SonicWall® Capture Client 3.0
Operations
## Contents

### Part 1. Introduction

- About Capture Client ................................................. 7
- Document Contents .................................................. 7
- Description ............................................................... 8
- Guide Conventions .................................................... 8

- Deployment Guidelines .............................................. 9
  - Pilot Exercise ......................................................... 9
  - Pilot Review ......................................................... 9
  - Policy & Configuration Customization and Assignment ........ 10
  - Defining Management Settings .................................. 10
  - Client Rollout ....................................................... 11

### Part 2. Getting Started

- Prerequisites ........................................................... 13
  - MySonicWall .......................................................... 13
  - Licensing .............................................................. 14
    - Licensing a New Deployment .................................. 15
    - Licensing for an Upgrade ...................................... 15
    - Flexspend Service Management ............................... 18
  - System Requirements .............................................. 19
    - Minimum Hardware Requirements ............................. 19
    - Supported Operating Systems ................................ 20
    - Installation Notes ................................................ 21
    - Capture Client Compatibility with S1 ...................... 22
    - Browser Levels ................................................... 23
    - Third Party Software Interoperability ....................... 23

- Installation ............................................................. 24
  - Accessing the Client Management Console .................... 24
  - Installation methods .............................................. 26
    - Pre-Configured Client Installation ........................... 26
    - Installation via Custom Installation Scripts ............... 26
    - Installation via Blocked Page ................................ 26
    - Installation via Command Line Interface ................... 27

### Part 3. Operations

- Protection .............................................................. 29
  - Configuring SonicWall Firewalls to Enforce Capture Client .. 29
  - Protecting the Devices ........................................... 29
Reviewing Registered Devices and Users ............................................................. 30
  Active Clients ................................................................................................. 31
  Performing a System Scan on a Group of Devices ........................................ 33
  Active Users .................................................................................................... 35
  Active Groups .................................................................................................. 35
Creating Groups for Policy Assignment ............................................................ 35
  Creating a Static User Group ......................................................................... 35
  Creating a Static Device Group ..................................................................... 36
  Creating a Dynamic Group .......................................................................... 37
  Creating Custom Rules for Dynamic Groups ................................................. 38
Threat Investigation ............................................................................................ 40
  Detected Threats ............................................................................................ 40
  Threats That Were Mitigated ......................................................................... 42
  Performing a Rollback .................................................................................... 42
  Resolving Threats ........................................................................................... 43
  Blacklisting Threats ....................................................................................... 43
  Benign Threats ................................................................................................. 43
Security Policies .................................................................................................. 44
  Policy Management ........................................................................................ 44
Threat Protection Policies ...................................................................................... 44
Trusted Certificate Policies .................................................................................... 50
Web Content Filtering Policies .......................................................................... 52
  Adding a Web Content Filter ....................................................................... 52
  Editing a Web Content Filter ....................................................................... 53
  Customizing the Default or Timed Filter Features ....................................... 54
  Localhost Filtering ......................................................................................... 54
Capture Client Policies ........................................................................................ 55
Assigning Capture Client Policies ..................................................................... 57
Configuration ...................................................................................................... 59
  Managing Exclusions .................................................................................... 59
    Hashes ......................................................................................................... 59
    Paths ........................................................................................................... 60
    Signer Identity ............................................................................................ 61
    File Types .................................................................................................. 62
    Browsers ..................................................................................................... 62
    Making Exclusions Global ....................................................................... 63
  Managing the Blacklist .................................................................................. 63
    Blacklisting a Threat .................................................................................. 64
Managing Device Control ..................................................................................... 65
  Adding Rules for Global Lists ...................................................................... 65
  Managing Rules for Global Lists ................................................................ 68
Managing Certificates .......................................................................................... 69
Managing Web Protection Domains .................................................................. 71
Management ...................................................................................................... 72
### Part 4. Monitoring

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing License Usage Statistics</td>
<td>72</td>
</tr>
<tr>
<td>Tenant Settings</td>
<td>73</td>
</tr>
<tr>
<td>Tenant Customization</td>
<td>74</td>
</tr>
<tr>
<td>Configuring Notifications</td>
<td>75</td>
</tr>
<tr>
<td>Email Settings</td>
<td>76</td>
</tr>
<tr>
<td>Notifications Settings—Threats</td>
<td>76</td>
</tr>
<tr>
<td>Notifications Settings—Device Events</td>
<td>77</td>
</tr>
<tr>
<td>Notifications Settings—License</td>
<td>79</td>
</tr>
<tr>
<td>Notifications Settings—Management</td>
<td>80</td>
</tr>
<tr>
<td>Managing Administrators</td>
<td>81</td>
</tr>
<tr>
<td>Adding a New Administrator</td>
<td>81</td>
</tr>
<tr>
<td>Resetting Administrator’s Password</td>
<td>81</td>
</tr>
<tr>
<td>Deleting an Administrator</td>
<td>82</td>
</tr>
<tr>
<td>Exporting Administrators details as a CSV file</td>
<td>82</td>
</tr>
<tr>
<td>Client Installers</td>
<td>82</td>
</tr>
<tr>
<td>Support for Linux Endpoints</td>
<td>83</td>
</tr>
<tr>
<td>Managing Client Upgrades</td>
<td>83</td>
</tr>
<tr>
<td>Self Managed</td>
<td>83</td>
</tr>
<tr>
<td>SonicWall Managed</td>
<td>84</td>
</tr>
<tr>
<td>Reviewing the API</td>
<td>85</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dashboard</strong></td>
<td>2</td>
</tr>
<tr>
<td>About the Dashboard</td>
<td>2</td>
</tr>
<tr>
<td>Threats Detected</td>
<td>3</td>
</tr>
<tr>
<td>Device Health</td>
<td>3</td>
</tr>
<tr>
<td>Web Protection</td>
<td>3</td>
</tr>
<tr>
<td>Unresolved Detections</td>
<td>4</td>
</tr>
<tr>
<td>Online Clients</td>
<td>5</td>
</tr>
<tr>
<td>Investigating and Responding to Active Clients</td>
<td>5</td>
</tr>
<tr>
<td>View Clients</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring and Managing the State of Devices</td>
<td>6</td>
</tr>
<tr>
<td>Reviewing Processes Running on a Device</td>
<td>8</td>
</tr>
<tr>
<td>Reviewing Policies Enforced on a Device</td>
<td>8</td>
</tr>
<tr>
<td>Investigating and Responding to Active Users</td>
<td>9</td>
</tr>
<tr>
<td>Enforce Trusted Certificates</td>
<td>10</td>
</tr>
<tr>
<td>Investigating and Responding to Risky Applications</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statistics</strong></td>
<td>13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analytics</strong></td>
<td>14</td>
</tr>
<tr>
<td>Threats</td>
<td>14</td>
</tr>
<tr>
<td>Downloading Threat File</td>
<td>15</td>
</tr>
<tr>
<td>Downloading Device Files</td>
<td>16</td>
</tr>
<tr>
<td>Web Protection</td>
<td>17</td>
</tr>
<tr>
<td>Activity</td>
<td>18</td>
</tr>
<tr>
<td>Logs</td>
<td>18</td>
</tr>
<tr>
<td>Sections</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Management Logs</td>
<td>18</td>
</tr>
<tr>
<td>Devices Logs</td>
<td>19</td>
</tr>
<tr>
<td>Reports</td>
<td>19</td>
</tr>
<tr>
<td>Generating Reports</td>
<td>20</td>
</tr>
<tr>
<td>Scheduling Reports</td>
<td>20</td>
</tr>
<tr>
<td>Alerts and Notifications</td>
<td>22</td>
</tr>
<tr>
<td>Accessing Notifications</td>
<td>22</td>
</tr>
<tr>
<td>Viewing Alerts</td>
<td>23</td>
</tr>
</tbody>
</table>

**Part 5. SonicWall Support**

<table>
<thead>
<tr>
<th>Sections</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SonicWall Support</td>
<td>26</td>
</tr>
<tr>
<td>About This Document</td>
<td>27</td>
</tr>
</tbody>
</table>
Part 1

Introduction

- About Capture Client
- Deployment Guidelines
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.

Document Contents

This document describes how to configure and deploy the SonicWall Capture Client. It includes the following:

- **Introduction**
  - About Capture Client provides a description of the SonicWall Capture Client and describes the conventions used within this guide.

- **Getting Started**
  - Prerequisites reviews the tasks that need to be done before SonicWall Capture Client site can be set up.
  - Deployment Guidelines provides an overview of the things you need to think about when deploying Capture Client into your environment.
  - Installation describes how to install and uninstall the SonicWall Capture Client.

- **Operations**
  - Protection describes how to get the endpoints protected from vulnerabilities.
  - Threat Investigation describes how to investigate and respond to threats.
  - Security Policies discusses how to set up the security policies.
  - Configuration describes how to perform basic administrative chores.
  - Management reviews basic management functions such as license management, tenant settings, administrator accounts and client installer options.

- **Monitoring**
  - Dashboard provides at-a-glance view of status of devices, number of active users, licenses, and number of malware or web threats.
  - Analytics provides the various detailed analytical reports about threats, activity and logs.

- **SonicWall Support**
  - SonicWall Support describes the support portal and how to get help from SonicWall Support.

Go to https://support.sonicwall.com/technical-documents for the latest version of this guide and to see other SonicWall documentation.

Topics in this section cover the following:

- Description
- 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.

Guide Conventions

The following conventions are used in this guide:

**Text conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text</strong></td>
<td>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.</td>
</tr>
<tr>
<td>**Menu divider</td>
<td>Menu item &gt; Menu item**</td>
</tr>
<tr>
<td><strong>Computer code</strong></td>
<td>Indicates sample code or text to be typed at a command line.</td>
</tr>
<tr>
<td><code>&lt;Computer code italic&gt;</code></td>
<td>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=&lt;your serial number&gt;</code>, replace the variable and brackets with the serial number from your device: <code>serialnumber=C0AEAA0000011</code>.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Deployment Guidelines

When deploying Capture Client to your endpoints, following a structured approach can optimize deployment efforts and minimize support calls after deployment. The following process is recommended:

**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.

Review Threat Protection Policies to understand how to set up an agent in Detect mode.

**Pilot Review**

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 be detected as suspicious due to the nature of their activity while others may conflict with the Capture Client due to the nature of their application architecture. Leverage the threat events to identify such conflicts and determine how you want to manage them. Review Analytics 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 Threat Protection Policies for mitigation modes and how to configure them. Review Assigning Capture Client Policies to learn how to assign different policies to different users or groups.

• 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 Web Content Filtering Policies to configure 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 Trusted Certificate Policies to see how to configure CPI SSL certificates for deployment to clients.

Policy & Configuration Customization and Assignment

Once you’ve identified the situations from the pilot where you want to deviate from the default policy, you need to define these additional configurations prior to rolling out Capture Client to the general population. This includes creating application exclusions either via the Global Exclusion List or on a per-policy basis. Similarly, multiple custom policies may be required for different user and device profiles. Review Managing Exclusions to learn how to exclude your business applications from being inspected by Capture Client.

To assign custom policies to different users or devices, use Groups (either static or dynamic) based on the use-case. Take advantage of the built-in and custom rules to assign polices based on OS, type of device, device hostname or regular expression patterns for these and other device attributes.

If a device matches multiple groups and could potentially be assigned multiple policies, the order of the policies listed determines how conflict is avoided.

Defining Management Settings

Prior to rollout, it is also useful to identify what administrative settings need to be set:

• Identify who should have access to the console.

The tenants support both admin and viewer roles, and users can be created with either role. If users have accounts with MySonicWall (MSW), they can authenticate via MSW, which is recommended. A local password may also be setup, and users can login locally. Given the kind of access users with the admin role have, you may want to take advantage of two-factor authentication (2FA) via authenticator applications like Google Authenticator and Microsoft Authenticator. Review Managing Administrators for more information.
• Identify what notifications to send out and to whom.

To avoid having to maintain eyes-on-glass monitoring at the console, setup email notifications for defined administrators and stakeholders. Multiple email addresses can be configured for notifications, including distribution lists or shared mailboxes. These email addresses need not be associated with users who have access to the console.

Client Rollout

When you are ready to roll the client to endpoints across the network, make sure that the right Capture Client version is selected. The version is defined as part of the Capture Client policy and could be different with different update settings for different device profiles. The console supports the ability to download a pre-configured client via a URL for multiple versions.

Mass deployment can be done in multiple ways. The following options are recommended depending on the complexity of the network and available tools:

• Using a third party software deployment tool
  If using a software management tool like Microsoft SCCM, the client can be downloaded and packaged with specific command-line parameters for silent installation on the clients.

