# SonicOS 7.1

# Capture ATP

## Administration Guide

SONICWALL®

# Contents


**About SonicOS** ... **3**
Working with SonicOS ... 3
SonicOS Workflow ... 5
How to Use the SonicOS Administration Guides ... 6
Guide Conventions ... 7

**Capture ATP** ... **8**
About Capture ATP ... 8
- Files are Preprocessed ... 9
- Files Blocked Until Completely Analyzed ... 9
- Files are Sent over an Encrypted Connection ... 9
- Capture ATP Friendly Filename Display ... 9
- Activating the Capture ATP License ... 10

Enabling Capture ATP ... 10
About the Capture ATP Page ... 11
- Basic Setup Checklist ... 11
- Bandwidth Management ... 13
- Exclusions ... 13
- Custom Blocking Behavior ... 15

Configuring Capture ATP Settings ... 16
Disabling GAV or Cloud Gateway Anti-Virus ... 17
Capture ATP Location ... 18

**Scanning History** ... **19**
Submit a Sample ... 19
Viewing Analyzed Results ... 20

**SonicWall Support** ... **22**
About This Document ... 23

1

# About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses onhow to use Capture ATP and the process followed to securely inspect, classify, and manage the files.

**Topics:**


- Working with SonicOS
- SonicOS Workflow
- How to Use the SonicOS Administration Guides
- Guide Conventions


## Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

| Firewall Type | Classic Mode | Policy Mode | Comments |
|---|---|---|---|
| TZ Series | yes | no | The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTPPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support. |
| NSa Series | yes | no | NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management. |
| NSsp 10700, NSsp 11700, NSsp 13700 | yes | no | The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need. |
| NSsp 15700 | no | yes | The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability. |
| NSv Series | yes | yes | The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed. |

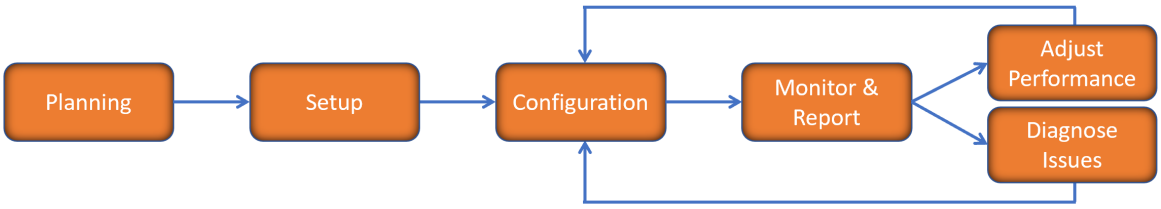
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- SonicOS 7.1 API Reference Guide

- *SonicOS Command Line Interface Reference Guide*

# SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

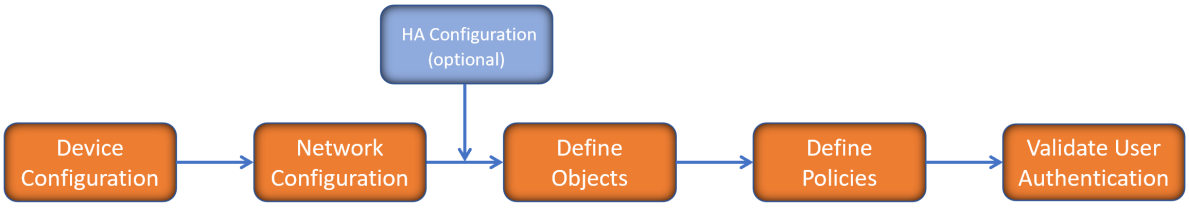



You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used use only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

