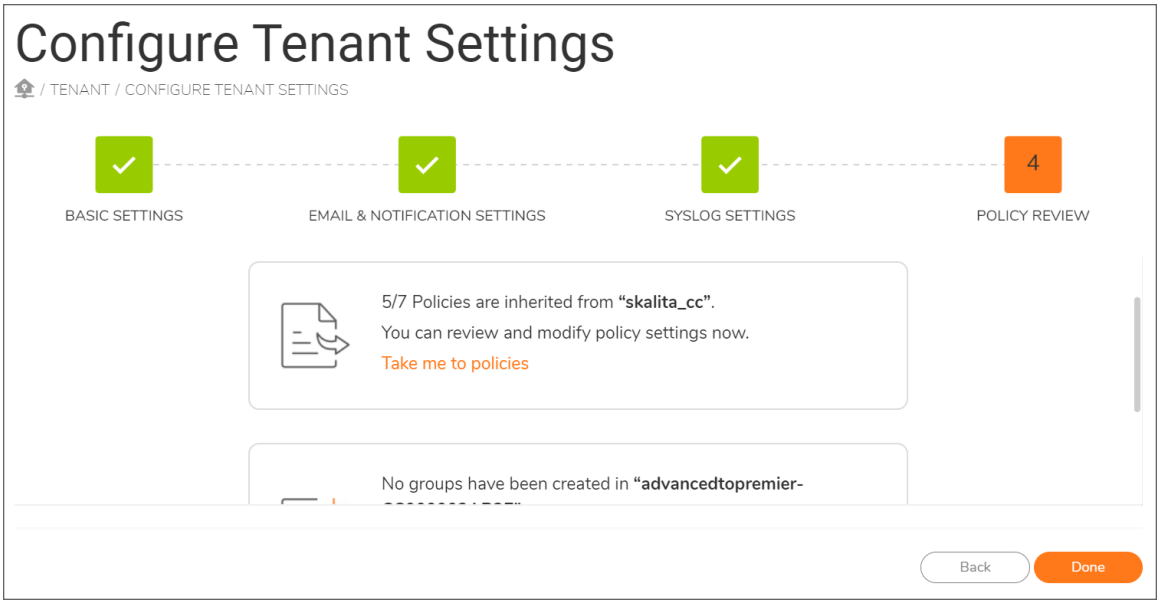
f. Under the **Notes** section set the **Minimum Severity** of the management activity from the drop down list. The options are:

- **Critical** (dark red)
- **High** (bright red)
- **Major** (orange)
- **Minor** (yellow)
- **Low** (light yellow)

- **Normal** (green)
- **Info** (blue)

ⓘ **NOTE:** Alert Severity is a notification alert level which will be shown in the email notification whereas Minimum Severity is a threshold value. An email notification will be sent for all events with Alert Severity level higher than this threshold(Minimum Severity). This feature is only applicable to "Other Console Event".

8. **To set up notifications for SysLog settings**:
   a. Slide the switch under **SysLog** section to green.
      ⓘ **NOTE:** If you select the **Enable Inheritance** option, you cannot edit the **SysLog** settings as the parent scope SysLog settings changes are automatically enforced.
   b. Specify the Host Name.
   c. Select the **TLS** checkbox to enable TLS Secure Connection.
   d. Select the **Information Format** options.
9. Click **Confirm** to review the policy.



This shows the current state of the tenant, indicating that all policies are inherited by default from a parent element. This has best practices enabled for Malware protection, but other settings are likely empty. You can also pivot to create groups for your tenant that allows further customization of policies.

