

# SonicOS and SonicOSX 7 Capture ATP

Administration Guide

SONICWALL®

# Contents

<b>Capture ATP</b> .....	<b>3</b>
About Capture ATP .....	3
Files are Preprocessed .....	4
Files Blocked Until Completely Analyzed .....	4
Files are Sent over an Encrypted Connection .....	4
Capture ATP Friendly Filename Display .....	4
Activating the Capture ATP License .....	5
Enabling Capture ATP .....	5
About the Capture ATP Page .....	6
Basic Setup Checklist .....	6
Bandwidth Management .....	8
Exclusions .....	8
Custom Blocking Behavior .....	9
Configuring Capture ATP Settings .....	10
Disabling GAV or Cloud Gateway Anti-Virus .....	12
<b>Scanning History</b> .....	<b>13</b>
Submit a Sample .....	13
Viewing Analyzed Results .....	14
<b>SonicWall Support</b> .....	<b>16</b>
About This Document .....	17

# Capture ATP

- ① **NOTE:** References to SonicOS/X indicate that the functionality is available in both SonicOS and SonicOSX.
- ① **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/X configuration is required.

## Activating the Capture ATP License

① | **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/X left navigation (left nav) panel below **Client Enforcement**.

**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

① | **IMPORTANT:** You must enable Gateway Anti-Virus and Cloud Gateway Anti-Virus before you can enable Capture ATP.

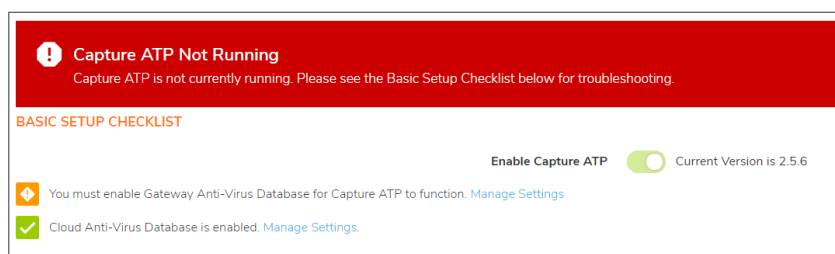
When Capture ATP is licensed but not enabled, the banner displays this message:

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 GAV and 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, click (enable it) in Capture ATP subscription is valid until date

but the service is not currently enabled, (enable it). The warning message disappears, and the status indicator becomes a green checkmark.

# About the Capture ATP Page

## Topics:

- [Basic Setup Checklist](#)
- [Bandwidth Management](#)
- [Exclusions](#)
- [Custom Blocking Behavior](#)

## Basic Setup Checklist

**BASIC SETUP CHECKLIST**

Enable Capture ATP  Current Version is 2.5.6

Gateway Anti-Virus is Enabled. [Manage Settings](#)

Cloud Anti-Virus Database is enabled. [Manage Settings](#)

DIRECTION	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP STREAM
Inbound	✓	✓	✓	✓	✓	✓	✓
Outbound	✗	✗	N/A	✗	N/A	N/A	✗

### 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.

① **NOTE:** 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
<b>Enabled</b>	Capture ATP service is enabled until <code>renewal_date</code> .	<code>disable it</code>	Click the link to turn off Capture ATP and put the service in disabled mode. You do not need to click <b>Accept</b> to apply this change.
<b>Disabled</b>	Capture ATP subscription is valid until <code>renewal_date</code>	<code>enable it</code>	Click the link to turn on Capture ATP and put the service in enabled mode.

Icon	Message	Link	Action
	but the service is not currently enabled.		You do not need to click <b>Accept</b> to apply this change.
<b>Disabled</b>	Capture ATP subscription expired on <code>renewal_date</code> .	<code>renew it</code>	Click the link to go to MySonicWall to renew the service.

### GATEWAY ANTI-VIRUS STATUS

Icon	Message	Link	Action
<b>Enabled</b>	Gateway Anti-Virus is Enabled.	<code>manage settings</code>	Click the link to display the <b>POLICY   Security Services &gt; Gateway Anti-Virus</b> page.
<b>Disabled</b>	You must enable Gateway Anti-Virus for Capture ATP to function.	<code>manage settings</code>	Click the link to display the <b>POLICY   Security Services &gt; Gateway Anti-Virus</b> page.