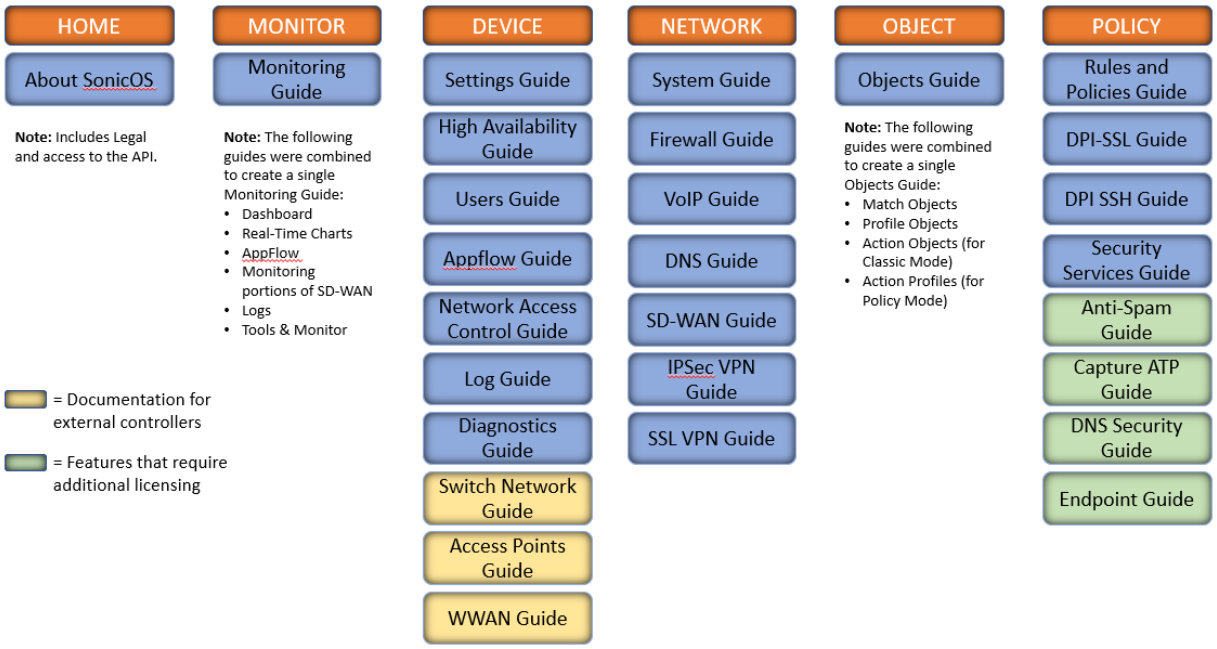


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

# How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 7.1 Monitor Guide and the SonicOS 7.1 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.




The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the https://www.sonicwall.com/support/technical-documentation/.

# Guide Conventions

These text conventions are used in this guide:

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

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

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

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

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

| Convention | Description |
|---|---|
| **Bold text** | Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface. |
| **Function \| Menu group > Menu item** | Indicates a multiple step menu choice on the user interface. For example, **NETWORK \| System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page. |
| `Code` | Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface. |
| ***<Variable>*** | Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=***<your serial number>*, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004. |
| ***Italics*** | Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept. |

2

# Capture ATP

**IMPORTANT:** Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV), that helps a firewall identify whether a file is malicious.
Before you can enable Capture ATP you must first get a license, and you must enable the Gateway Anti-Virus (GAV) and Cloud Gateway Anti-Virus Database services. After Capture ATP is licensed, you can view Capture ATP status in your MySonicWall account as well as configure and receive alerts and notifications.

**Topics:**


- About Capture ATP
- Enabling Capture ATP
- About the Capture ATP Page
- Configuring Capture ATP
- Disabling GAV or Cloud Anti-Virus


## About Capture ATP

Capture Advanced Threat Protection (ATP) helps a firewall identify whether a file is malicious by transmitting the file to the cloud where the SonicWall Capture ATP service analyzes the file to determine if it contains a virus or other malicious elements. Capture ATP then sends the results to the firewall. The analysis and reporting are done in real time while the file is being processed by the firewall.

All files are sent to the Capture ATP cloud over an encrypted connection. Files are analyzed and deleted within minutes of a verdict being determined, unless a file is found to be malicious. Malicious files are submitted via an encrypted HTTPS connection to the SonicWall threat research team for further analysis and to harvest threat information. Files are not transferred to any other location for analysis. Malicious files are deleted after harvesting threat information within 30 days of receipt

Capture ATP provides a file analysis report (threat report) with detailed threat behavior information.

The firewall is located on your premises, while the Capture ATP server and database are located at a SonicWall facility. The firewall creates a secure connection with the Capture ATP cloud service before transmitting data.

Capture ATP works in conjunction with the Gateway Anti-Virus (GAV) and Cloud Gateway Anti-Virus services. Capture ATP also logs/displays email header information (to, cc, bcc) parsed by GAV.

**Topics:**


- Files are Preprocessed
- Files Blocked Until Completely Analyzed
- Files are Sent over an Encrypted Connection
- Capture ATP Friendly Filename Display
- Activating the Capture ATP License


# Files are Preprocessed

All files submitted to Capture ATP for analysis are first preprocessed by the GAV service to determine if a file is malicious or benign. You can also use GAV settings to select or define address objects to exclude from GAV and Capture ATP scanning.

Preprocessed files determined to be malicious or benign are not analyzed by Capture ATP. If a file is not determined to be malicious or benign during preprocessing, the file is submitted to Capture ATP for analysis.

# Files Blocked Until Completely Analyzed

For HTTP/HTTPS downloads, Capture ATP has an option, **Block file download until a verdict is returned**, that ensures no packets get through until the file is completely analyzed and determined to be either malicious or benign. The file is held until the last packet is analyzed. If the file has malware, the last packet is dropped, and the file is blocked. The threat report provides information necessary to respond to a threat or infection.

# Files are Sent over an Encrypted Connection

All files are sent to the Capture ATP cloud over an encrypted connection. SonicWall does not keep the files. All file types, whether they are malicious or benign are removed from the Capture ATP server after a certain time period.

The SonicWall privacy policy can be accessed at https://www.MySonicWall.com/privacypolicy.aspx.

# Capture ATP Friendly Filename Display

SonicWall Capture Advanced Threat Protection logs the friendly filename of scanned files for the following non-HTTP protocols:

| | | |
|---|---|---|
| • SMTP | • POP3 | • FTP |
| • IMAP | • NetBIOS | |

With this feature, you can easily identify the files being scanned by Capture ATP and their status displayed for filenames of these protocol types in the **POLICY > Capture ATP > Scanning History** table and in log messages. Friendly filenames can be up to a maximum of 256 characters.

This feature cannot parse:

- Filename information for TCP protocol streams.
- A filename if it is not part of a single network packet.

No SonicOS configuration is required.

# Activating the Capture ATP License

ⓘ | **IMPORTANT:** Capture ATP requires the Gateway Anti-Virus service, which must also be licensed.