10. Review the policy and , click **Done**.

5

Rollout

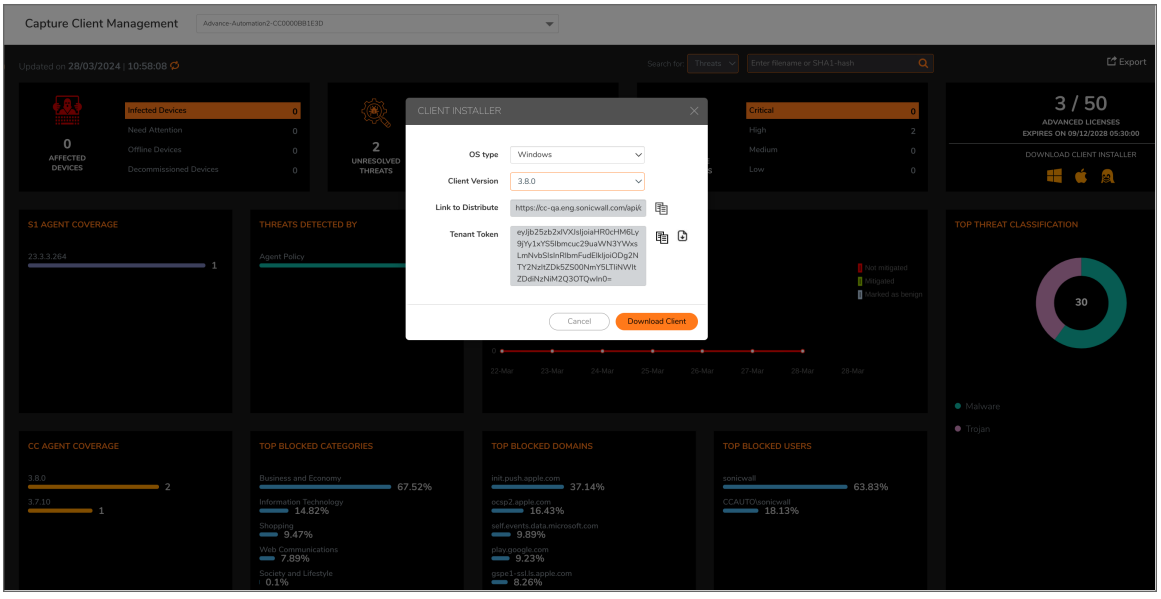
To install Capture Client on an endpoint, use one of the following methods:

- Manual Client Installation
- Installation via Blocked Page
- Installation via Command Line Interface

For more information on how to use tenant token for installation and migrate clients to a tenant in other console or datacenter, refer to the *Protecting Assets with Security Policies* guide on technical-documentation.