• Using Microsoft Global Policy Objects (GPO) or Scripts
  With the help of Microsoft GPO or with custom PowerShell or bash scripts, the client can also be pushed by simply calling the custom URL available for the specific tenant and client version.

• Using Emails
  For networks that are not connected by a domain and do no leverage any third party tools or scripts, sending custom emails with links to the client URL from the console can be used to encourage users to install the client on their machines.

A reboot is required to fully enable the next generation anti-virus protection and the user is notified of the need to reboot the system. Device installations can be periodically monitored on the console to ensure that all devices that are in-scope are getting the client installed, and that the client is also not getting installed to unintentional targets.
Part 2

Getting Started

- Prerequisites
- Installation
Prerequisites

Prior to configuring and deploying the SonicWall Capture Client, several activities need to be completed to receive the benefits of SonicWall security services, firmware updates, and technical support:

- Create or validate your MySonicWall account in MySonicWall.
- License or activate the Capture Client software in Licensing.
- Review System Requirements.

This chapter reviews these activities and provides guidance for ensuring their completion.

MySonicWall

SonicWall requires a MySonicWall account prior to configuring your SonicWall Capture Client and security services. MySonicWall is used to license your site and to activate or purchase licenses for other security services, support, or software specific to your security solution. If you haven’t already done so, create a MySonicWall account; otherwise, you can skip to Licensing.

To create a new MySonicWall account from any computer:

2. In the login screen, click the Sign Up link.
3. Complete the ACCOUNT information, including email and password.
4 Enable two-factor authentication, if desired.

5 If you enable two-factor authentication, select one of the following authentication methods:
   - Email (one-time passcode) where an email with a one-time passcode is sent each time you log into your MySonicWall account.
   - Microsoft/Google Authentication App where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code.

6 Click on Continue to go the COMPANY page.

7 Complete the company information and click Continue.

8 On the YOUR INFO page, select whether you want to receive security renewal emails.

9 Identify whether you are interested in beta testing new products.

10 Click Continue to go to the EXTRAS page.

11 Select whether you want to add additional contacts to be notified for contract renewals.

12 If you opted for additional contacts, input the information and click ADD CONTACT.

13 Click DONE.

14 Check your email for a verification code and enter it in the Verification Code* field. If you did not receive a code, contact Customer Support by clicking on the link.

15 Click Done. You are returned to the login window so you can login into MySonicWall with your new account.

### Licensing

A mechanism has been put in place to provision and license tenants for Capture Client via MySonicWall (MSW) for new installations and for expanding existing deployments.

On activation of a Capture Client key against a firewall, a virtual tenant is created within the MSW tenant (previously called product group). The virtual tenant hosts the chosen firewall or client license that’s associated with it. It can also represent a tenant with unallocated licenses, allowing you to share the licenses amongst one or more of firewalls, or some combination. This new licensing model provides several benefits:

- Enforces Capture Client against multiple firewalls by sharing licenses from a common pool of endpoint licenses.
- Allows you to easily add or remove firewalls for enforcement when adding new sites, transferring devices from one MSW account to another, performing RMAs (return materials authorizations) or running secure upgrades.
- Uses a single tenant to protect both users behind the firewall and those who are roaming. You no longer separate tenants for each type of user.
- Provides self-service configuration so license sharing can be done without help from Support Services.

To activate a brand new Capture Client license, refer to Licensing a New Deployment. To activate a license for an existing Capture Client deployment, refer to Licensing for an Upgrade.

NOTE: Your password must be at least 8 characters, but no more than 30 characters.
Licensing a New Deployment

Licensing Capture Client for a new deployment is an easy process. In this scenario, you have no prior tenants defined and no firewalls are configured to enforce the endpoint security.

To license Capture Client for a new deployment:

1. Navigate to mysonicwall.com and login.
2. Click the Add Product icon (also known as the Quick Register icon).
3. Enter the Capture Client activation key.
4. Click Confirm.
5. Navigate to Product Management > My Products to validate that the product has been registered and it appears under the right tenant name.

Once you license Capture Client, go to Installation for the next steps.

Licensing for an Upgrade

The steps to upgrade Capture Client differs according to how you set up your initial environment.

- If you want your firewall to enforce the client rules, go to Licensing with a Network Security Appliance for details.
- If you are enforcing clients rules directly from Capture Client, go to Licensing without a Network Security Appliance for details.

Licensing with a Network Security Appliance

To license SonicWall Capture Client with a network security appliance:

1. Log into your network security appliance as an administrator.
2. Navigate to the MANAGE | Updates > Licenses page.
3. In the pane to Manage Security Services Online, click the link to log into MySonicWall and activate the Capture Client license.
4. Click the SYNCHRONIZE button to synchronize all your licenses on the appliance.
Licensing without a Network Security Appliance

To provision Capture Client without a network security appliance:

2. Navigate to Products Management > My Products.
3. Click the + (Add Client Licenses) icon.

4. To register a client licenses group, Enter the client license name, select the appropriate Tenant Name from the drop-down list, and then click Confirm.

5. Click <Licenses> icon on the newly created client license in the table.
6. On the **LICENSES** page, scroll down to the **DESKTOP & SERVER SOFTWARE** section, find **Capture Client** in the list, and click **Action on Tenant**.

7. Enter the activation key if you have and click **Confirm**, or click **Cancel**.

8. Click the **Cart** icon to purchase a license for Capture Client, click **Try** for a free trial, or click the **Key** icon to activate your license with a key from your provider.

9. Once the Capture Client has been licensed, click on the **Service Status** icon.
10 Select **Click here to access your Security Center**. This redirects you to the Client Management Console for login.

**Flexspend Service Management**

You can use FlexSpend to manage activation codes and other FlexSpend activities. If you have no Flexspend credits available in your account, you can enter simulation mode with 10,000 virtual credits. Simulation mode is disabled when you add actual FlexSpend credits to your account.

1. Log into MySonicWall at [https://www.mysonicwall.com/](https://www.mysonicwall.com/).
2. Navigate to **Products Management > Flexspend**.
3. Choose the devices and services to manage, and then click **Allocate** to allocate the credits.
4. After allocation, click **Checkout**.
5. Click **My FlexSpend** to add activation codes to your account. Type the activation code in the field, and click **Add Code**.
6. Click the FlexSpend link to see the FlexSpend reports. Select **Activity Report** or **Billing Report** from the drop-down list. Then define the start and end date for the report period and click **Apply**. The report data is displayed in tabular format.

**System Requirements**

Capture Client is a comprehensive endpoint security solution that protects Windows, Linux, and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection. To get maximum performance and protection, the following standards are recommended:

- **Minimum Hardware Requirements**
- **Installation Notes**
- **Installation Notes**
- **Browser Levels**
- **Browser Levels**
- **Third Party Software Interoperability**

**Minimum Hardware Requirements**

To install Capture Client on a PC or macOS, the device must meet the following hardware requirements:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU requirements</td>
<td>1 GHz or better</td>
<td>Dual-core processor is recommended. Beginning with Capture Client 1.0.24 for Windows and macOS, you can install on a single-core CPU, but performance is not optimal.</td>
</tr>
<tr>
<td>Memory requirements</td>
<td>1 GB RAM or more</td>
<td>3 GB RAM is recommended</td>
</tr>
<tr>
<td>Storage requirements</td>
<td>2 GB free disk space on the Windows partition.</td>
<td></td>
</tr>
</tbody>
</table>

To install Capture Client on a system running Linux, the device must meet the following hardware requirements:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU requirements</td>
<td>1 GHz or better</td>
<td>Dual-core processor is recommended.</td>
</tr>
<tr>
<td>SSE4.x instruction support CPU</td>
<td>NOTE: Some virtual environments mask support for advanced CPU capabilities. See your VM vendor documentation.</td>
<td></td>
</tr>
<tr>
<td>Memory requirements</td>
<td>1 GB RAM or more</td>
<td>2 GB RAM is recommended.</td>
</tr>
<tr>
<td>Storage requirements</td>
<td>1 GB free disk space</td>
<td>3 GB in /opt/sentinelone</td>
</tr>
</tbody>
</table>
Supported Operating Systems

Capture Client supports endpoints (PCs, laptops, tablets, and other devices) running the following operating systems. Capture Client’s advanced threat protection is powered by SentinelOne, and the SentinelOne agent is automatically installed and configured according to the Threat Protection security policy. The recommended SentinelOne agent version is listed below.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Preferred SentinelOne Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Operating System</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server</td>
<td>2019</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2016</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2012 R2, 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2008 R2</td>
<td></td>
</tr>
<tr>
<td>Windows 10</td>
<td>32- and 64-bit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 10 RS5 on 32- and 64-bit</td>
<td></td>
</tr>
<tr>
<td>Windows 8</td>
<td>Version 8.1 on 32- and 64-bit</td>
<td></td>
</tr>
<tr>
<td>Windows 7</td>
<td>Version 7 SP1 on 32- and 64-bit</td>
<td></td>
</tr>
<tr>
<td><strong>mac Operating System</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS 10.15.3</td>
<td>Catalina</td>
<td>4.0.3.3085 or later</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Due to Apple Notarization requirements, macOS 10.15 up to 10.15.2 requires Capture Client 2.0.20 or later and SentinelOne 3.2.1.2800 or later. macOS 10.15.3 or later requires SentinelOne 3.6.1.2964 or later to be installed before upgrading macOS to 10.15.3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS 10.14 and newer up to 10.14.6</td>
<td>Mojave</td>
<td>4.0.3.3085 or later</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The SentinelOne macOS 2.6.3 or later is required for macOS Mojave. An existing SentinelOne 2.6.2 or 2.6.0 version must be upgraded to 2.6.3 or later, before upgrading to macOS Mojave.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>macOS 10.13 or later</td>
<td>High Sierra</td>
<td>4.0.3.3085 or later</td>
</tr>
<tr>
<td>macOS 10.12</td>
<td>Sierra</td>
<td>4.0.3.3085 or later</td>
</tr>
<tr>
<td><strong>Linux Operating Systems</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Linux</td>
<td>2018.03</td>
<td>4.0.3.11</td>
</tr>
<tr>
<td></td>
<td>2017.03</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMI 2</td>
<td></td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>8</td>
<td>4.0.3.11</td>
</tr>
<tr>
<td></td>
<td>7.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.4+</td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>19.04, 19.10</td>
<td>4.0.3.11</td>
</tr>
<tr>
<td></td>
<td>18.04</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16.04</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14.04</td>
<td></td>
</tr>
</tbody>
</table>
To ensure Capture Client operates effectively, the following guidelines are recommended:

- .NET Framework 4.0 or later needs to be installed. For Windows 7 and Windows 2008 R2, you may be prompted for .NET 4.0 to be installed.
- On Windows 7, install the update to enable TLS 1.1 and TLS 1.2 as the default secure protocols in WinHTTP in Windows. Add the registry subkey. These options are not supported in the default Windows 7 installation.
- When the following Microsoft Security Updates are installed, you must restart the endpoint and run the Agent installation again.
- Configure Microsoft Windows Volume Shadow Copy Service (VSS) before you install the agent. More information is available in this knowledgebase article: [https://www.sonicwall.com/support/knowledge-base/180614060954053/](https://www.sonicwall.com/support/knowledge-base/180614060954053/).
### Capture Client Compatibility with S1

The following table lists which SentinelOne (S1) agents are compatible with each Capture Client release.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.17</td>
<td>2.8.2.6745</td>
<td>3.0.2.2629</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>3.0.2.35</td>
<td>3.0.4.2657</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.1.5.63</td>
<td>3.2.0.2671</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.3.29</td>
<td>3.4.2.2857</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.4.5.1</td>
<td>3.6.0.2908</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.6.104</td>
<td>4.0.3.3085 (recommended)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.0.4.81 (recommended)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0.20</td>
<td>3.0.2.35</td>
<td>3.0.2.2629</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>2.8.2.6745</td>
<td>3.0.4.2657</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.1.5.63</td>
<td>3.2.0.2671</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.3.29</td>
<td>3.2.1.2800</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.0.4.81 (recommended)</td>
<td>4.0.3.3085 (recommended; must for fresh install of 2.0.20)</td>
<td></td>
</tr>
<tr>
<td>2.0.24</td>
<td>3.0.2.35</td>
<td>3.0.4.2657</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>3.1.5.63</td>
<td>3.2.0.2671</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.3.29</td>
<td>3.2.1.2800</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.4.51</td>
<td>3.4.2.2857</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.0.4.81 (recommended)</td>
<td>4.0.3.3085 (recommended; must for fresh install of 2.0.24)</td>
<td></td>
</tr>
<tr>
<td>2.0.27</td>
<td>3.0.2.35</td>
<td>3.0.4.2657</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>3.1.5.63</td>
<td>3.2.0.2671</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.3.3.29</td>
<td>3.2.1.2800</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.4.4.51</td>
<td>3.4.2.2857</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.6.6.104</td>
<td>3.6.0.2098</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4.0.4.81 (recommended)</td>
<td>4.0.3.3085 (recommended; must for fresh install of 2.0.27)</td>
<td></td>
</tr>
</tbody>
</table>
SonicWall Capture Client 3.0 Operations

Prerequisites

Based on the operating system you are using, the following browser levels are supported.