After the Capture ATP service license is activated, **Capture ATP** appears in the SonicOS left navigation (left nav) panel under **Policy** > **Capture ATP**.
**NOTE:** Click **Synchronize** on the **DEVICE | Settings > Licenses** page if Capture ATP does not appear shortly after the Capture ATP service license is activated.

To activate the license, go to the **DEVICE | Settings > Licenses** page where you can view all service licenses and initiate licensing for Capture ATP.

# Enabling Capture ATP

ⓘ | **IMPORTANT:** You must enable Gateway Anti-Virus and Cloud Gateway Anti-Virus before you can enable Capture ATP.

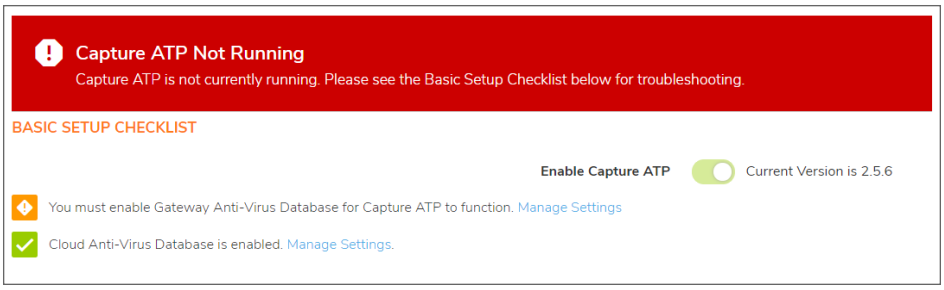
When Capture ATP is licensed but not enabled, the banner displays this message:

```
Capture ATP is not currently running. Please see the Basic Setup Checklist below for
troubleshooting.
```

In disabled mode, the **Basic Setup Checklist** section is visible, but the other sections are dimmed.

***To enable Capture ATP:***

1. Navigate to **POLICY > Capture ATP > Settings**.
2. Enable both Gateway Anti-Virus (GAV) and Cloud Gateway Anti-Virus.
3. Optionally, you can configure GAVand Cloud Gateway Anti-Virus settings, which also apply to Capture ATP.
4. Navigate to **POLICY > Capture ATP > Settings**. If Capture ATP is not enabled, a warning message displays:



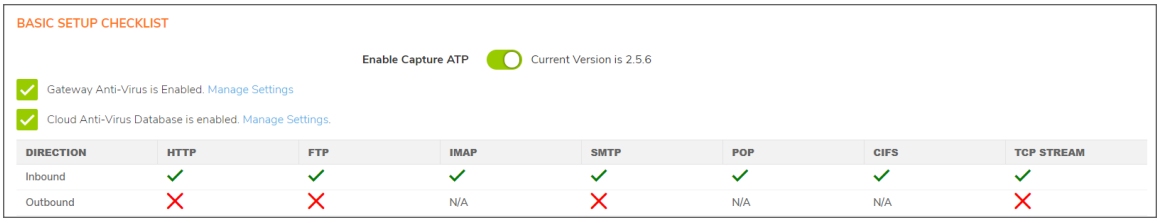

5. In the Basic Setup Checklist section, toggle **Enable Capture ATP** to enable Capture ATP.

# About the Capture ATP Page

**Topics:**

- Basic Setup Checklist
- Bandwidth Management
- Exclusions
- Custom Blocking Behavior

# Basic Setup Checklist




The **Basic Setup Checklist**:

- Displays the status of Capture ATP and its components, Gateway Anti-Virus and Cloud Gateway Anti-Virus.
- Displays any error states that might be present.
- Allows enabling or disabling of the Capture ATP service.
- Provides links to the **POLICY > Security Services > Gateway Anti-Virus** page for the GAV, Cloud Gateway Anti-Virus, and protocol inspection settings.
- Displays a matrix of the protocol inspection settings and whether the inbound and outbound directions have been enabled.
- For messages that display in this section, see the Capture ATP Status through Protocols Inspection Settings tables. **Enabled** corresponds to a green checkmark, and **Disabled** corresponds to a red X.

### CAPTURE ATP STATUS

| Icon | Message | Link | Action |
|---|---|---|---|
| **Enabled** | Capture ATP service is enabled until `renewal_date`. | `disable it` | Click the link to turn off Capture ATP and put the service in disabled mode. You do not need to click **Accept** to apply this change. |
| **Disabled** | Capture ATP subscription is valid until `renewal_date` but the service is not currently enabled. | `enable it` | Click the link to turn on Capture ATP and put the service in enabled mode. You do not need to click **Accept** to apply this change. |
| **Disabled** | Capture ATP subscription expired on `renewal_date`. | `renew it` | Click the link to go to MySonicWall to renew the service. |

### GATEWAY ANTI-VIRUS STATUS

| Icon | Message | Link | Action |
|---|---|---|---|
| **Enabled** | Gateway Anti-Virus is Enabled. | `manage settings` | Click the link to display the **POLICY \| Security Services > Gateway Anti-Virus** page. |
| **Disabled** | You must enable Gateway Anti-Virus for Capture ATP to function. | `manage settings` | Click the link to display the **POLICY \| Security Services > Gateway Anti-Virus** page. |