### CLOUD GATEWAY ANTI-VIRUS DATABASE STATUS

Icon	Message	Link	Action
<b>Enabled</b>	Cloud Gateway Anti-Virus Database is enabled.	<code>manage settings</code>	Click the link to display the <b>POLICY   Security Services &gt; Gateway Anti-Virus</b> page.
<b>Disabled</b>	You must enable the Cloud Gateway Anti-Virus Database for Capture ATP to function.	<code>manage settings</code>	Click the link to display the <b>POLICY   Security Services &gt; Gateway Anti-Virus</b> 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
<b>Enabled</b>	Protocol is inspected.
<b>Disabled</b>	Protocol is not inspected.
n/a	Inspection is not applicable to this protocol in this direction.

# Bandwidth Management

**BANDWIDTH MANAGEMENT**

Specify the file types that may be transferred to Capture ATP for analysis.

Executables (PE, Mach-O, and DMG)

PDF

Office 97-2003(.doc, .xls, ...)

Office(.docx, .xlsx, ...)

Archives (.jar, .apk, .rar, .bz2, .bzp2, .7z, .xz, .gz, and .zip)

Specify the maximum file size that may be transferred to Capture ATP for analysis.

Use the default file size specified by the Capture Service (10240 KB)

Restrict to  KB

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.

By default, only the **Executables (PE, Mach-O, and DMG)** file type is enabled.

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.

**EXCLUSIONS**

Choose an Address Object to exclude from Capture ATP

MD5 checksum of files to exclude from Capture ATP

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.

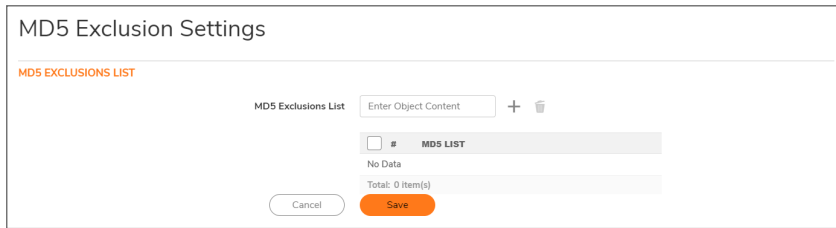
### **To exclude an Address Object:**

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



### To exclude an MD5 file:

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



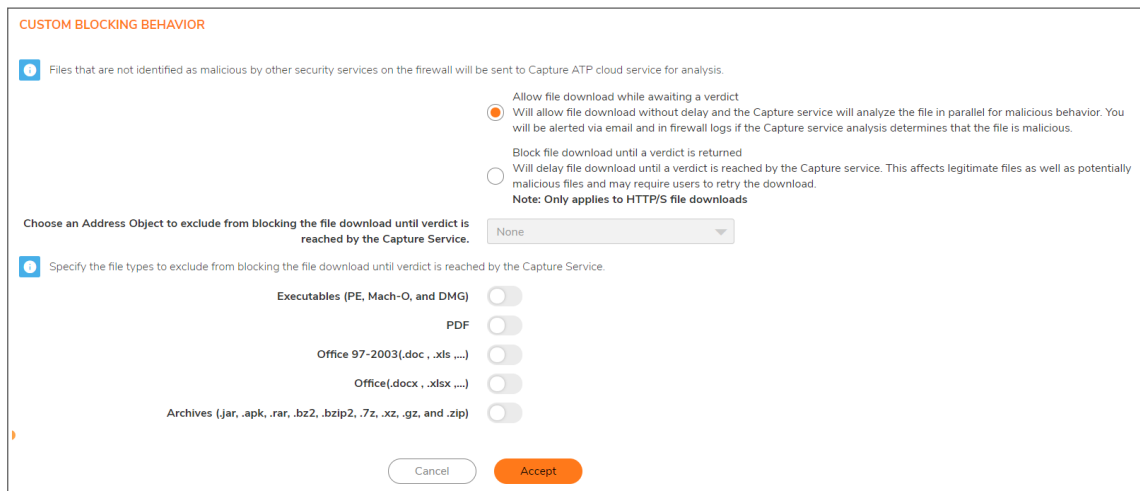
2. Add the 32-hexadecimal-digit hash function to be excluded.
3. Click **Save**.