NOTE: These browser levels apply to the browser running the Cloud Management Console.

<table>
<thead>
<tr>
<th>Browser Supported</th>
<th>Windows Server</th>
<th>Windows 10</th>
<th>Windows 8</th>
<th>Windows 7</th>
<th>Vista</th>
<th>Linux</th>
<th>macOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Edge (latest version)</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mozilla Firefox (version 52.5 ESR or later)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Google Chrome (latest version)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Apple Safari (latest version)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Third Party Software Interoperability

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 this knowledge base article for more information: https://www.sonicwall.com/support/knowledge-base/180514100738172/.
Capture Client can be deployed to the endpoints in several different ways. This chapter describes three key distribution methods, as well as how to access the Client Management Console.

**Topics:**
- Accessing the Client Management Console
- Installation methods

**Accessing the Client Management Console**

You can access the Client Management Console either by: Launching Capture Client service from Capture Security Center (recommended) or Logging into the Capture Client site.

- Launching Capture Client service from Capture Security Center
  1) Navigate to https://cloud.sonicwall.com/.
  2) Log in with your MySonicWall credentials.
  3) In the Capture Security Center homepage, select appropriate tenant in the TENANTS/GROUPS list.
  4) Select Capture Client to launch.
• Logging into the Capture Client site

1) Navigate to https://captureclient.sonicwall.com/.

2) Click Login with MySonicWall and log in with your MySonicWall credentials.

**NOTE:** After the service has been licensed, you can access your site by clicking the link Login with MySonicWall and using your MySonicWall credentials.

After you log into the console, the default view is the Dashboard. You can see at a glance the number of active endpoints, the number of active users, the status of the policies and the number of active threats. Each item on the dashboard is assigned a color based on the status of the item.
Installation methods

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

- Pre-Configured Client Installation
- Installation via Custom Installation Scripts
- Installation via Blocked Page
- Installation via Command Line Interface

Pre-Configured Client Installation

SonicWall Capture Client can be easily installed on a client system. The client installers can be downloaded from the Client Installers page located at Management > Client Installers. Currently Windows, Linux, and macOS are supported devices, and pre-configured installation scripts are provided. Once the license for your tenancy has been established, you can send a link to your users and have them download and install the client on their own devices. You need only provide the link to the console and the appropriate login credentials. Refer to Protecting the Devices for the steps for this process.

Installation via Custom Installation Scripts

IT teams can use their scripts to install Capture Client on endpoints; SonicWall Capture Client is compatible with this method of provisioning. You need to download only the .msi, .sh, and .pkg files from the Client Installers page (Management > Client Installers). No configured parameters need to be manually entered during the installation, so IT teams can ensure a seamless and transparent installation experience for their end users.

Installation via Blocked Page

NOTE: 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 Configuring SonicWall Firewalls to Enforce Capture Client 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 that has a link for installing SonicWall Capture Client.

To install the client:

1. Click Install Capture Client on the block 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.
5 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.

### Installation via Command Line Interface

1 Navigate to **Management > Client Installers**.
2 Hover over the Capture Client version you want and then 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:
   - **Windows**: `C:\> msiexec /quiet /l*v /i "SonicWall Capture Client.<version>.msi" tenantID=<>`
   - **macOS**: `sudo installer -pkg "SonicWall Capture Client.<version>.pkg" tenantID=<> -target /`

Tenant ID is required to report the device to the right tenant context. The tenant ID can be found in **Management > Tenant Settings**.
Part 3
Operations

• Protection
• Threat Investigation
• Security Policies
• Configuration
• Management
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:**
- Configuring SonicWall Firewalls to Enforce Capture Client
- Protecting the Devices
- Reviewing Registered Devices and Users
- Creating Groups for Policy Assignment

**Configuring SonicWall Firewalls to Enforce Capture Client**

The first key step to ensuring Capture Client coverage is to log into your SonicWall firewall and enable anti-virus enforcement.

***To enable anti-virus enforcement from the firewall:***

1. Log into your network security appliance as an administrator.
2. On the **MANAGE** view, navigate to **Security Configuration | Security Services > Client AV Enforcement**.
3. On the **SentinelOne Client AV Status** panel, click on the link to manage SentinelOne AV settings.
4. Define the settings as desired for your configuration.

**Protecting the 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. On the Dashboard (**Overview > Dashboard**), click the options icon (gear icon) on the upper-right corner of the page.
3. Select **Download Client installers**.
4 Select the Capture Client version needed:
   - Windows
   - macOS
   - Linux

\[\text{NOTE:} \] The Linux installer is available only for Capture Client version 3.0.x or later. For installing Capture Client for Linux, see \textit{Client Installers}.

\[\text{NOTE:} \] The star icon, to the left of the version, identifies the recommended version of the Capture Client.

\[\text{NOTE:} \] The steps below show how to download the agent for a Windows device. The process is similar for a Mac system.

5 Confirm whether you want to run or save the .msi file locally.
6 Click \textit{Run} to confirm you want to run the setup wizard.
7 Click \textit{Next} to run the Capture Client Setup Wizard.
8 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 and Users**

You can quickly check the status of active devices and active users by going to the \textit{Dashboard}. The \textit{Dashboard} is the default view when you first login to Capture Client, or you can easily access it by selecting \textit{Overview > Dashboard} on the left menu. By reviewing the options listed across the top of the dashboard, you can quickly see how many clients and protected devices are associated with Capture Client.

You can also see the list of Online Clients by selecting \textit{Online Clients} option under the tiles. Scroll down to see the list of \textit{Online Clients}. 
Active Clients

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

To view the geographical locations of the devices, click World Map on the 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.

The Devices list includes the following information for each devices being monitored:

- Alerts
- Name
- Status
- Last Active
- Users
- Console Visible IP address
- Location
- OS
- Client version
- Options (gear icon)

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.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="green_check" /></td>
<td>Commissioned—Capture Client is installed and running on the device</td>
</tr>
<tr>
<td><img src="image" alt="red_cross" /></td>
<td>Decommissioned—Capture Client is not running on the device</td>
</tr>
<tr>
<td><img src="image" alt="green_circle" /></td>
<td>Activated—The device can access the network</td>
</tr>
<tr>
<td><img src="image" alt="red_beat" /></td>
<td>Offline (Capture Client console offline, SentinelOne console offline)</td>
</tr>
<tr>
<td><img src="image" alt="green_beat" /></td>
<td>Online (Capture Client console online, SentinelOne console online)</td>
</tr>
<tr>
<td><img src="image" alt="yellow_bell" /></td>
<td>Either Capture Client console or SentinelOne console is offline</td>
</tr>
</tbody>
</table>

The options icon (gear icon) is only visible when you mouse over a particular device. The Options icon activates a drop-down list of actions you can take on that particular endpoint.
Performing a System Scan on a Group of Devices

To perform the system scan on a group of devices:

1. To select the devices on which you want to perform the system scan, do one of the following:
   - Navigate to Protection > Devices. Select the devices on which you want to perform a scan, and click <initiate scan> icon at the upper-right corner of the table.
• Navigate to Protection > Groups, hover over the device group on which you want to perform a scan, and click <initiate scan> icon.

• To perform system scan on all the devices associated with a tenant, navigate to Protection > Devices, click <initiate scan> icon at the upper-right corner of the table.

2 Select Action Approved and click Confirm in the below prompt.

   ![Action Approved](image)

   **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.
Active Users

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

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:

- Username
- Full Name
- Devices
- Group

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

Active Groups

To see all the active groups associated with a configuration, navigate to Protection > Groups. The Groups page has two tabs: 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

For more information about creating groups, refer to Creating Groups for Policy Assignment.

Creating Groups for Policy Assignment

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.

Creating a Static User Group

To create a new static user group:

1. Navigate to Protection > Groups.
2 Select **Static Groups > User Groups**.

3 Click + to create a new static user group.
4 Type the **Group Name** in the field provided.
5 Select **Static** as the assignment mode.
6 In the **Group Type** drop-down box, select **User Group**.
7 Click **Next**.
8 Select users and click **Next**.
9 Review the users that are part of the static user group being created.
10 Click **Finish**.

### Creating a Static Device Group

**To create a new static device group:**

1 Navigate to **Protection > Groups**.
2 Select **Static Groups > Device Groups**.

3 Click + to create a new static device group.
4 Type the **Group Name** in the field provided.
5 Select **Static** as an assignment mode.
6 Click **Next**.
7 Select devices and click **Next**.
8 Review the devices that are part of the static device group being created.
9 Click **Finish**.

**NOTE:** If at some point you want to turn a static device group into a dynamic group, follow these steps:

1 Select the static group and click the **Edit** icon.
2 Select the **Rules** tab.
3 Click on **Make dynamic**.
Creating a Dynamic Group

To create a new dynamic group:

1. Navigate to Protection > Groups.
2. Click on + to create a new group.
3. Enter the Group Name, confirm Dynamic in the Assignment Mode box, and then click Next.
4. From the Add Rule drop-down menu, select the options as needed:

   ☛ **NOTE:** You can add multiple rules for a group if needed.

<table>
<thead>
<tr>
<th>Add Rule Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Rule</td>
<td>Devices that meet the custom rule set by an administrator is added to this group. See Creating Custom Rules for Dynamic Groups to create a custom rule.</td>
</tr>
<tr>
<td>Desktop Devices</td>
<td>If a device is one of these types, it is automatically added to the selected device group.</td>
</tr>
<tr>
<td>Laptops</td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
</tr>
<tr>
<td>Virtual Machines</td>
<td></td>
</tr>
<tr>
<td>Windows Devices</td>
<td></td>
</tr>
<tr>
<td>Windows Servers</td>
<td></td>
</tr>
<tr>
<td>Mac Devices</td>
<td></td>
</tr>
<tr>
<td>Linux Devices</td>
<td></td>
</tr>
<tr>
<td>32-bit Platforms</td>
<td></td>
</tr>
<tr>
<td>64-bit Platforms</td>
<td></td>
</tr>
</tbody>
</table>

5. Select the ASSIGNMENT MODE for this rule. Options are:

   • Apply to New Devices Only
     The rule is applicable only for devices that are added under a tenant after you create a dynamic group.

   • Apply to All Devices
     The rule is applicable for all the devices that are under a tenant, and also the new ones that are added after you create a dynamic group.

   • Refresh All Group Assignments
     Go through the whole list of groups, and re-calculate the group assignment for each user and device.

     This ensures that all dynamic group rules are respected, and may remove devices from groups they no longer satisfy.

6. Click Finish.
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 Protection > Groups.
2. Click + to add a Dynamic Group.
3. Create the group by providing a Group Name and Assignment Mode.
4. Click Add Rule and select Custom Rule from the drop-down list.
5. Choose the criterion and then select the operation from the drop-down lists.

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

6. Add a reference value and click +.
7. Continue adding rules until done and click Next.
8 Select the **ASSIGNMENT MODE** and click **Finish**.

**NOTE:** The Refresh All Groups Assignments is needed if the dynamic group rules were changed and the administrator chose to not refresh the rules at the time of that update. In this way the administrator can make one or more rules changes and apply the rules at one time.
Threat Investigation

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

The Threats page shows all the threats detected in reverse chronological order with the latest detection at the top of the first page. The colors of the represent different stages of the threat:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Green indicates a mitigated or resolved threat.</td>
</tr>
<tr>
<td>🟢</td>
<td>Orange indicates a suspicious event has been detected.</td>
</tr>
<tr>
<td>🔴</td>
<td>Red indicates the threat is currently unresolved.</td>
</tr>
<tr>
<td>🟧</td>
<td>Gray indicates that the threat has been detected and blocked.</td>
</tr>
</tbody>
</table>

Detected Threats

You can select individual threats for details of that threat and actions taken by SonicWall Capture Client. You can also see the current status of the threat and, in some instances, you are given a list of options for further actions, like Mark as resolved benign, Mark as resolved, Mark as threats, and Add to blacklist.