### CLOUD GATEWAY ANTI-VIRUS DATABASE STATUS

| Icon | Message | Link | Action |
|---|---|---|---|
| **Enabled** | Cloud Gateway Anti-Virus Database is enabled. | `manage settings` | Click the link to display the **POLICY \| Security Services > Gateway Anti-Virus** page. |
| **Disabled** | You must enable the Cloud Gateway Anti-Virus Database for Capture ATP to function. | `manage settings` | Click the link to display the **POLICY \| Security Services > Gateway Anti-Virus** page. |

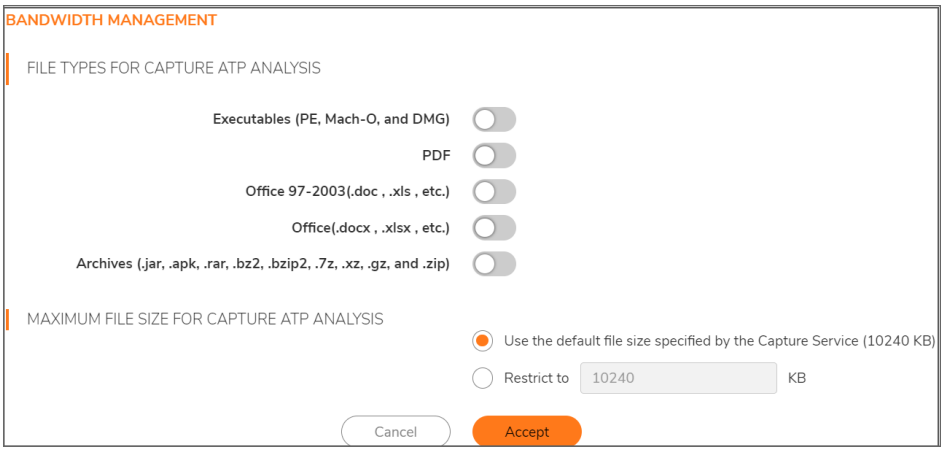
The **Inspected Protocols** table also provides a `manage settings` link that takes you to the **POLICY | Security Services > Gateway Anti-Virus** page. There, you can enable or disable inspection of specific network traffic protocols, including HTTP, FTP, IMAP, SMTP, POP, CIFS, and TCP Stream. Each protocol can be managed separately for inbound and outbound traffic.

The table that follows **Inspected Protocols** displays the current inspection settings for each protocol, in each direction; see Protocols Inspection Settings.

**PROTOCOLS INSPECTION SETTINGS**

| Icon | Message |
|---|---|
| **Enabled** | Protocol is inspected. |
| **Disabled** | Protocol is not inspected. |
| n/a | Inspection is not applicable to this protocol in this direction. |

# Bandwidth Management




The **Bandwidth Management** section enables you to select the types of files to be submitted to Capture ATP and to specify the maximum size of submitted files. You can also specify an address object to be excluded from inspection.

The default option for the maximum file size is **Use the default file size specified by the Capture Service (10240 KB)**. This specifies a file size limit of 10 megabytes (10 MB).

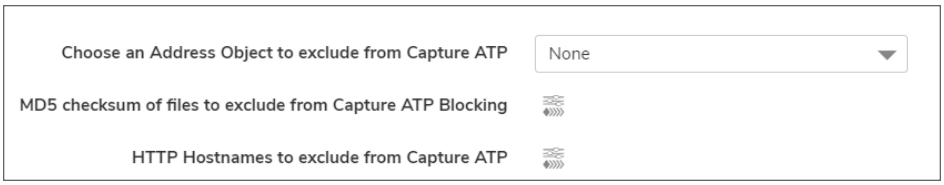
If you select **Restrict to KB**, you can enter your own custom value. This value must be a non-zero value and must not be greater than the default limit.

# Exclusions

The **Exclusions** section allows you to exclude an Address Object or MD5 hash function from Capture ATP.

***To exclude an Address Object:***

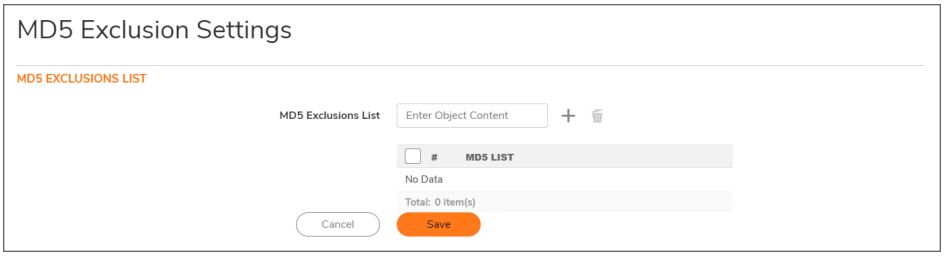
1. Go to **Policy > Capture ATP > Settings > Advanced> Exclusions**.
2. For **Choose an Address Object to exclude from Capture ATP**, optionally select an address object from the drop-down menu, or select the option to create a new address object. Members of the selected address object are excluded from inspection by the Capture ATP service.