Manual Client Installation

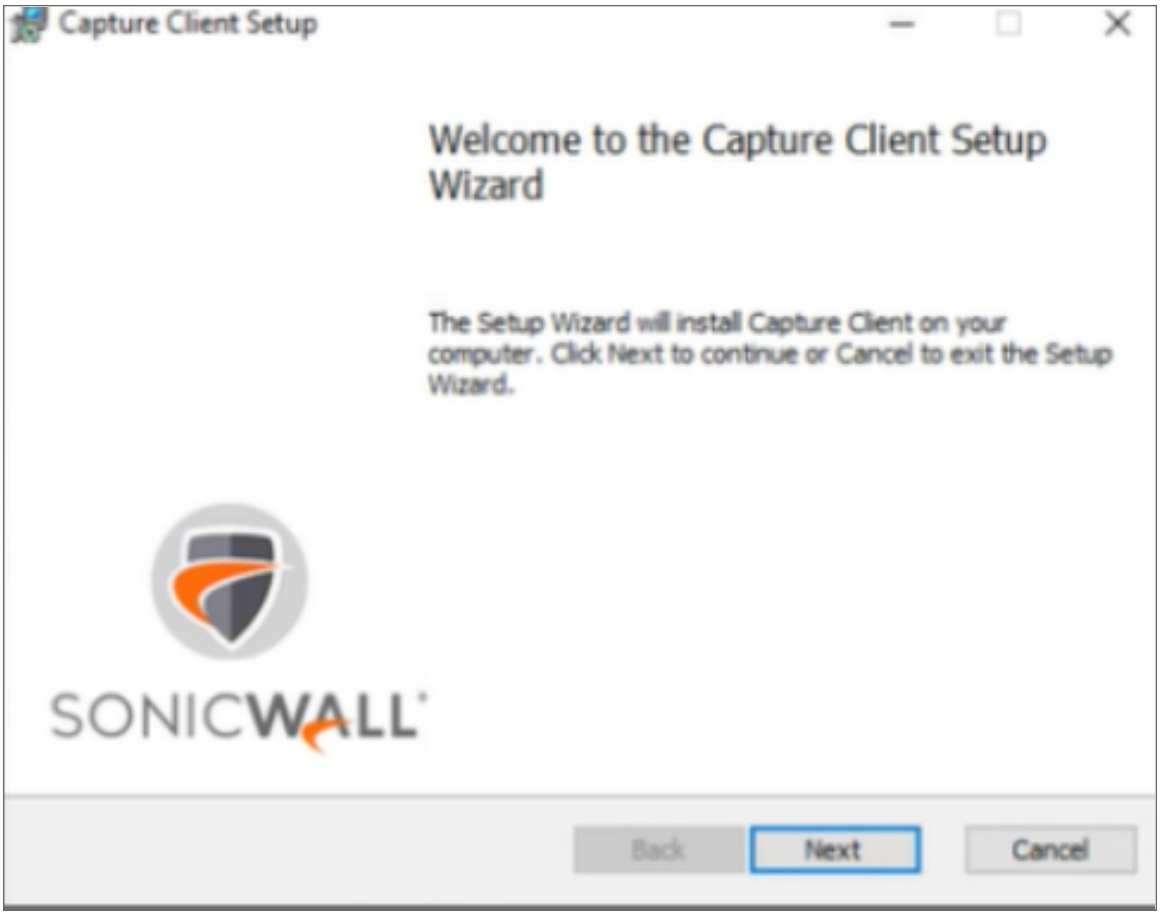
The Dashboard provides access to the **Download** links that can be used to download the clients for each OS type with choices for versions. We always recommend installing the latest General Release version. You can also copy the link to distribute the client via custom installation scripts or third-party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



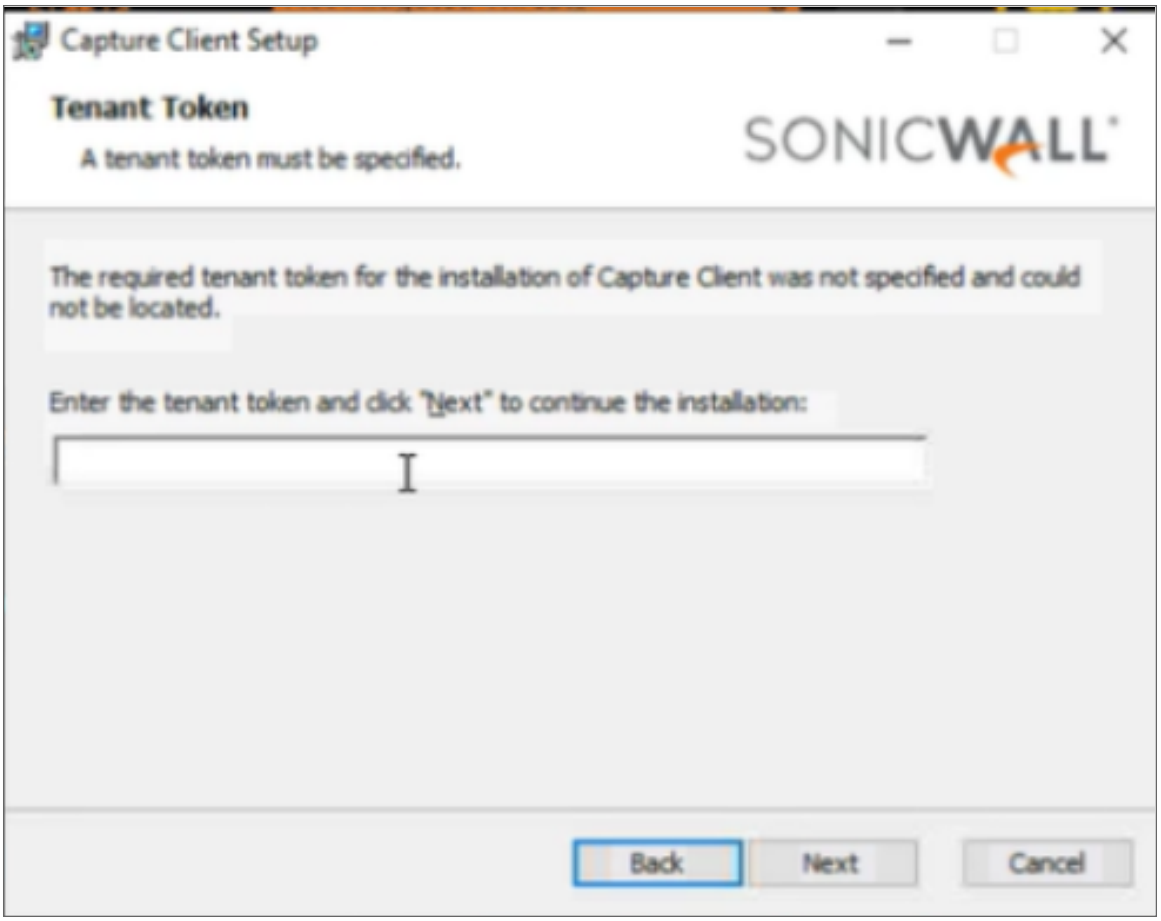
To install the client:

1. Click **Install Capture Client** on the blocked page.

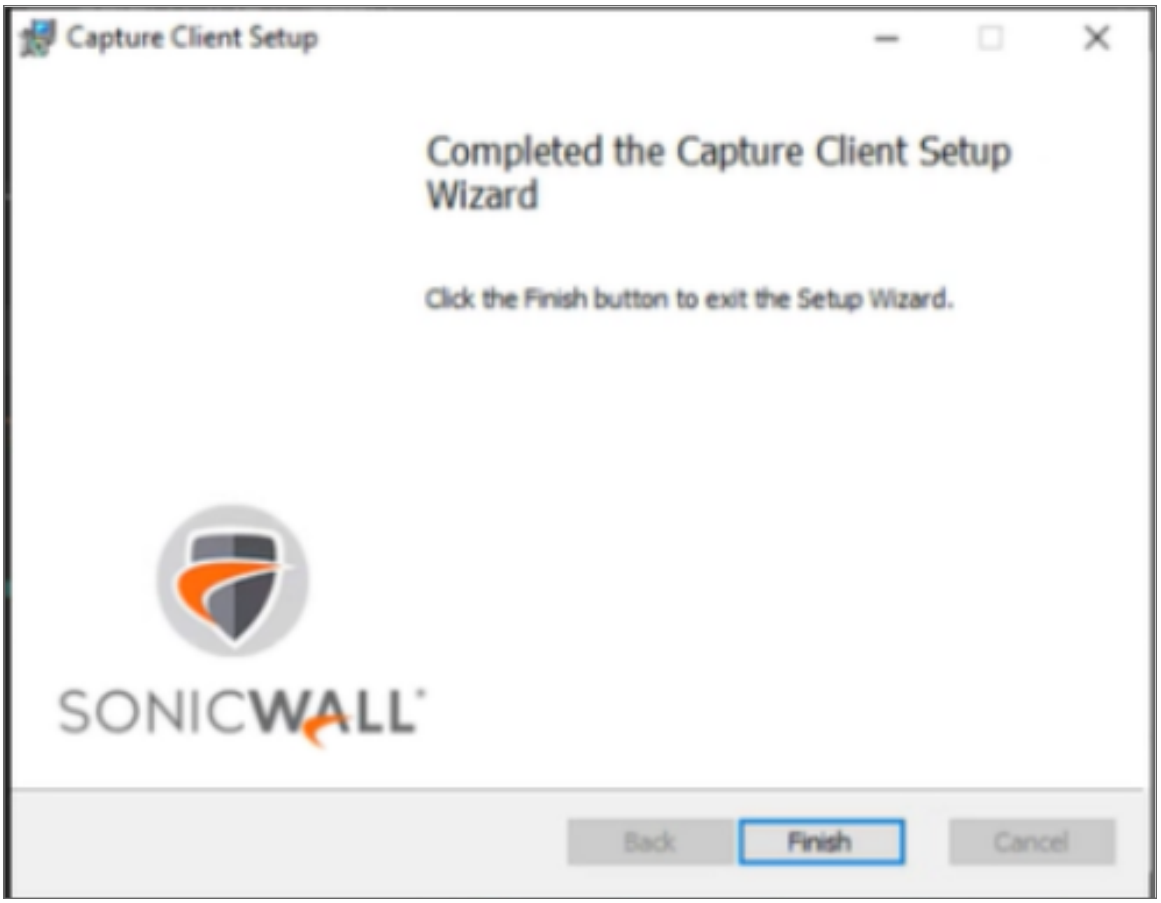
2. Click the **Download** button.
3. After the installer file is downloaded, click **Run** to confirm you want to run the setup wizard.
4. Click **Next** to run the Capture Client Setup Wizard. The **Client Installer** window is displayed.