### To add more than one file:

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


## 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.

 **Are you sure you want to change this setting?**  
 I understand that this may cause delays in download times for my users and may require users to retry the download.

Cancel
Confirm

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

- 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, .gz, and .zip)

## Configuring Capture ATP Settings

*To configure Capture ATP:*

1. Navigate to **POLICY | Capture ATP > Settings**.

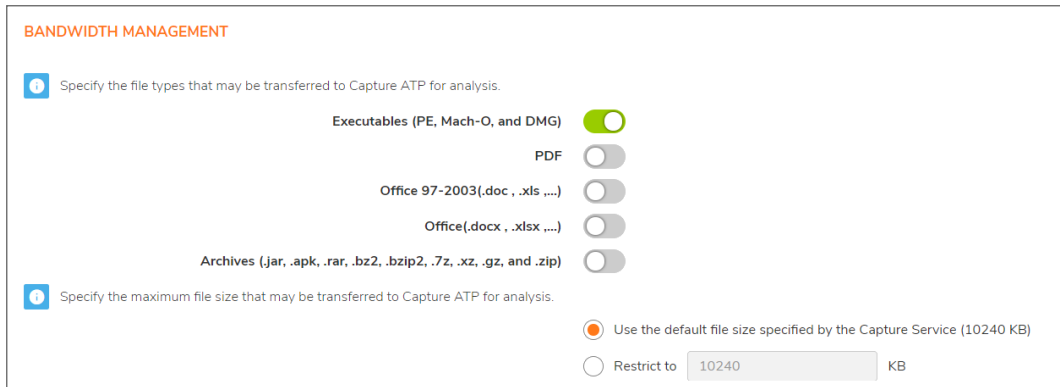
**BASIC SETUP CHECKLIST**

Enable Capture ATP  Current Version is 2.5.6

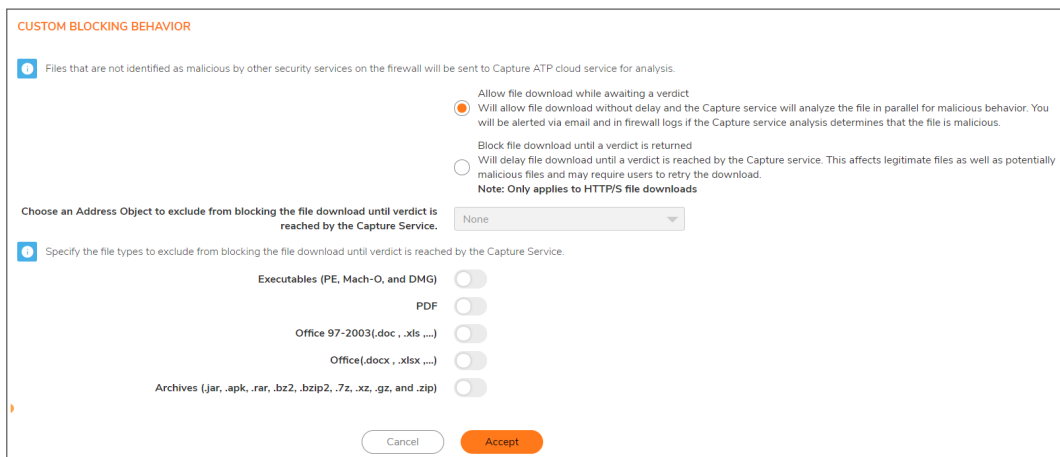
- Gateway Anti-Virus is Enabled. [Manage Settings](#)
- Cloud Anti-Virus Database is enabled. [Manage Settings](#)

DIRECTION	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP STREAM
Inbound	✓	✓	✓	✓	✓	✓	✓
Outbound	✗	✗	N/A	✗	N/A	N/A	✗

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. By default, only **Executables (PE, Mach-O, and DMG)** is selected.



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 from Capture 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.