3. Select the Address Object from the drop-down menu or create a new one.
4. Click **Accept**.

***To exclude an MD5 file:***

1. Click **MD5 Exclusion List Settings**. The **MD5 Exclusion Settings** dialog displays.



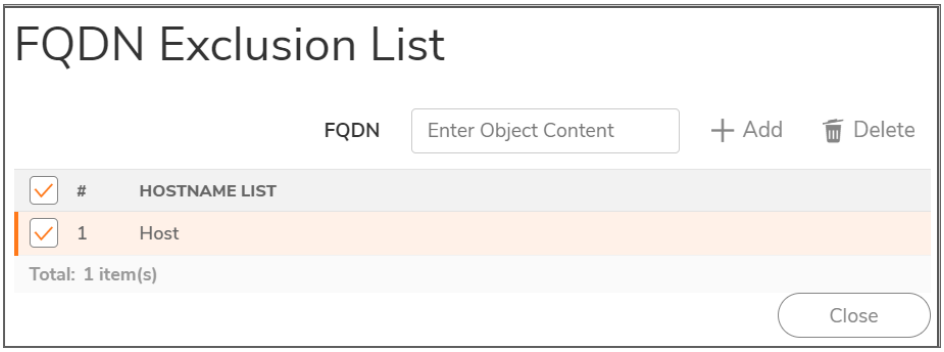

2. Add the 32-hexadecimal-digit hash function to be excluded.
3. Click **Save**.

***To add more than one file:***

1. Repeat Step 2 and Step 3 for each hash function
2. Click **Save**.
3. Click **Accept**.

***To exclude HTTP Hostname:***

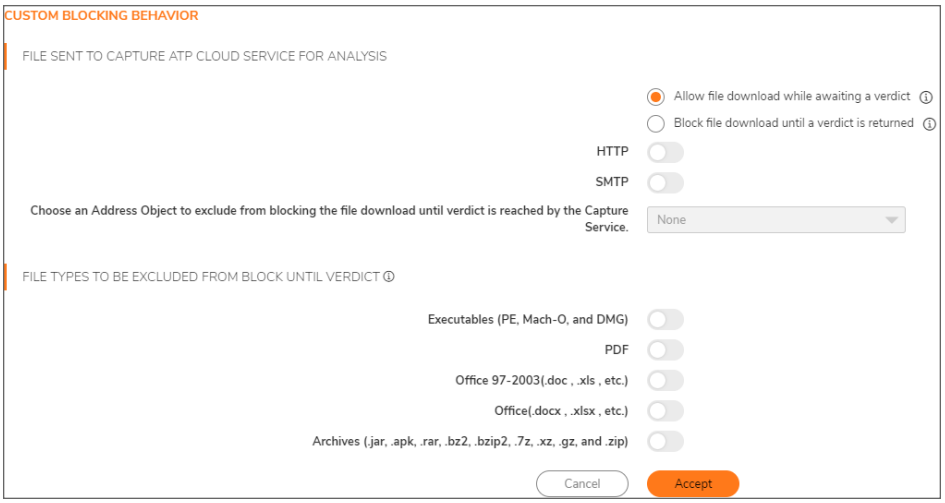
1. Click **HTTP Hostname Settings**. The **FQDN Exclusion List** dialog displays.
2. Enter the hostname in the text box and click **Add**.




3. You can also edit the name by clicking the **Edit** icon. To delete, check the box and click **Delete** icon.

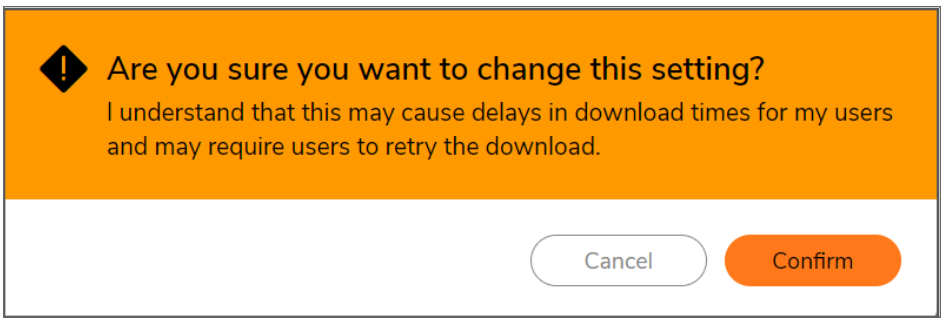
# Custom Blocking Behavior

The **Custom Blocking Behavior** section allows you to select the **Block file download until a verdict is returned** feature.




The default option is **Allow file download while awaiting a verdict**. This setting allows a file to be downloaded without delay while the Capture service analyzes the file for malicious elements. You can set email alerts or check the firewall logs to find out if the Capture service analysis determines that the file is malicious.

The **Block file download until a verdict is returned** feature should only be enabled if the strictest controls are desired. If you select this feature, a warning dialog appears.