If you click on a threat that was only detected, it shows a page similar to the following. Under the Actions section, you can see that the Threat has only been detected. It shows that the reason for non-prevention of the threat is because the policy is set to Detect (Alert only) threats. It does not Protect (Kill & Quarantine).
• By looking at **File Info** section, you can see the file name, path, and the device on which it was detected, as well as device details such as IP address and time of detection and alerting.

• By looking at **Summary** section, you can see the Risk level associated with the threat, the SHA1 Hash (typically used to identify unique files), the signing authority for the file and the engine that detected the threat.

• To determine if this threat was seen by anyone else, you can click on the **VirusTotal** link in the summary section to open a browser window with a search against the **VirusTotal** database for the SHA1 Hash of the file.
  
  • Check the signing authority for the file. If it is a legitimate organization and is verified, this may be a false positive. But some threats steal legitimate certificates for signing malware code.

  • The detection engine reflects which engine enabled via the policy actually detected this threat.

• If you deem that the threat is real, you can immediately kill and quarantine the threat using the **Kill** link located in the **Actions** section.

• If you are not sure and would like to investigate further, you can contain the threat from spreading to other endpoints or from causing network-based impact (like exfiltration of data). You can also logically disconnect the endpoint from the network by clicking on the **Disconnect Network** button. This ensures that the endpoint can talk to the Capture Client Management Console but not to any other destination. You can reset this action by clicking on the button again which is now labeled **Reconnect to Network**.

• If the file looks like a legitimate file to your organization (custom app/script), then you can mark it as benign by clicking on **More Actions** and selecting **Mark as Benign**.
• If the file is definitely malicious, you can also select More Actions > Add to Blacklist to mark it as a legitimate threat across the organization. This reduces the need to do any analysis on this threat if it is seen again.

**Threats That Were Mitigated**

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

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

**Performing a Rollback**

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

**IMPORTANT:** Before performing rollback on Windows endpoints, you need to configure Volume Shadow Copy Service (VSS). To configure VSS on Windows computers for Capture Client rollback feature to work, see [https://www.sonicwall.com/support/knowledge-base/180614060954053/](https://www.sonicwall.com/support/knowledge-base/180614060954053/).

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

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

The time it takes for a rollback to complete depends on the size of the shadow copy, but for a large disk, it should only take a few minutes.
Once you have clicked Rollback and the rollback is complete, the Actions section shows that the rollback was completed successfully.

**Resolving Threats**

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

**NOTE:** Marking an issue as resolved does not ensure that the system is not infected. Be sure you’ve taken the appropriate action to investigate and resolve the threat before you mark it resolved.

**Blacklisting Threats**

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

**To blacklist a known threat:**

1. Navigate to Analytics > Threats.
2. Click on a threat to access threat details.
3. Click More Actions drop-down box, click Add to blacklist.
4. Click Confirm.

**Benign Threats**

In the event that Capture Client reports a false positive, you are able to mark the file as benign. This instructs the endpoint client to ignore the process when it occurs again. To mark an event as benign, go to More Actions in the Status pane and select Mark as benign.
Policy Management

The security policies define the conditions and constraints for connection. Multiple policies can be used as an ordered set of rules where the policy at the top of the list has the highest priority. The second policy has the next priority and so forth. Policies can be organized by clicking on the orange up/down arrowheads to the left of the policy name. The Default Policy is always the lowest priority and cannot be deleted.

The available security policies are:

- Threat Protection policy
- Trusted Certificate policy
- Web Content Filtering policy
- Capture Client policy

**NOTE:** The number of policies is limited to 100 per tenant.

Capture Client policy defines which version of Capture Client should be installed, links users, groups, firewalls, and other security policies: threat protection policy, web-content filtering policy, and trusted certificate policy. Refer to Capture Client Policies for more information.

Threat Protection Policies

Threat Protection policy is one of the security policies that Capture Client offers. To view the Threat Protection policies, navigate to Security Policies > Threat Protection. The Threat Protection table lists all the Threat Protection policies that have been created. To the right of the Threat Protection list, use the Actions icons to edit, clone or delete the policies. Click the arrowhead on the left to expand a policy to see more details.
To define a threat protection policy:


2. Select Add (the + icon).

3. Type the new name in the Policy Name field.

4. Select Create. You may need to refresh your screen to see the new policy in the list.

5. Click the Edit icon to define policy parameters.

6. Click Add (the + icon) to update the usage of the policy.

7. From the list, select the Capture Client policy or policies you want and click Add.

8. Confirm your choice when asked if you want to overwrite the current threat policy assignment: Cancel to opt out or Overwrite to confirm the new policy choice.

9. Click on the Overview tab.
   a. Edit the policy name.
   b. Select whether the policy is Enforced or not.
   c. In the drop-down list, select which SentinelOne agent version you want to apply.
   d. Click Update. Anytime you make a change to the policy, you are asked to confirm the new choice.
10 Click on the Protection Modes tab.

In the THREATS section, set the **Mitigation Mode** for when a threat is detected. Choose either **Protect** (the default) or **Detect (Alert Only)**.

- **Detect**—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.
- **Protect**—Detects a potential threat, reports it to the management console, and immediately performs the configured Mitigation Action to mitigate the threat.

Set the **Mitigation Action**. Choose from **Kill & quarantine**, **Remediate**, or **Rollback**.

**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.

In the SUSPICIOUS ACTIVITIES section, set the **Mitigation Mode** for when suspicious activities are detected. Choose either **Capture ATP (Auto-mitigation)**, **Protect**, or **Detect (Alert Only)**.

Set the remaining options for the Mitigation Mode selected.
Click Update to save the new settings.

4 Click Engine Settings tab.

Capture ATP (Auto-mitigation)

1. 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.
   - Mark as Threat — Automatically quarantines the file, marks it as a threat, and performs the corresponding mitigation action.
   - Detect (Alert only)

2. Set the action to take if Capture ATP returns a Not Malicious Verdict:
   - Detect (Alert only)
   - Mark as Benign

3. Set the action to take if Capture ATP returns a Not Undetermined Verdict:
   - Detect (Alert only)
   - Kill & Quarantine
   - Mark as Threat

Protect

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.

Detect (Alert Only)

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.
In the **DETECTION ENGINES** section, select the **On-Write Engines** you want to use:

<table>
<thead>
<tr>
<th>On-Write Engine</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation</td>
<td>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.</td>
</tr>
<tr>
<td>Deep File Inspection</td>
<td>This is a preventive static AI engine that scans for malicious files written to the disk.</td>
</tr>
<tr>
<td>Deep File Inspection - Suspicious</td>
<td>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.</td>
</tr>
</tbody>
</table>

Select the **On-Execute Engines** you want to use:

<table>
<thead>
<tr>
<th>On-Execute Engine</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Behavior Tracking</td>
<td>This is a behavioral AI engine that implements advanced machine learning tools. It detects malicious activities in real-time, when processes execute.</td>
</tr>
<tr>
<td>Documents, Scripts</td>
<td>This is a behavioral AI engine on Windows devices that focuses on all types of documents and scripts.</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>This is a behavioral AI engine on Windows devices that detects attacks that are initiated by remote devices.</td>
</tr>
<tr>
<td>Anti-Exploitation/Fileless</td>
<td>This is a behavioral AI engine focused on exploits and all fileless attack attempts, such as web-related and command line exploits.</td>
</tr>
<tr>
<td>Potentially unwanted applications</td>
<td>This is a static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>This is a behavioral AI engine on Windows devices focused on insider threats such as malicious activity through PowerShell or CMD.</td>
</tr>
</tbody>
</table>

Click the switch to enable the **Web Protection Engine**. Green indicates *enabled* and gray indicates *disabled*.

Web Protection Engine, when enabled, provides protection against malicious web sites that host malware, trojans or worms that can damage, disrupt, attack or manipulate computer systems. It also blocks other types of software that can be covertly downloaded to collect information and monitor user activity.

**IMPORTANT:** To take advantage of Web Threat Protection, you must have the Capture Client Advanced Threat Protection and the legacy Content Filtering Client should be removed.

In the **DEVICE CONFIGURATION** section, select the device configuration options you want to use:

<table>
<thead>
<tr>
<th>Device Configuration Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User notifications</td>
<td>Sends the user a notification for each threat or suspicious activity.</td>
</tr>
<tr>
<td>Scan New Devices</td>
<td>Performs a full disk scan when a new device first registers with the management console.</td>
</tr>
<tr>
<td>Enable Logging</td>
<td>Saves logs for troubleshooting and support. Best practice is to keep this enabled.</td>
</tr>
</tbody>
</table>
### Device Configuration Options

<table>
<thead>
<tr>
<th>Device Configuration Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Anti-Tamper</td>
<td>Does not allow end users or malware to manipulate, uninstall, or disable the client. Best practice is to keep this enabled.</td>
</tr>
<tr>
<td>Enable Snapshots</td>
<td>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.</td>
</tr>
</tbody>
</table>

**e** Click **Update** to retain any changes.

5 Click on **Exclusions** tab. The **Exclusions** tab has several different types of exclusion lists: Hash, Path, Signer Identify, File Type, and Browser.

   a To add an exclusion, click the **+** (Add) button.
   
   b Select the **Type** from the drop-down menu.

   Depending on the type selected, additional fields appear.

<table>
<thead>
<tr>
<th>Exclusion Type</th>
<th>Fields Added</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA1 Hash</td>
<td>SHA1 Hash</td>
<td>Input the SHA1 Hash to be used.</td>
</tr>
<tr>
<td>Path</td>
<td>Path</td>
<td>Type the pathname in the field provided.</td>
</tr>
<tr>
<td></td>
<td>As</td>
<td>Select <strong>File</strong>, <strong>Folder</strong> or <strong>Folder and Subfolders</strong> from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>Monitor</td>
<td>Enable or disable monitoring. <strong>Exclusion Modes</strong> is enabled by default.</td>
</tr>
<tr>
<td>Signer Identity</td>
<td>Certificate ID</td>
<td>To find the certificate ID:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Go to <strong>Analytics &gt; Threats</strong> and select the relevant threat.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Copy the certificate ID from the <strong>Signer Identity</strong> field (in <strong>SUMMARY</strong> section).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Paste to <strong>Certificate ID</strong> text field on the <strong>Add Exclusion</strong> window.</td>
</tr>
<tr>
<td>File Type</td>
<td>File Type</td>
<td>Type in a file type as shown in the example.</td>
</tr>
<tr>
<td>Browser</td>
<td>Browser</td>
<td>Select the browser from the drop-down list.</td>
</tr>
</tbody>
</table>

   c Select the **OS** from the drop-down menu.
   
   d Enter a **Description**.
   
   e Select **Add** to save the exclusion.

**NOTE:** If you want to add more exclusions, check the box **Keep Open (Add Another Item)**. You can then add another exclusion without having to go back to the main window and select the **+** (Add) button again.

   Validate the Exclusion type in the table to see if your exclusion was added correctly.

6 Click **Device Control** tab.

Device control inheritance is enabled. Rules in the Global Device Control page are also enforced but policy rules always have higher priority over global rules. For information on adding and managing rules for global lists, see **Managing Device Control**.

**To manage device control inheritance:**

   1 Navigate to **Security Policies > Threat Protection**.
   
   2 Highlight the policy you want to apply the Device Control to and click the **Edit** icon.
3 Select the **Device Control** tab.

4 Click the **Settings** icon.

5 Click the switch to allow the settings and rules to be inherited from the globe device control policy. Green indicates enabled; gray indicates disabled.

6 Click Save.

You can also manage the rule configuration from the policy rules page. The same options are available to you as on the **Global Device Control** page. Highlight the rule and click on the Options icon to edit, copy, move, disable/enable, or delete a rule.

Click **GO BACK** to return to the Threat Protection policy list.

## Trusted Certificate Policies

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

**To define a Trusted Certificate policy:**

1 Navigate to **Security Policies > Trusted Certificates**.

2 ![Trusted Certificates](image)

2 Select + (Add).

3 ![Create Trusted Certificate Policy](image)

3 Type the new name in the **Policy Name** field.

4 Select **Create**. You may need to refresh your screen to see the new policy in the list.
5 Click on the **Edit** icon to define policy parameters.

6 Click on + to add this trusted certificate policy to the selected client policy.

7 Select the **CLIENT POLICY** to which you want to add the certificate policy, and click **Add**.

8 Click **Overview** tab.
   a Edit the policy name if needed.
   b Select whether the policy is enforced or not.
   c Click **Update**.