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



6. Enter the **Tenant Token** and 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.



Installation via Blocked Page

Blocked page installation is only available on Windows and macOS. A blocked page installation cannot be performed on devices running other operating systems.

A Blocked Page Installation can be enforced when Capture Client is used jointly with one or more network appliances enforcing the policy. A series of conditions must be met before the Blocked Page Installation is triggered:

- Capture Client enforcement is enabled on the firewall. Refer to Attaching to a SonicOS Firewall for more information
- The client tries to communicate with an untrusted network zone using a browser via HTTP.
- The network security appliance has determined that the client system does not have SonicWall Capture Client installed.

If all these conditions are met, the network security appliance redirects the end user to a Blocked Page message that has a link for installing SonicWall Capture Client.

For more information on installation, refer to Manual Client Installation .

Installation via Command Line Interface

IT teams can use their own scripts to install Capture Client on endpoints; SonicWallCapture Client is compatible with this method of provisioning.

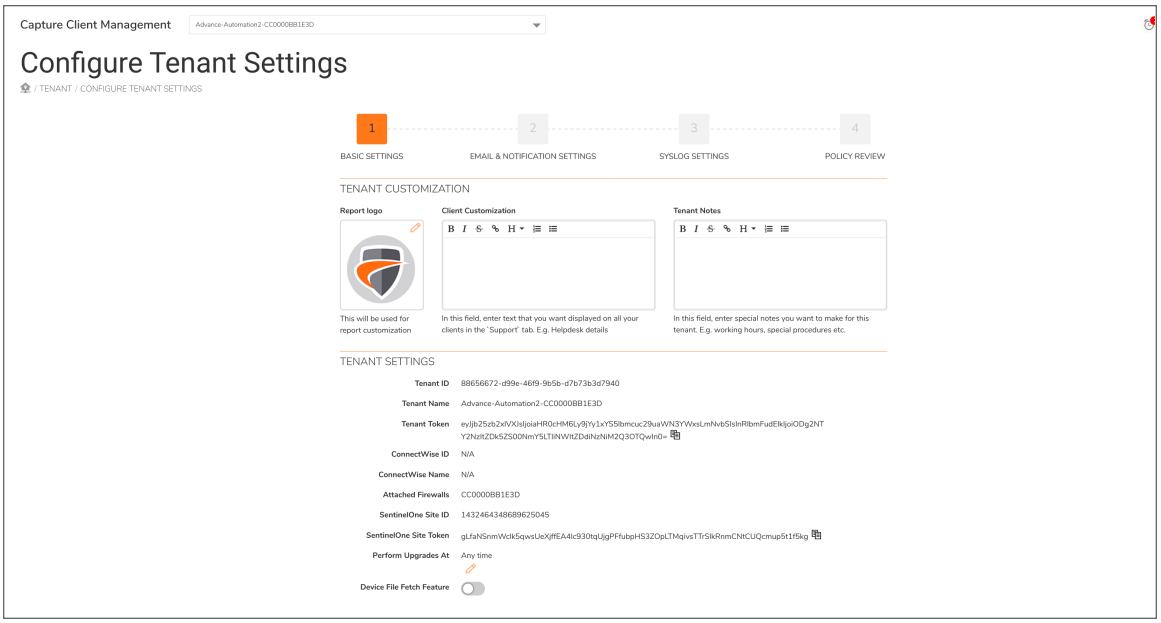
1. Navigate to the **Dashboard** of the tenant where you want to install clients.
2. Click on the Windows or macOS or Linux icon to download appropriate client.
3. To install Capture Client, open the Command Prompt with **Run as administrator** and run the command:
    - **For Windows:** `C:\>msiexec /i "Sonicwall Capture Client.<version>.msi" tenantToken=<> /qn`