When the **Block file download until a verdict is returned** feature is enabled, the other options become available. You can:

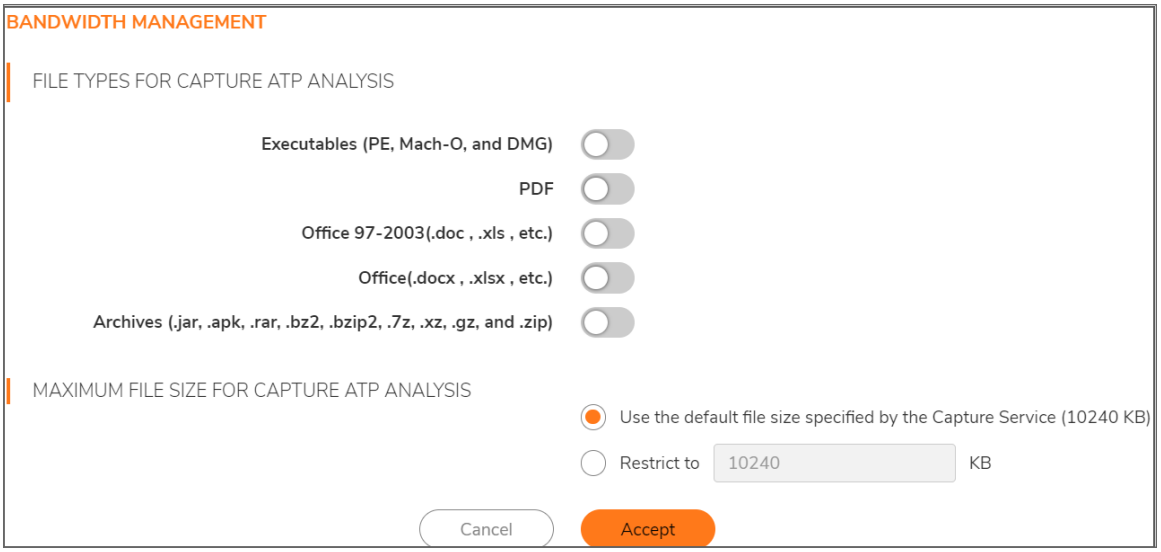
- Select **HTTP** and **SMTP** files sent to Capture ATP cloud service for analysis.
- Select an address object from **Choose an Address Object to exclude from blocking the file download until verdict is reached by the Capture Service**. The default is **None**.
- Select one or more file types to block from **Specify the file types to exclude from blocking the file download until verdict is reached by the Capture Service**:

- **Executables (PE, Mach-O, and DMG)**
- **PDF**
- **Office 97-2003(.doc , .xls ,...)**
- **Office(.docx , .xlsx ,...)**
- **Archives (.jar, .apk, .rar, .bz2, .bzip2, .7z, .xz, .gz, and .zip)**

# Configuring Capture ATP Settings

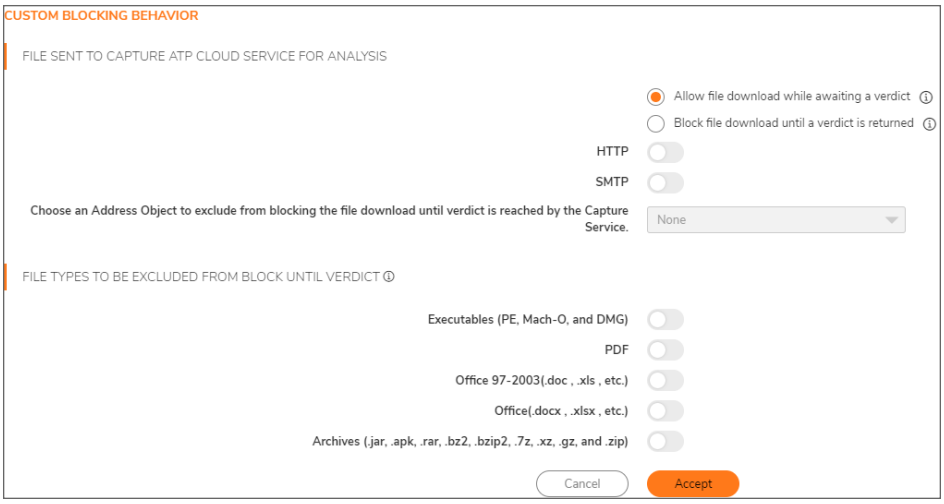
***To configure Capture ATP:***

1. Navigate to **POLICY | Capture ATP > Settings**.
2. Ensure Capture ATP, GAV, Cloud Gateway Anti-Virus database, and relevant protocols are enabled.
3. In the **Bandwidth Management** section, select the file types to be analyzed by Capture ATP.




4. By default **Use the default file size specified by the Capture Service (10240 KB)** is selected. To specify a custom size, enter a value between 1 and 10240 in the **Restrict to KB** field.
5. Optionally, to exclude an Address Object from Capture ATP, select an Address Object from the **Choose an Address Object to Exclude fromCapture ATP** drop-down menu.
6. Optionally, to exclude a file based on its MD5 checksum, click **MD5 Exclusion List Settings** to display the **MD5 Exclusion Settings** dialog.
    a. Add the 32-digit hexadecimal hash to the **MD5 Exclusions List** field.
    b. Click **Save**
    c. Repeat Step a and Step b for each file to exclude.
    d. Click **Save**.

7. If you are analyzing HTTP/HTTPS files, in the **Custom Blocking Behavior** section, you can specify whether all files are to be blocked until analysis is completed.




By default **Allow file download while awaiting a verdict** is selected.

ⓘ **IMPORTANT:** The **Block file download until a verdict is returned** feature should only be enabled if the strictest controls are desired.

If you select this feature, a warning dialog appears.