9 Click on the **Settings** tab.
   a Add or remove certificates in the OS Certificate Store 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.
   b Define Firefox support from the drop-down list, if needed.
   c To retain certificates on an endpoint when Capture Client is uninstalled, enable **Retain trust when Capture Client is uninstalled** option. The option is disabled by default.
   d Click **Update** to save the **CERTIFICATE TRUST** settings.
   e To add certificates to the **ENFORCED CERTIFICATES** section, click on + (Add).
f Highlight the certificate you want to add and click the + icon on that row. The selected certificate is added to the Certificates table.

g Click GO BACK to return to the Trusted Certificates list.

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.

**IMPORTANT:** If devices protected by Capture Client have Content Filtering Client (CFC) service enforced, the Web Threat Protection & Web-Content Filtering functionalities of CFC are implemented, even if the web-content filtering policy of Capture Client is enforced. In this case, it is recommended to abort CFC service.

To know the status of CFC enforcement on any protected device, right-click on the Capture Client icon on the desktop tray of the protected device. If CFC is enforced, it will be listed in the window.

**NOTE:** To configure web content filtering, the Capture Client Advance License is required.

There are several aspects to creating a strong content filtering policy. First it needs to be created, followed by editing it to set the parameters you want. Use the following steps to guide you:

- Adding a Web Content Filter
- Editing a Web Content Filter
- Customizing the Default or Timed Filter Features
- Localhost Filtering

Adding a Web Content Filter

*To create a web content filtering policy:*

1 Navigate to Security Policies > Web Content Filtering.
2. Click the **Add** icon and type the **Policy Name** in the field provided and click **Create**.

![Create Web Content Filtering Policy](image)

The policy appears in the table.

### Editing a Web Content Filter

Once you create a Web Content Filter, it is listed in the **Web Content Filtering** table at **Security Policies > Web Content Filtering page**. To configure the web content filter, hover over the policy and click the **Edit** icon.

![Web Content Filtering Table](image)

Navigate to each of the tabs and set the values on each. The following table provides more detail on each.

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usage</strong></td>
<td>To assign the web-content filtering policy to any of the Capture Client policies, click the <strong>Add</strong> icon, select the Capture Client policies and click <strong>Add</strong>. If the Capture Client policy you selected to associate with the web-content filtering policy is already associated with another web-content filtering policy, you will get an option to overwrite.</td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td>Set whether the web-content filtering policy is being enforced on the Capture Client policy associated with it.</td>
</tr>
</tbody>
</table>
| **Settings** | Customize several settings on this tab:  
  - Enable web content filtering.  
  - Choose to still enforce the policy even if the device is behind a SonicWall firewall.  
  - Define the type of Block page used (**default** or **customized**). |
| **Schedule** | Hover over **Timed Filter** and click the **Edit** icon to set the schedule during which the **Timed Filter** should be active. The **Default Filter** will be active at all the other times. |
Customizing the Default or Timed Filter Features

The Default Filter and Timed Filter tabs on the Edit option have several additional tabs where information needs to be set. They have the same settings so the following procedure applies to both.

1. Navigate to the filter you want to update and click Edit.
2. Select the Default Filter or Timed Filter tab, depending on the type of policy you want to build.
3. Define the Filter Settings.
   Enable or disable the features for General Settings or Filtered Events, as needed. Click to the Information icon for each setting for more details.
4. Click on Categories and select Forbidden Categories to be added to the filter, if desired. The default settings are Hacking/Proxy Avoidance System and Malware.
5. Click on Domains to set up the Allowed Web Domains and the Forbidden Web Domains.
6. Click on Keywords to create a list of keywords, which will block websites that contain any of the keywords listed.
   For HTTPS connections, websites containing a keyword in the domain will be blocked. For HTTP connections, a keyword anywhere in the URL will be blocked. E.g., the keyword 'guns' will block https://www.guns.com, http://www.example.com/search/?q=guns, etc...
7. Click on Processes to create a list of file paths of processes you wish to allow. For example: C:\Users\noobw\AppData\Local\NVIDIA Corporation\GeForceNOW.
   **NOTE:** System processes and those in the installed programs locations, for example: C:\Program Files\ are always allowed.
8. Click on Subject Names to create a list of subject names for processes you wish to explicitly allow.
   Enter a partial or full code signing certificate subject name for the processes you wish to explicitly allow. For example: 'CN=Microsoft Corporation'.
9. Click Update to save the policy parameters.
10. Click GO BACK to return to the Web Content Filtering table.

Localhost Filtering

Filtering local host traffic can be enabled or disable, as needed. Navigate to Security Policies > Web Content Filtering to set localhost filtering. In Filtered Events section, click the Filter requests to localhost switch to enable or disable.

If enabled (green), requests to the loopback interface is filtered in the same as requests to the network. This option is disabled by default.
Capture Client Policies

Capture Client policies are the top-level policies protecting a client. To view the Capture Client policies, navigate to Security Policies > Capture Client. The table lists all the Capture Client policies that have been created. Policies in this table are ordered in descending order of priority. When several policies could apply to a client, the policy with the highest priority is preferred. You can re-order them, or click on the arrowhead beside the status icon to expand the filter to see more detail.

Before defining a Capture Client Policy, create threat protection policy, web content filtering policy, and trusted certification policy that you want to associate with the Capture Client policy. To create these policies, see Threat Protection Policies, Web Content Filtering Policies, and Trusted Certificate Policies.

**NOTE:** When creating a Capture Client policy, always be sure to add a Threat Protection policy to it.

**To define a top-level Capture Client policy:**

2 Select + (the Add icon).

3 Type the new name in the Policy Name field.

4 Select Create. You may need to refresh your screen to see the new policy in the list.

5 Click on the Edit icon to define policy parameters for the new policy.

6 To assign users, user groups, or device groups to the policy:
   • Click +, select users from the list and then click Assign.
   • Click User Groups tab, click +, select groups, and then click Add.
   • Click Device Groups tab, click +, select groups, and then click Add.

7 Click on the Settings tab.
   a Select whether the policy is enforced or not.
   b In the drop-down list, select the Capture Client Version you want to enforce for this policy.
   c Check the box for the serial numbers of the enforced firewalls.
   d Click Update to save the changes.
8 Click on the Agent Policies tab.

NewPolicy

Usage Settings Agent Policies

<table>
<thead>
<tr>
<th>AGENT POLICY</th>
<th>AGENT POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Content Filtering</td>
<td>None (Do not overwrite)</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>None (Do not overwrite)</td>
</tr>
<tr>
<td>Trusted Certificate</td>
<td>None (Do not overwrite)</td>
</tr>
</tbody>
</table>

TIP: When several policies could apply to a client, the policy with the highest priority is preferred.

Assigning Capture Client Policies

You can assign capture client protection policies to either users, user groups, or device groups as required.

To assign client protection policies:
1 Navigate to Security Policies > Capture Client.
2 Find the policy that you want to apply and click the Edit icon.
   - To review or update the settings of the client policy click Settings.
   - To review or update the agent policies associated with the client policy click Agent Policies.
3 Click Usage.
4 Choose either the **Users**, **User Groups**, or **Device Groups**.

5 Click +.

6 Select the users, user groups, or device groups to assign the client policy, and click **Assign**.

   **TIP:** When using user-groups to assign policies, ensure that the target policy has a higher priority.

The assigned users, user groups, or device groups appear under their respective tabs. You can also view the client policy to verify whether the policy is assigned to specified users or groups.
The Configuration section of Capture Client gives you direct access to the tools for managing exclusions, blacklists, certificates, device control, and web protection domains.

**Topics:**
- Managing Exclusions
- Managing the Blacklist
- Managing Device Control
- Managing Certificates
- Managing Web Protection Domains

**Managing 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 **Configuration > 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

**IMPORTANT:** Items in the **Global Exclusions List** is enforced on all the devices associated with a tenant. To manage exclusions on devices associated with a Capture Client Policy, configure exclusion settings in the threat protection policy associated with the Capture Client policy.

**NOTE:** Multi-tenant administrators can copy an exclusion created for a tenant to all the other partner tenants at once. To make an exclusion global, see **Making Exclusions Global**.

**Hashes**

*To add a Hash exclusion:*
1. Navigate to **Configure > Exclusions**.
2. Select the **Hashes** tab.
3 Click the + button.
4 In the Type drop-down list, select SHA1 Hash.
5 Enter the hash string in the SHA1 Hash field.
6 Choose the OS from the drop-down menu.
7 Add a Description in the field provided.
8 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 Configuration > Exclusions.
2 Select the Paths tab.
3 Click the + button.
4 In the Type drop-down list, select Path.
5 In the OS field, select an operating system from the drop-down list.
6 Enter the path to a directory or file the Path field.
7 From the drop-down list in the As field, select the one of the following: File, Folder, or Folder and Subfolders.
8 Add a Description.
9 Select an Exclusion Mode. The options are defined below:

<table>
<thead>
<tr>
<th>Exclusion Mode</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress Alerts</td>
<td>Does not display alerts on any of the processes.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>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).</td>
</tr>
<tr>
<td>Interoperability—Extended</td>
<td>Reduces the monitoring level of the processes and their child processes.</td>
</tr>
<tr>
<td>Performance Focus</td>
<td>Disables monitoring of the processes associated with this path. You might select this option if monitoring these processes creates performance issues.</td>
</tr>
<tr>
<td>Performance Focus—Extended</td>
<td>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.</td>
</tr>
</tbody>
</table>

10 Click the Add button to save the exclusion.

**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. To get the Signer ID:
   a. Go to Analytics > Threats.
   b. Click on a threat that you want the Signer ID for.
   c. Look in the Summary section for the Signer Identity field. Either the signature is displayed and you can copy it or Not Signed is reported.
   d. Copy the Signer Identity string.

2. Navigate to Configuration > Exclusions.
3. Select the Signer Identity tab.
4. Click the + button.
5. Select Signer Identity from the drop-down list in the Type field.
6. Paste the signer ID from Step 1 in the Certificate ID field.
7. Choose the OS from the drop-down menu.
8. Add a Description.
9. Click the Add button to finalize your exclusion.
File Types

You can exclude specific file types from scanning.

To exclude particular file types:
1. Navigate to Configuration > Exclusions.
2. Select the File Types tab.
3. Click the + button.
4. In the Type field, select File Type from the drop-down list.
5. Enter the File Type.
6. Choose the OS from the drop-down list.
7. Add a Description.
8. 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 Configuration > Exclusions.
2. Select the Browsers tab.
3. Click the + button.
4. In the Type field, select Browser from drop-down list.
5. Select a Browser type from the drop-down list.
6. Choose the OS from the drop-down menu.
7 Add a Description.
8 Click the Add button to save the exclusion.

Making Exclusions Global

Multi-tenant administrators can copy an exclusion created for a tenant to all the other partner tenants at once.

To copy an exclusion to all the active tenants:

1 Navigate to Configuration > Exclusions.
2 Click the type of exclusion that you want to copy to all the tenants.
3 Hover over the exclusion, click <Make Global> icon.
4 Select Action Approved.
5 Click copy on all tenants.

Managing the Blacklist

With the Blacklist feature you can chose to block known threats or unwanted files by curating a list of denied files.
To set up the Blacklist:

1. Navigate to Configuration > Blacklist.

2. Click the + button.

3. Select an operating system from the OS drop-down list.
4. Input a SHA1 hash for the file you wish to have blocked.
5. Add the Description in the field provided.
6. Click the Add button to add the item to your blacklist.

Blacklisting a Threat

To blacklist a known threat:

1. Navigate to Analytics > Threats.
2. Click on a threat for more details.
3. Click More Actions drop-down box, click Add to blacklist.
Managing 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 malware threats from spreading via USB devices and also to prevent data exfiltration. 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.

Adding Rules for Global Lists

*To create a new rule:*

1. Navigate to **Configuration > Device Control**.
2. Click the **Add icon**.
3. Enter the **Rule Name** in the field provided.
4. Select the **Interface** from the drop-down list.
5. Choose to either **Allow** or **Block** the action.
6. Select the **Criterion** for the rule from the drop-down list. The options include:
   - Class
   - Vendor ID
   - Product ID
- Device serial number
Additional fields are displayed, depending on the option you chose.

To obtain the serial number of a particular USB device to be blocked/allowed:

**Prerequisite**: A rule that allows all the USB devices should be effective.

a. Navigate to Configuration > Device Control.
b. Click settings icon, and select **Report “approved device” events to activity log**.

c. Click **Save**.
d. Navigate to Analytics > Activity and filter the events to list the approved events under Device Control.
e. Locate the USB device log event and click **View event details** to see details of the device.

f. In the **DEVICE CONTROL EVENT** dialog, you can locate the serial ID of the USB device.

| NOTE | You can also block the USB device from **DEVICE CONTROL EVENT** dialog. |
7 Provide the additional information required for the rule.