    Alternatively, you can also use this command without passing the Tenant Token parameter, if the Tenant Token is already downloaded on the same location of the client installer.

    The Tenant Token can be downloaded from the **Dashboard** Page under **Download Client Installer**. For more information, refer to the *Protecting Assets with Security Policies* guide on Technical-Documentation.

    Where *<version>* is replaced with the appropriate version number and the **Tenant Token** must be added to the command where indicated. The tenant Token can be found in **Management > Tenant Settings**.

    ⓘ | **NOTE:** Capture Client 3.8.0 does not support installation in the command line mode, for macOS.



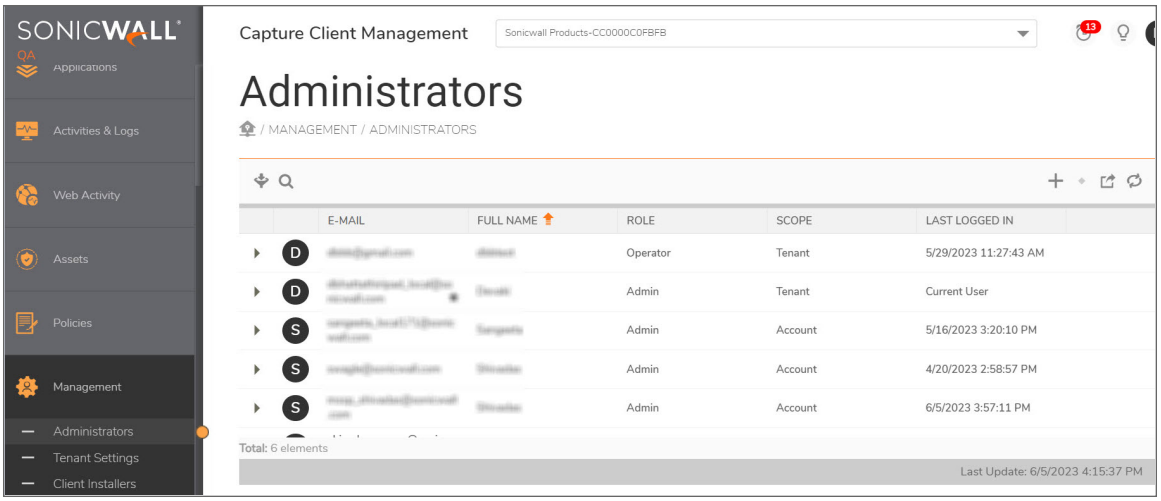
For more information on Tenant Token, refer to the *Protection Guide*, on Technical-Documentation.

6

Roles and Privileges

SonicWallCapture Client provides each of the administrative users with different privileges, depending on the roles assigned to them.

To view the roles of a user navigate to **Management | Administrators** page.



Capture Client has three types of users

- **Admin** - An Admin can access and edit all the sections to get any changes reflected in the management console, and assign others with different types of privileges.
- **Operator** - An Operator can perform device operations and can read and write the Assets and the Reports sections.
- **Viewer** - A Viewer can only read any sections in the console.