Clicking the:

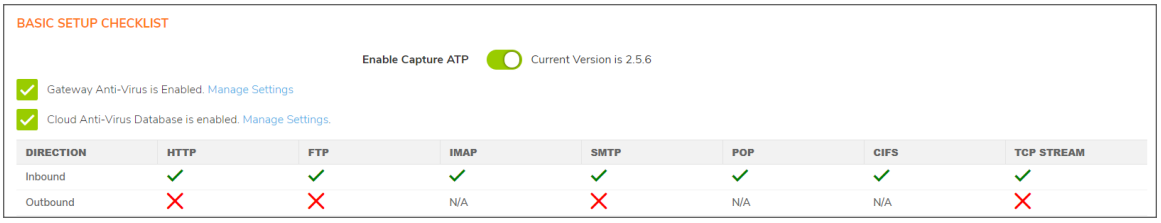
- **I agree, apply the setting** button selects the **Block file download until a verdict is returned** option. You also must click **Accept** for the change to take effect.
- **Never mind, do not apply** link closes the dialog and leaves **Allow file download while awaiting a verdict** selected.

8. Click **Accept**.

# Disabling GAV or Cloud Gateway Anti-Virus

You can disable the Gateway Anti-Virus or Cloud Gateway Anti-Virus services by clearing the checkboxes for them on the **POLICY | Security Services > Gateway Anti-Virus** page. If you disable either service while Capture ATP is enabled, a pop-up message is displayed warning you that Capture ATP is also disabled.

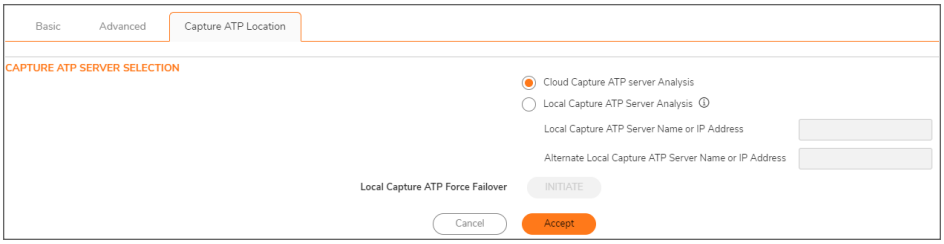
Capture ATP stops working when either Gateway Anti-Virus or Cloud Gateway Anti-Virus is disabled. For example, if Gateway Anti-Virus is not enabled, the **POLICY | Capture ATP > Settings** page shows **You must enable Gateway Anti-Virus for Capture ATP** to function, along with a manage settings link that takes you to the **POLICY | Security Services > Gateway Anti-Virus** page where you can enable it.




# Capture ATP Location

The Capture ATP Server Selection section enables you to select the types of server analysis.

- **Cloud Capture ATP server Analysis**
- **Local Capture ATP Server Analysis**



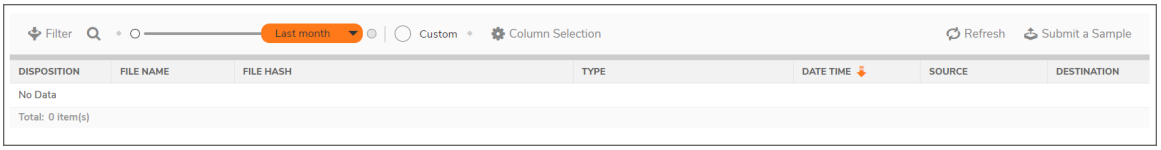

***To view the local server analysis report, use appliance GUI to view the report. :***

1. Select **Local Capture ATP Server Analysis**.
2. Enter the **Local Capture ATP Server Name or IP Address** and **Alternate Local Capture ATP Server Name or IP Address**.
3. Click **Initiate** in **Local Capture ATP Force Failover** to use the server name or ip address, to view the local server analysis reports.
4. Under **Diagnostics** section provide **MD5 Hash for Look up on Capture ATP server** and click **Test Connectivity** to test connectivity to Capture ATP server.

3

# Scanning History

The Capture ATP **Scanning History** page located at **POLICY | Capture ATP > Scanning History** displays a list of all the files that have been scanned and analyzed. You can filter results, search, narrow results to show scans from the last month, last week, last 24 hours, and in the last hour. You can also search for specific strings, so this page lists only items that contain those search strings. Use custom date periods to view windows of scan instances, and customize your view of the **Column Selection**.