8 To Enable rule immediately after saving, verify that the box is checked. Uncheck the box if you want to define the rule, but not enable it immediately.

9 Click Create to save the rule.
Managing Rules for Global Lists

You can manage the rule by using the Options icon that appears when you highlight the rule. The options include:

- Edit
- Copy
- Move
- Disable/Enable
- Delete

**To edit a rule:**

1. Navigate to Configuration > Device Control.
2. Highlight the rule you want to change and click on the options icon at the end of the line.
3. Select Edit.
4. Make the changes to the fields you want.
   - **NOTE:** You can edit only the fields that are enabled for editing.
5. Click Submit.

**To copy or move a rule:**

1. Navigate to Configuration > Device Control.
2. Highlight the rule you want to change and click on the options icon at the end of the line.
3. Select Copy or Move.
4. Select a destination from the list and confirm.
   - **NOTE:** To move or copy multiple rules, check the box on the left to select the rules; then follow the same steps as above.

**To enable or disable a rule:**

1. Navigate to Configuration > Device Control.
2. Highlight the rule you want to change and click on the options icon at the end of the line.
3. Select Disable or Enable. A message verifies the new state for the rule.
To delete a rule:

1. Navigate to Configuration > Device Control.
2. Highlight the rule you want to change and click on the options icon at the end of the line.
3. Select Delete.
4. Check the box to confirm that you want to delete the rule.
5. Click Delete.

**NOTE:** You can also enable or disable a rule by clicking on the checkmark by the rule name. A green check indicates that the rule is enabled. A gray check indicates that the rule is disabled.

**Managing Certificates**

You can manage the certificates by going to Configuration > Certificates:

The Certificates table lists the certificate names being used, information about the public key, when the license was put in place (valid from), and when it’s valid to. Below the table, you can see a graphical view of the certificates and when they expire.
To see more information on a specific certificate, hover over the certificate and click the View icon.

To delete a certificate, hover over it and click on the Delete icon.

You can easily upload a certificate by clicking on the Upload icon. Then drag-and-drop certificates to add them to the list or navigate to the file by selecting Choose File.
Managing Web Protection Domains

When you enable web threat protection, Capture Client automatically monitors and blocks any known malicious websites, for example, sites that have been rated as Malware or Hacking/Proxy Usage. If a website, for example: www.safevpn.com (rated as Hacking/Proxy Avoidance Systems) is blocked incorrectly by the Web Protection agent, add the website to the web protection domains to allow access to it on all your devices.

To add a domain:

1. Navigate to Configuration > Domains.
2. Click +.

3. In the ADD TRUSTED DOMAIN window, enter a website that you want to whitelist in the Domain box and enter a Description.
4. Click Add.
Topics:

- Viewing License Usage Statistics
- Tenant Settings
- Tenant Customization
- Configuring Notifications
- Managing Administrators
- Client Installers
- Support for Linux Endpoints
- Managing Client Upgrades
- Reviewing the API

Viewing License Usage Statistics

Navigate to **Management** > **Licenses** to view statistics of usage of licenses.

The Licenses table lists the agents being used and the vendor that provides them. The usage of those licenses are shown in bar graph along with the number used and the number available listed under it. The table also lists when the license was put in place (valid from) and when it is valid to.
Tenant Settings

On the Tenant Settings page, you can manage the tenant settings associated with a tenancy.

1. Navigate to Management > Tenant Settings.

   In the TENANT SETTINGS section, the Tenant Name and Tenant ID is displayed.

2. In the ENFORCED FIREWALLS section:
   - To add firewalls, enter the Firewall Serial number and click Add. The firewalls that are registered are displayed in Registered Firewalls.
   - To remove the registered firewalls, enter the Firewall Serial number and click Remove.

3. In the ADMINISTRATOR ACCOUNT SETTINGS section:
   - Set the Auto-Logout duration. This sets the time for how long users can be inactive before they are logged out.
   - Enable Password Complexity if you want. If enabled:
     - Specify how many numbers the password must include.
     - Specify the number of special characters the password must include.
     - Specify the numbers of lower case characters the password must include.
     - Specify the numbers of upper case characters the password must include.

4. In the DEVICE MANAGEMENT section:
   - To schedule device upgrades, click Edit next to Perform Upgrades At and set the schedule as required. Click Save.
   - Enable or disable Device File Fetch Feature.
     The Device File Fetch feature is disabled by default. To enable the feature:
     a) Click Device File Fetch Feature button.
The button turns green.

b) Click Update and approve the license agreement.

- 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.

5 Click Update.

**Tenant Customization**

Tenant customization enables administrators to add a custom logo in the reports and to include a custom message that helps users to contact IT support easily.

On the **Tenant Customization** page, you can manage the tenant customization associated with a tenancy.

**NOTE:** The custom logo appears on the first page of a report; the custom message that you enter is displayed in the Support tab on the Capture Client console.

**NOTE:** Tenant customization isn’t supported in Linux endpoint devices.

To configure tenant customization:

1. Navigate to **Management > Tenant Settings**.
2. Click **Tenant Customization**.

To set a new logo in the reports:

a) In the **REPORT CUSTOMIZATION** section, click **Change**.

b) Click **Choose File** and select the logo and click **Open**.
c  Click **Upload**.

4  To include a custom note in the Capture Client console:
   a  In the **CLIENT CUSTOMIZATION** section, enter appropriate text in the **Custom Support Info** box.
   b  Click **Preview** to see how the message is displayed in the Capture Client console on endpoint devices.
   c  Click **Update**.

The custom message appears in the **SUPPORT** section in the client UI.

![SonicWall Capture Client](image)

### Configuring Notifications

You can customize alerts and notification settings to notify you of the things you are most concerned with. Navigate to **Management > Notifications**.
Topics:

- Email Settings
- Notifications Settings—Threats
- Notifications Settings—Device Events
- Notifications Settings—License
- Notifications Settings—Management

### Email Settings

**To enable the email settings for your notifications:**

1. Navigate to Management > Notifications.
2. Enable Email Settings.
3. 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.
4. Type in the Email Recipients in the field provided. Separate email addresses by a comma (,) or semicolon (;).
5. Select the default Time Zone from the drop-down list.
6. Click Save to retain the new settings.

### Notifications Settings—Threats

**To set up notifications for threats:**

1. Navigate to Management > Notifications.
2. Under the Notifications Settings heading, select the Threats tab.
3 Slide the switch 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
4 Slide the switch to green for each type of threat for which you want to **SEND EMAIL**.
5 Slide the switch to green for each type of threat for which you want to **CREATE** an **ALERT**.
6 To customize a threat’s settings:
   a Mouse over a threat type to highlight it.
   b Click on the **Edit** icon.
   c Select the **Alert Severity** from the drop-down list. The options are:
      - **Critical** (dark red)
      - **High** (bright red)
      - **Major** (orange)
      - **Minor** (yellow)
      - **Low** (light yellow)
      - **Info** (green)
   d To send an email when the event occurs, enable **Send Email**.
   e To create an alert that is reported in the **Notification Center**, enable **Create Alert**.
   f Click **Confirm** to save the settings.

### Notifications Settings—Device Events

*To set up notifications for device events:*

1 Navigate to **Management > Notifications**.
2 Under the **Notifications Settings** heading, select the **Device Events** tab.
3 Slide the switch 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

4 Slide the switch to green for each type of device event for which you want to SEND EMAIL.

5 Slide the switch to green for each type of device event for which you want to CREATE an ALERT.

6 To customize a device event’s settings:
   a Mouse over a device event type to highlight it.
   b Click on the Edit icon.
   c Set the Activity Threshold (days) by incrementing or decrementing the count.

   d Select the Alert Severity from the drop-down list. The options are:

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

e. To send an email when the event occurs, enable Send Email.

f. To create an alert that is reported in the Notification Center, enable Create Alert.

g. Click Confirm to save the settings.

Notifications Settings—License

To set up notifications for licensing:

1. Navigate to Management > Notifications.
2. Under the Notifications Settings heading, select the License tab.
3. Slide the switch to green for each type of license event you want to be notified about. The options include:
   - License Expiring Soon
   - License Expired
4. Slide the switch to green for each type of license event for which you want to send email.
5. Slide the switch to green for each type of license event for which you want to create an alert.
6. To customize a license event’s settings:
   a. Mouse over a license type to highlight it.
   b. Click on the Edit icon.
   c. Select the Alert Severity from the drop-down list. The options are:
      - Critical (dark red)
      - High (bright red)
      - Major (orange)
      - Minor (yellow)
      - Low (light yellow)
      - Info (green)
   d. To send an email when the event occurs, enable Send Email.
   e. To create an alert that is reported in the Notification Center, enable Create Alert.
   f. Click Confirm to save the settings.
Notifications Settings—Management

To set up notifications for management functions:

1. Navigate to Management > Notifications.
2. Under the Notifications Settings heading, select the Management tab.

3. Slide the switch 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

4. Slide the switch to green for each type of license event for which you want to send email.

5. Slide the switch to green for each type of license event for which you want to create an alert.

6. To customize a management activity’s settings:
   a. Mouse over a management activity to highlight it.
   b. Click on the Edit icon.
   c. Select the Alert Severity from the drop-down list. The options are:
      - Critical (dark red)
      - High (bright red)
      - Major (orange)
      - Minor (yellow)
      - Low (light yellow)
      - Info (green)
   d. To send an email when the event occurs, enable Send Email.
To create an alert that is reported in the Notification Center, enable Create Alert.

Click Confirm to save the settings.

Managing Administrators

The Administrators page provides a consolidated list of the administrators associated with the tenancy. You can add, edit, and delete administrators from this page. You can also export administrators details as a CSV file.

Adding a New Administrator

To add a new administrator:

1. Navigate to Management > Administrators.
2. Click the + button.
3. Add the Email for the new administrator.
4. Enter the Name of the new administrator.
5. Select the administrator’s role from the drop-down list. Options include:

<table>
<thead>
<tr>
<th>Role</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewer</td>
<td>Has viewing privileges; can see administrative settings, but does not have permission to make any changes to the settings.</td>
</tr>
<tr>
<td>Admin</td>
<td>Has administrative privileges for the tenancy the administrator was set up on.</td>
</tr>
</tbody>
</table>

6. Set the Inactivity Logout period. The administrator is logged out after this period expires. If you set the value to 0 the system uses the global idle logout period.

7. Set and confirm the password for the administrator. The password must be 8-30 character if password complexity is disabled.

8. Click Create.

Resetting Administrator's Password

To reset the administrator’s password:

1. Navigate to Management > Administrator.
2. Find the administrator you want to update in the Administrator table. You can filter, search or browse through the pages.
3 Highlight the administrator you want to update by mousing over it and select the **Edit** icon that appears on the right.

4 Enter the **Current Password**.

5 Type the **New Password**.

6 **Confirm New Password**.

7 Click **Update**.

### Deleting an Administrator

**To add a new administrator:**

1 Navigate to **Management > Administrators**.

2 Find the administrator you want to delete in the Administrator table. You can filter, search or browse through the pages.

3 Highlight the administrator you want to update by mousing over it and select the **Delete** icon that appears on the right.

4 Approve the request to delete the administrator.

5 Confirm that the administrator was removed from the list.

### Exporting Administrators details as a CSV file

**To export administrator details as a CSV file:**

1 Navigate to **Management > Administrators**.

2 Click **Export as CSV** <icon> in the upper-right corner of the page.

The file is downloaded to your system.

### Client Installers

Several different versions of the Capture Client are available for the endpoints.

1 Navigate to **Management > Client Installers**.

2 Hover over the Capture Client version you want to download and then click on the Windows or macOS or Linux icon.

**NOTE:** The recommended client version is indicated by a **star** icon next to it.
Depending on the OS, do the following:

- **Windows or macOS**
  a) Run the installer file.
  b) 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.

- **Linux**
  a) Make the downloaded shell script executable (chmod 755).
  b) Run the script on a compatible Linux device. A series of messages are displayed as the installation process runs. The final message indicates when activation is complete and your device is protected.

The SentinelOne Linux agent is installed and provisioned for your tenant.

**Support for Linux Endpoints**

By leveraging the native SentinelOne Linux agent, Capture Client now protect Linux endpoints from malware. It allows autonomous detection and protection to function in a mission-critical datacenter or in a standalone/disconnected network. To protect Linux endpoints, see Client Installers.

**NOTE:** Linux endpoint devices do not support Capture Client UI.

Listed are the features that are not supported for Linux devices:

- Device control
- Web Protection
- Firewall enforcement
- Rollback
- Capture ATP

**Managing Client Upgrades**

You can choose to upgrade client software on devices either manually or let SonicWall manage the upgrades.