The following table describes the accessibility and rights of the CMC users:

CMC Sections	Admin	Viewer	Operator
Administrators page	Read and Write	Read-only	Read-only
Tenant Settings	Read and Write	Read-only	Read-only
Notifications	Read and Write	Read-only	Read-only

Policies	Read and Write	Read-only	Read-only
Assets	Read and Write	Read-only	Read and Write
Reports	Read and Write	Read-only	Read and Write
Threats	Read and Write	Read-only	Read-only

The read only sections:

- Dashboards
- Web Activity
- Applications

For more information, refer to SonicWall Technical-Documentation.

7

Operation

Now that you have your tenant up and running with clients rolled out, you may want to customize settings and policies based on specific requirements. Refer to the following books in the Capture Client document set for additional information:

- *Capture Client Protecting Assets with Security Policies*–use this guide to understand how to customize policies, and create groups for specific policies.
- *Capture Client Monitoring with Dashboards, Threats and Applications*–use this guide to understand how to monitor for new threats and how to respond to them.
- *Capture Client Activities, Logs, and Reports*-use this guide to understand how to review administrative activity in the environment for auditing purposes and to generate reports of the state of your environment and endpoints.

All documents can be found at the Capture Client section of the Technical Documentation portal.

8

Best Practices for a Pilot Exercise

When deploying Capture Client to a complex environment (for example: diverse device profiles, multiple servers, devices spread across multiple networks, and so forth.) you should first run a pilot exercise with a limited, but typical, set of endpoints. This can help you identify what kinds of custom conditions you may need to plan for in your environment. You may need to set up custom whitelists and blacklists, as well as custom policies.

When running the pilot, the client application should be initially deployed in **Detect** mode to the chosen endpoints. The chosen endpoints should represent the various types of devices in your environment. The pilot set should also be small enough to easily manage if any issues arise. By deploying in Detect mode, the client can be run and monitored without any impact to business productivity and can also run side-by-side with existing endpoint security products to allow a smooth transition.

Learn about Threat Protection Policies in the *Capture Client Protecting Assets with Security Policies* to understand how to set up an agent in **Detect** mode.

Depending on the number of pilot endpoints, the pilot exercise should be run for two to four weeks to allow coverage of all types of real-time scenarios. During the pilot, review the threat events generated and validate any issues that may arise. Key issues that you can typically expect are:

- Conflict with known good business applications

  Some business applications may trigger false positives due to the nature of their activity while others may conflict with the Capture Client due to the nature of their application architecture. Review knowledge base article, Capture Client Inter-Operability With Third Party Applications, for a list of known applications with interoperability challenges. Create exclusions for applications that you see in your environment that may create issues.

  Also, leverage the threat events to identify such conflicts and determine how you want to manage them. Review *Capture Client Protecting Assets with Security Policies* to learn how to create Exclusions and review *Capture Client Monitoring with Dashboards, Threats and Applications* to learn how to review threat events and the actions to take.

- Aggressive threat mitigation policies

  The default policy calls for auto-remediation of identified threats as the best practice. However, for certain users or devices, you may not want automatic remediation on all threats. You may only want to generate alerts for them. Review *Capture Client Protecting Assets with Security Policies* for mitigation modes in Threat Protection policies and how to configure them, as well how to create groups with customized policies.

- Certain websites are not filtered

The default web-content filtering policy associated with the default Capture Client policy restricts access only to websites belonging to categories: Hacking and Malware. See *Capture Client Protecting Assets with Security Policies* to configure web content filtering policies that allow or block access to websites of various categories. The association of web content filtering policy with Capture Client policy 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.

- Failure to see encrypted traffic on SonicWall firewalls

  You may see some cases where the DPI-SSL certificates get pushed to the endpoints to enforce DPI-SSL inspection on SonicWall firewalls. Ensure that the policy is setup correctly to not only push it to the native operating system certificate store, but make sure it is also setup to enforce it for Firefox users. You can choose to either push the certificate to the Firefox certificate store or to force Firefox to use the native operating system store. Review *Capture Client Protecting Assets with Security Policies* to see how to configure Trusted Certificate policies with DPI SSL certificates for deployment to clients.

9

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

Capture Client Getting Started Guide
Updated - September 2024
232-005516-00 Rev G

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