**BASIC SETUP CHECKLIST**

Enable Capture ATP  Current Version is 2.5.6

- Gateway Anti-Virus is Enabled. [Manage Settings](#)
- Cloud Anti-Virus Database is enabled. [Manage Settings](#)

DIRECTION	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP STREAM
Inbound	✓	✓	✓	✓	✓	✓	✓
Outbound	✗	✗	N/A	✗	N/A	N/A	✗

## 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**.

DISPOSITION	FILE NAME	FILE HASH	TYPE	DATE TIME	SOURCE	DESTINATION
No Data						
Total: 0 Item(s)						

## Submit a Sample

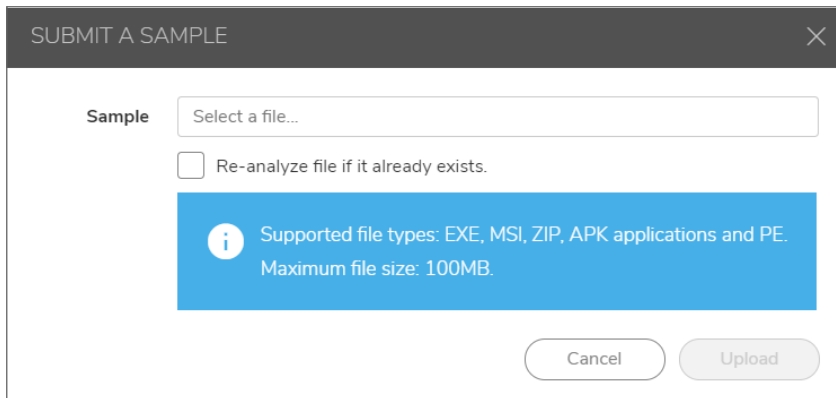
The **Submit a Sample** option allows you to browse for supported files, submit, and scan them for analysis. Supported files include .EXE, .MSI, .ZIP, .APK, and .PE files with a maximum file size of 10240 KB.

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 **Upload**.
6. After a few moments, click **Refresh**. Verify that the file appears on the **Scanning History** page.

DISPOSITION	FILE NAME	FILE HASH	TYPE	DATE TIME	SOURCE	DESTINATION
Benign	V600_EScan_3930_...	9a3fcb284e74315f438d0c8d5df701529f7c96dad2acffb6630d87...	PE32 executable (GUI) Intel 80386	Jun 30 - 1:15pm	127.0.0.1	127.0.0.1

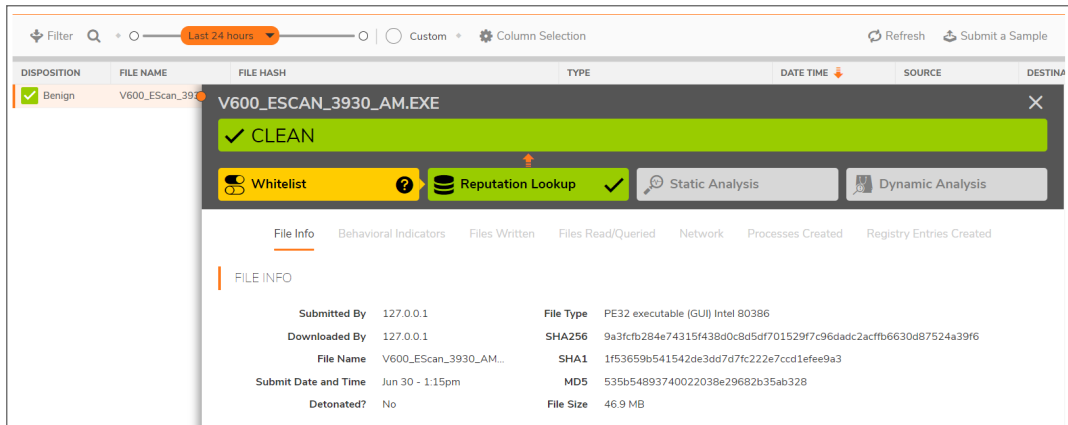
## Viewing Analyzed Results

### 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.
  - **File Hash:** A fixed-length value computed by a number of input bytes processed through a one-way digest function.
  - **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.
  - **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.

# 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

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

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

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

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

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

SonicOS and SonicOSX Capture ATP Administration Guide

Updated - August 2020

Software Version - 7

232-005328-00 Rev B

Copyright © 2020 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-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