- **Self Managed**
- **SonicWall Managed**

**Self Managed**

If you choose the self-managed option, you control which version of the client gets installed on your devices by manually updating the required client version in the Capture Client policy.

**NOTE:** The Linux installer is available only for Capture Client version 3.0.x or later.
To configure the client software upgrade as self-managed:

2. Hover over the Capture Client policy you want to update and click the Edit icon.
3. Click the Settings tab.
4. From drop-down list for the Capture Client version field, select any self-managed Capture Client version you want this current policy to enforce and click Update.

The Client policy would then enforce the new upgrade onto all the devices associated with it.

To push the updated Capture Client policy on to a client machine instantly, go to Protection > Devices page, hover over the device, click gear icon, and select Update Policy.

SonicWall Managed

If you let SonicWall manage the Capture Client version upgrades to the client machines, any latest available version that SonicWall releases and promotes will be pushed to the client machines by automatically updating the Capture Client Policy.

To configure client software upgrade as Sonicwall-managed:

2. Hover over the Capture Client policy that you want to update and click the Edit icon.
3. Select the Settings tab.
4. From drop-down list for the Capture Client version field, select any one of the available SonicWall managed versions policy and click Update.
The Client policy would then enforce the new upgrade onto all the devices associated with it.
To push the updated Capture Client policy on to a client machine instantly, go to Protection > Devices page, hover over the device, click gear icon, and select Update Policy.

Reviewing the API

Documentation for the public APIs used within SonicWall Capture Client can be accessed from the product.

To review the public APIs:

1. Navigate to your login ID in the upper-right corner and click on your initials.

2. Select API Docs. The API documentation opens in a separate window so you can review it.

The APIs are grouped by topic. The topics are listed alphabetically in the left menu, and the APIs within each group are listed alphabetically as well. You can filter the list to more easily find the specific API you want. Just enter a search string in the Filter... field and the results are shown immediately. Click on the X in Filter... field to clear the filter.
Part 2

Monitoring

- Dashboard
- Statistics
- Analytics
- Alerts and Notifications
The Dashboard menu page is the landing page for the console and also the first place to monitor for alerts and threats.

**Topics:**
- About the Dashboard
- Investigating and Responding to Active Clients
- Investigating and Responding to Active Users
- Enforce Trusted Certificates
- Investigating and Responding to Risky Applications

### About the Dashboard

At the top of the page, you can see a quick summary of the Capture Client performance by looking at the counts across the top of the page. They identify:

- **ONLINE CLIENTS**
- **PROTECTED DEVICES**
- **USERS**
- **TRUSTED CERTIFICATES**
- **LICENSES**
Threats Detected

In **THREATS DETECTED** section, four different tiles providing numerical data points about threats. The tiles include:

- **ACTIVE THREATS** — the number of threats that are currently active.
- **SUSPICIOUS ACTIVITY** — the number of suspicious items that were detected and have not been resolved.
- **MITIGATED THREATS** — the number of threats identified and mitigated per the policies.
- **BLOCKED THREATS** — the number of threats blocked per the policies.

Device Health

In the **DEVICE HEALTH** section, three different tiles providing numerical data points about infected devices, vulnerable applications, and offline device alerts. The tiles include:

- **INFECTED DEVICES** — the number of devices that have active threats and require immediate attention.
- **VULNERABLE APPS** — the number of applications (across all devices) that are not upgraded with the latest patches, therefore vulnerable to exploits.
- **OFFLINE DEVICE ALERTS** — the number of alerts.

Web Protection

In the **Web Protection** section, there are two tiles: **TOP BLOCKED CATEGORIES** and **TOP BLOCKED DOMAINS**.

- **TOP BLOCKED CATEGORIES** — the categories that are blocked as per the web content filtering policy that is associated with the protected devices. For example: Hacking, Malware. Categories: Hacking and Malware are selected by default in a newly created Web Content Filtering Policy.

- **TOP BLOCKED DOMAINS** — the websites that are blocked as per the web content filtering policy. Each Forbidden Web Domains explicitly blocks all URLs for the configured domain.

Click on **TOP BLOCKED CATEGORIES** or **TOP BLOCKED DOMAINS** to analyze the web protection events. For more information, see [Web Protection](#).

You can take further action on the Dashboard information by clicking on the Options, or gear, icon at the top of the Dashboard. The table below provides more detail on what each action does:
### SonicWall Capture Client 3.0 Operations

#### Dashboard

- **Unresolved Detections**

  The bottom of the **Dashboard** shows the **Unresolved Detections** section. The slider options allow you to select the time period displayed in the table. Options range from **last 5 min** to **All**; the default is **last month**. Double-click on any threat to expand the information to see **Threat Status** and **Threat Details**. From this page you can **Disconnect Network** or select **More actions**.

### Action Instructions and Information Path to Page

<table>
<thead>
<tr>
<th>Action</th>
<th>Instructions and Information</th>
<th>Path to Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze threats</td>
<td>Threat Investigation</td>
<td>Analytics &gt; Threats</td>
</tr>
<tr>
<td>Configure security policies</td>
<td>Threat Protection Policies</td>
<td>Security Policies &gt; Threat Protection</td>
</tr>
<tr>
<td>Manage exclusions</td>
<td>Managing Exclusions</td>
<td>Configuration &gt; Exclusions</td>
</tr>
<tr>
<td>View blacklist</td>
<td>Managing the Blacklist</td>
<td>Configuration &gt; Blacklist</td>
</tr>
<tr>
<td>View all devices</td>
<td>Investigating and Responding to Active Clients</td>
<td>Protection &gt; Devices</td>
</tr>
<tr>
<td>View all users</td>
<td>Investigating and Responding to Active Users</td>
<td>Protection &gt; Users</td>
</tr>
<tr>
<td>Configure client policies</td>
<td>Security Policies</td>
<td>Security Policies &gt; Capture Client</td>
</tr>
<tr>
<td>Configure licenses</td>
<td>Viewing License Usage Statistics</td>
<td>Management &gt; Licenses</td>
</tr>
<tr>
<td>Download report</td>
<td>Generating Reports</td>
<td>Analytics &gt; Reports</td>
</tr>
<tr>
<td>Download client installers</td>
<td>Client Installers</td>
<td>Management &gt; Client Installers</td>
</tr>
</tbody>
</table>

---

**cmd.au8**

**THREAT STATUS**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DETECT</td>
<td>Detect and classify the threat as malicious.</td>
</tr>
<tr>
<td>APPROVE</td>
<td>Approve the threat as non-malicious.</td>
</tr>
<tr>
<td>QUARANTINE</td>
<td>Quarantine the threat.</td>
</tr>
<tr>
<td>BLOCK</td>
<td>Block the threat.</td>
</tr>
</tbody>
</table>

**Threat Details**

- **File Info**
  - **Name**: cmd.au8
  - **Type**: Unknown
  - **Hash**: 00000000
  - **Size**: 0 bytes
  - **File**: 00000000
  - **Start**: 00000000
  - **End**: 00000000
  - **MD5**: 00000000

- **Suspicious Activity**
  - **File Name**: cmd.au8
  - **Image History**: Unknown
  - **File Version**: 0

- **Suspicious Data**
  - **Suspicious Bytes**: 0
  - **Suspicious Bytes Count**: 0

- **Suspicious Operations**
  - **Suspicious Operations Count**: 0
  - **Suspicious Operations**: 0

---

**License Usage**

- **License Information**
  - **License Type**: Enterprise
  - **License Count**: 0
  - **License.expiration**: Unknown

---

**Client Installers**

- **License Information**
  - **License Type**: Client Installers
  - **License Count**: 0
  - **License.expiration**: Unknown

---

SonicWall Capture Client 3.0 Operations

Dashboard
Online Clients

To view the Online Clients section of the Dashboard, select the Online Clients option listed under the tiles.

Click on the name of a client to see details. The default is the Overview tab, but select the other tabs to see other information that can help with diagnostics.

You can also take other actions on the ONLINE CLIENTS. Hover over the client you want until the Options Icon (gear icon) appears and click on it. You can click on any command on the list to take the appropriate action.

Investigating and Responding to Active Clients

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

To view the list of endpoints and take any actions, navigate to Protection > Devices.
View Clients

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

Once the list of devices shows, you can either search for a specific endpoint using the Search box, or you can directly click on any of the devices you would like to investigate.

You can also export the device details to a CSV file by clicking on the Download Device icon on the upper-right corner of the page.

Monitoring and Managing the State of Devices

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

To collect information for troubleshooting or to manage state of the device, click on the Options icon on this page and select:

- **Send Logs** or **Send TSR** to pull specific data from the endpoint for investigation purposes
- **Update Policy** to update the Endpoint Policy assigned to the user
- **Uninstall Client** to uninstall Capture Client from the endpoint
- **Decommission** to decommission Capture Client from the endpoint
The key data points to be observed here are the three icons at the top of the Overview tab that represent the state of the endpoint. The green colored icons represent a healthy state while red icons indicate that a problem with that device.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Icon" /></td>
<td>Commissioned—Capture Client is installed and running on the device</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Decommissioned—Capture Client is not running on the device</td>
</tr>
<tr>
<td><img src="image" alt="Green Icon" /></td>
<td>Activated—The device can access the network</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>The device is unavailable when red</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Pending connectivity information when gray</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Offline (Capture Client console offline, SentinelOne console offline)</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Online when green (Capture Client console online, SentinelOne console online)</td>
</tr>
<tr>
<td><img src="image" alt="Red Icon" /></td>
<td>Either Capture Client console or SentinelOne console is offline</td>
</tr>
</tbody>
</table>

- **Commissioned**—This state means that Capture Client was detected on the endpoint and it is running in a healthy state.
  - **Possible Problem**—The Capture Client was recently uninstalled or is not functioning properly on this device.
  - **Resolution**—This may require an uninstallation/reinstallation of the Capture Client package. Navigate to **Management > Client Installers** for the package.
- **Activated**—This state means that the device on which Capture Client is running is connected to the network and can access the network.
  - **Possible Problem**—The Capture Client and/or any of its modules needs an upgrade to the most current version. The device is unavailable when the icon is red; pending connecting information when gray.
  - **Resolution**—Navigate to **Settings > Client Settings** for the package and roll out the latest version of the package.
- **Online**—This state means that this device is up and running and is communicating with the Cloud Management Console.
  - **Possible Problem**—The endpoint is disconnected from the network and cannot communicate with the Client Management Console. If you see the icon in yellow, the device can either communicate with Cloud Management Console or SentinelOne.
  - **Resolution**—Validate with the user that the endpoint is up and running and online. If yes, then check for any firewalls or network connectivity issues that may be impacting connectivity to the console. Check the Logs folder in the Capture Client installation folder for the endpoint for any connectivity errors. If no error is identified, attempt a reboot of the system to restore it to a good state.

**NOTE:** Even if the device is offline, the device is still protected.
Reviewing Processes Running on a Device

Capture Client also obtains the list of processes running on an endpoint at any given time. Knowing what processes are running can be useful in malware incident investigations, but can also give you an idea of whether a dubious application or process is being run on the endpoint. By clicking on the Processes tab on the Devices page (Protect > Devices), you can see the entire list of processes running on that endpoint. You can also search for specific processes by name or filter the list if you are looking for a specific process.

You can easily build bulk exclusions from the Processes tab of any device. Simply select the process or set of processes and then click on the gray checked shield in the upper right corner above the table. This icon Adds paths to exclusions. You can even search for processes belonging to a specific application or vendor (for example, Apple or Adobe) and exclude all their applications.

You can also de-list processes on the Processes tab (remove them from the Exclusions list). Those processes that are already excluded are identified by a gray checked shield at the end of the name. Select all those processes that your want to de-list, and click on the gray shield with the x. This icon Removes paths from exclusions.

Reviewing Policies Enforced on a Device

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

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

Clicking on any user entry opens an overview page that shows the user’s profile information as well as devices registered to that user; refer to Active Users for more information. Clicking on that device open up details of the state of that device; refer to Active Clients for more information.

Click on the Policies tab to see what policies have been assigned to this user. This page also allows for manual modification of policies assigned to this user. Refer to Capture Client Policies for more information.
Enforce Trusted Certificates

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

![Trusted Certificates](image)

When a certificate is expanded, the **Trusted Certificate** page displays the following information:

- **POLICY INFO**: Displays information about the Trusted Certificate Policy such as policy name, required version, enforced firewalls, and last changed (time and date when the policy was modified for the last time.)