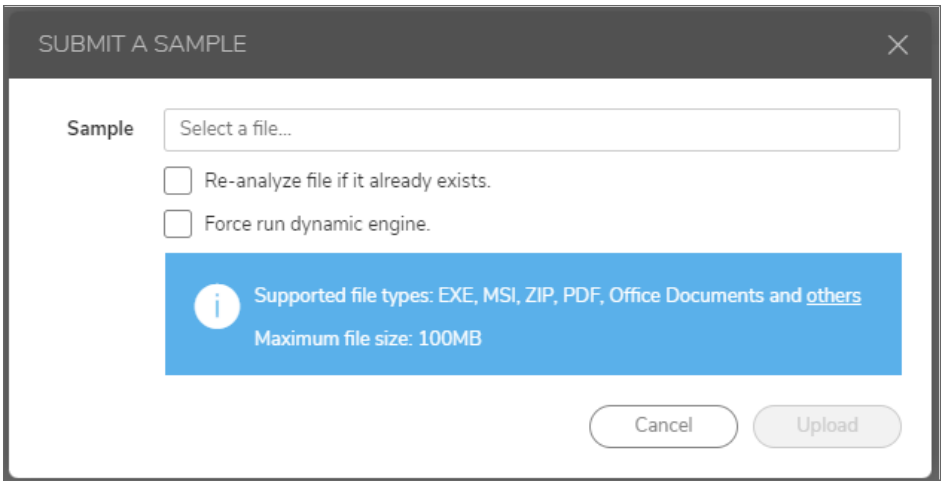

# Submit a Sample

The **Submit a Sample** option allows you to browse for supported files, submit, and scan them for analysis. Supported files include .PE files, match object (Mach-O), Apple Disk Image (DMG), pdf, office documents (.doc , .xls, .docx , .xlsx) and others (jar, apk, rar, bz2, bzip2, 7z, xz, gz, zip) with a maximum file size of 10240 KB.

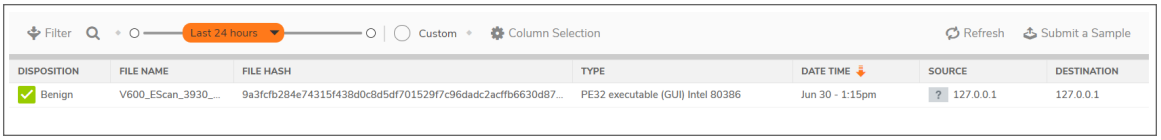
You can restrict the maximum file size that can be submitted on the **POLICY | Capture ATP > Settings** page, under **Bandwidth Management**. You can enter any number between 0 and the maximum size that is set by the License Manager (10240 KB). Entering a zero (0) indicates that the file size is unlimited, but that is not recommended.

***To submit a file to Capture ATP for analysis:***

1. Navigate to the **POLICY | Capture ATP > Scanning History**.
2. Click the **Submit a Sample** icon.
   The **Submit a Sample** dialog appears.




3. Click in the **Select a file...** field and browse to the file you want to submit.
4. Click the **Re-analyze file if it already exists** option if you would like to resubmit a previously scanned file.
5. Click the **Force run dynamic engine** option if you want to scan the static analysis cannot determine the verdict of the file, and run dynamic analysis. It is much slower but can detect unseen malicious files which generates file reports with behaviors. **Force run dynamic engine** skips the static part and always run the dynamic engine.
6. Click **Upload**.
7. After a few moments, click **Refresh**. Verify that the file appears on the **Scanning History** page.




# Viewing Analyzed Results

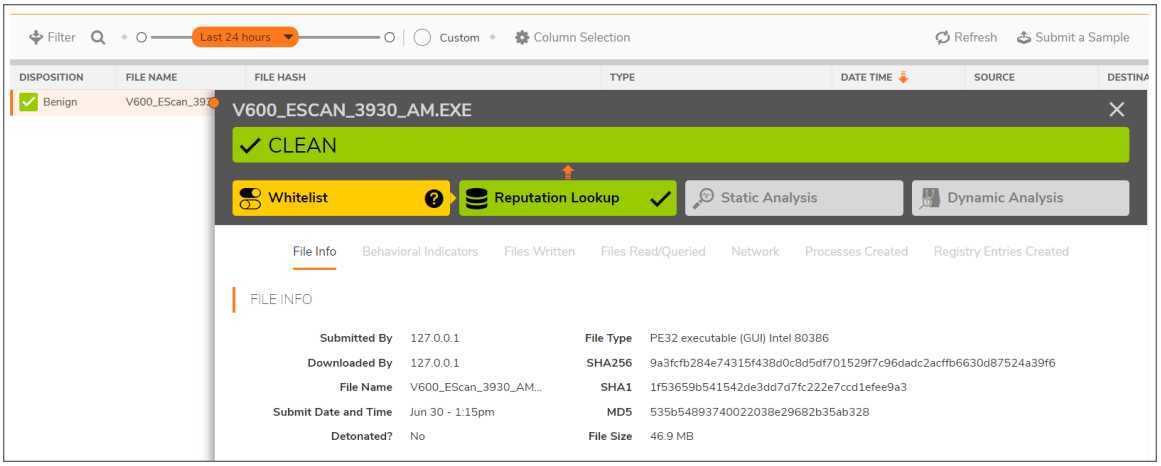
***To view the detailed results of a scanned file:***

1. Navigate to the **POLICY | Capture ATP > Scanning History**.
2. The columns for the **Scanning History** page are as follows:
   - **Disposition**: The results of the analysis for this file, **Benign** or **Malicious**.
   - **File Name**: Lists the file name of the scanned file.
   - **URL**: Lists the original URL of the downloaded file.
   - **Type**: The type of file that was analyzed, such as an executable file or a zip file.
   - **Date Time**: The time that the file was submitted for analysis.
   - **User Name**:Lists the user name of who uploaded or downloaded file.

- **Source**: The IP address from which the file was sent.
- **Destination**: The IP address to which the file was sent.

From the detailed results view, you can click a scanning report to launch the scanning report for that file.

3. Click the **Disposition** check mark for that file. The details of the analysis results for that file display.




4. Click the **Disposition** check mark again to close the results.

4

# SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. 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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- 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

SonicOS Capture ATP Administration Guide
Updated - December 2023
Software Version - 7.1
232-005883-00 Rev A



## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035