- **POLICY SETTINGS**: Displays certificates associated with the Trusted Certificate Policy

- **USAGE**: Displays Capture Client Policy names to which the Trusted Certificate policy is associated.

A search function is also provided so you can more easily find a specific policy.

Investigating and Responding to Risky Applications

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

**NOTE**: For this feature to function, the Capture Client Advance License is required.

The Dashboard displays the number of vulnerable apps across all devices associated with a tenant.
To investigate and respond to vulnerable applications:

1. Click VULNERABLE APPS box in the dashboard or navigate to Analytics > application Risk for the list of vulnerable applications.

   The table on the Application Risk page lists the unpatched applications and displays a risk level for each. You can sort the applications based on their risk level by clicking the upward/downward arrow next to RISK LEVEL in the header row. The risk levels are:

   - Critical (dark red)
   - High (bright red)
   - Medium (orange)
   - No known risk (green)
2 You can choose to filter the vulnerable apps with **device type**, **OS**, and (or) **risk level** to attend to the vulnerable apps on your priority.

![Application Risk Dashboard](image)

3 For more information about vulnerabilities in each application, hover over the application until the **View** icon appears at the end of the line. Click **View** to see details about **APPLICATION INFO** and **KNOWN VULNERABILITIES**. A risk level and CVSS (Common Vulnerability Scoring System) base score are listed for each vulnerability along with a description and date published.

![Known Vulnerabilities for Microsoft .NET Framework 4.8](image)

4 You can export the filtered list of vulnerable applications into a CSV file that helps to prioritize patching of applications.
Capture Client offers the ability to review statistics on the health and threat trends for the Capture Client deployment on the network.

To review statistics and trends:

1. Navigate to Overview > Statistics.
2. Under the Threats tab, review statistics for Threats, including a grouping of threats by their status in the network, their evolution over time, and a grouping by threat classification.
3. Under the Advanced Threat Protection tab, review the current state of the threats (blocked or whitelisted) that are analyzed by Capture ATP, their evolution over time.
4. Under the Application Risk tab, review application risk summary and data of applications with vulnerabilities.
5. Under the Web Protection tab, review the categories to which the blocked websites belong to and the total number or percentage of blocked websites belonging to each category. The graphical representation of blocked-website categories data and evolution of blocked events over time helps in the analysis.
6. Under the Devices tab, review statistics for protected endpoints, including a grouping by their commissioning status, evolution of how devices are added to the network over time, and a list of devices that need an administrator’s attention.
The Analytics options provide valuable information that can help with diagnostics.

**Topics:**
- Threats
- Downloading Threat File
- Downloading Device Files
- Web Protection
- Activity
- Logs
- Reports

**Threats**

Navigate to Analytics > Threats to see the list of threats found by Capture Client.

At the top of the page, you can see the icons that allow you to:

- Filter the list: Check the boxes for the **Status** and **Classification** options you want to filter on.
- Search: Enter the search string after clicking on the **Search** icon.
- Detailed view: click to expand the options in the table. Click it again to return to the simple view.
Double-click on a threat to expand it and see the details on the Threat Details page.

Once you expand the threat, you have access to additional actions. You can click on Disconnect Network to disconnect the device from the network.

You can click on Download drop-down tab and select the required format (pdf, json, or csv) to download the threat report. To download threat file, see Threat Files.

You can also select the More Actions drop-down list, which provides other actions you can take on the threat.

When done with the threat details, scroll down to the bottom of the page and click on GO BACK to return to the Threat list.

### Downloading Threat File

**To download a threat file:**

1. Navigate to Analytics > Threats.
2. To find a threat:
   - Filter the list: Check the boxes for the Status and Classification options you want to filter on.
   - Search: Enter the search string after clicking on the Search icon.
3. Click on the threat to expand it and see details on the Threat Details section.
4. Click on Download drop-down tab in the Threat Status section and select Threat File.
5 Enter the **Password** and confirm to protect the ZIP file archive that will contain the threat.

6 Click **Download**.

A request is sent to the client to upload the threat file in a password-protected ZIP file. The file is uploaded to the console and made available on the **Threats Files** page. Files uploaded to the console are deleted after 3 days, or earlier if more than 15 files are uploaded.

7 Navigate to **Analytics > Threats Files**.

8 Hover over the threat file, click on the download icon and approve to download the threat file to your system.

---

**Downloading Device Files**

Capture Client enables you to download up to ten device files, up to 10 MB size, in a single request from any of your clients. These files may contain sensitive data. The files are packed as a ZIP archive encrypted by a password that you set.

**NOTE:** You can download files only from Mac OS devices.

**To download device files:**

1 Navigate to **Management > Tenant Settings**.

2 Enable the device fetch feature if you haven’t:
   a Click **Device File Fetch Feature** button.
      The device fetch feature is disabled by default. The button turns green when enabled and gray otherwise.
   b Click **Update**.
   c Approve the legal agreement and click **Confirm**.

3 Navigate to **Analytics > Threat Files**.

4 Click **+**.

5 Select the device from **Device** drop-down box.

6 Enter the full path of the file that you need to download and click **Add**; enter additional file paths if needed and click **Add**.

7 Enter the password for the ZIP archive file.
   Click the question mark icon to see the password constraints.

8 Click **Request Files**.
   The ZIP file is available on the **Threat Files** page.

9 Hover over the file and click the download icon to download the file to your system.
Web Protection

To monitor Web Protection events:

1. Navigate to Analytics > Web Protection.

2. Under the Events tab, review individual events triggered by Web Protection engine and Web Content Filtering policy.

For information on enabling web protection engine and web-content filtering policy, see Threat Protection Policies and Web Content Filtering Policies.

3. Under the Blocked Web Sites tab, review statistics for actual malicious websites visited, including which users attempted to visit them and how many attempts were blocked.

You can choose to whitelist the websites that are listed in the Events tab and Blocked Web sites tab:

<table>
<thead>
<tr>
<th>CAUTION: Whilisting these websites might lower protection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a Hover over the blocked website and click Add to whitelist icon that appears at the end of the row.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>b In the confirmation dialog, select Action Approved, and then click Confirm.</td>
<td></td>
</tr>
</tbody>
</table>
Activity

The Activity page displays the activity as reported by SentinelOne. The time period for the data can be adjusted by sliding the orange marker along the scale at the top of the list. The predefined options for the scale ranges from last 5 min to all.

Logs

Logs are generated from both Capture Client console and endpoints. Both management logs and device logs are recorded. Access each by navigating to Analytics > Logs and then selecting the appropriate tab.

Management Logs
The time period for the Management logs can be adjusted by sliding the orange marker along the scale at the top of the list. The predefined options for the scale ranges from **last 5 min** to **all**.

At the top of the page, you can see the icons that allow you to:

- Filter the list: Check the boxes for the **Priority** options you want to filter on.
- Search: Enter the search string after clicking on the **Search** icon.
- Email logs: Click the icon and confirm that you want to email the tenant logs to yourself.
- Download logs: Click the icon and confirm that you want to download the tenant logs.

### Devices Logs

The time period for the Management logs can be adjusted by sliding the orange marker along the scale at the top of the list. The predefined options for the scale ranges from **last 5 min** to **all**.

At the top of the page, you can see the icons that allow you to:

- Filter the list: Check the boxes for the **Priority** and **Device** options you want to filter on.
- Detailed view: click to expand the options in the table. Click it again to return to the simple view.
- Email logs: Click the icon and confirm that you want to email the tenant logs to yourself.
- Download logs: Click the icon and confirm that you want to download the tenant logs.

### Reports

Capture Client offers the ability to generate distributable reports on the health and threat trends for the Capture Client deployment on the network. Reporting is an important function that allows administrators to review how their network is being protected, what gaps exist, how threats are being addressed and what actions they may need to take. The various reports can help communicate the value of deploying Capture Client endpoint protection to the business stakeholders.
Generating Reports

To generate a distributable statistics report:

1. Navigate to Analytics > Reports.
2. Click Request Report tab.
3. Enter a name for the report that is being generated in the Report Name field and select the time period for the data to be included in the report in the Time Period field.
4. Choose what sections and types of data should be included in the report. As you change options, the contents list changes.
5. To generate the report:
   - To download the report to your system, select Download, and click Request Report.
   - To send the report to your Email account, select Email, click Request Report. In the EMAIL REPORT dialog, select the administrators email ID available in the dropdown or enter the email ID, and click Send. You will receive the report as an email attachment from the SonicWall team.

\[\text{\textbf{NOTE: You can select multiple email accounts as recipients of the report.}}\]

The reports that are generated are available for download in the Available Reports page. To download the report, hover over the report and click Download icon that appears at the end of the row.

The reports that are sent through email are displayed on the page.

Scheduling Reports

Capture Client enables administrators to configure automated reports that are delivered at regular intervals for the Capture Client deployment on the network. Scheduled reports help administrators to review the health and threat status periodically.
To schedule reports:

1. Navigate to Analytics > Reports.
2. Click Schedule Reports.
3. Click +.
4. Configure the following in the SCHEDULE INFO section:
   - Name—this is the filename of the report.
   - File Format—a PDF report is sent as an email attachment.
   - Report Frequency—determines how often the report is generated. The options are: Daily, Weekly, and Monthly. If you select Weekly or Monthly, you need to specify the day or date on which the report is delivered.
   - At—the time when the report is sent as an email attachment.
5. In the RECIPENTS section: enter the email address to receive reports to your Email account, and click Add.
6. Choose what sections and details that should be included in the report. At the bottom of the screen, under REPORT CONTENT, the contents of the report are listed. As you change options, the contents list changes:
   - Threats
   - Capture ATP Events
   - Devices
   - Activities
   - Web Protection
   - Applications
   - Tenants
7. Click Save.

You will receive reports through email from the SonicWall team at the scheduled time, periodically, at the frequency you have set.

After you schedule reports, you can deactivate (clear the selection next to the report’s name), delete, or edit as needed. You can also download a sample report to see how a scheduled report looks when it is delivered.
Alerts and Notifications

The Notifications feature allows administrators and users to see the status of any threats, events or alerts and to set the rules for the kinds of notifications associated with these activities. To configure what kind of events or threats needs to be displayed as notifications and to assign a severity level, see Configuring Notifications.

Topics:
- Accessing Notifications
- Viewing Alerts

Accessing Notifications

When you first log into the Capture Client, you can quickly see the number of notifications that are pending some kind of acknowledgment. Click the Notifications icon in the upper-right corner, which opens the Notification Center.

Click See all alerts to view a full list of notifications. This is same as navigating to Overview > Alerts.
Viewing Alerts

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Message</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/31/2020 8:33:32 AM</td>
<td>Threat</td>
<td>Threat event remediated: s1c2.com</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 12:58:54 PM</td>
<td>Threat</td>
<td>Threat event remediated: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:19:59 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:17:20 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:14:08 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:14:08 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:11:29 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:09:20 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:05:40 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
<tr>
<td>1/29/2020 7:05:40 AM</td>
<td>Threat</td>
<td>Suspicious activity detected: GWUnblock.exe</td>
<td>New</td>
</tr>
</tbody>
</table>

The below table shows what level of severity an event is assigned by default; this is based on the category the event belongs to. To assign severity level to events based on the category they belong to, see Configuring Notifications.

<table>
<thead>
<tr>
<th>Type</th>
<th>Category/Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Threat detected</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Threat Killed and Quarantined/Remediated</td>
<td>Major</td>
</tr>
<tr>
<td></td>
<td>Suspicious Activity Detected</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Suspicious Activity K&amp;Q/Remediated</td>
<td>Major</td>
</tr>
<tr>
<td>Operational</td>
<td>Infected Device</td>
<td>Major</td>
</tr>
<tr>
<td></td>
<td>Device is offline for more than 8 days</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Scan Started</td>
<td>Minor</td>
</tr>
<tr>
<td></td>
<td>Scan Completed Successfully</td>
<td>Minor</td>
</tr>
<tr>
<td></td>
<td>Scan Completed with Errors</td>
<td>Major</td>
</tr>
<tr>
<td></td>
<td>Other Device Event</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>License Expiring Soon</td>
<td>Major</td>
</tr>
</tbody>
</table>
To refine your search for particular kinds of issues, click on the Filter icon. It expands and you can select a combination of parameters to filter against.

You can also export the table to a CSV file by clicking the Export as CSV icon on the upper right above the table.
Part 3

SonicWall Support

• SonicWall Support
SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.
About This Document

Legend

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

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

💡 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO**: An information icon indicates supporting information.

Capture Client Operations
Updated - April 2020
Software Version - 3.0
232-005272-00 Rev A

Copyright © 2020 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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

Open Source Code
SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035