



# SonicOS 6.2.6 Capture Advanced Threat Protection Beta Feature Guide

July 2016

This feature guide describes how to license, configure, and use SonicOS 6.2.6 Capture Advanced Threat Protection (ATP). Capture ATP is an add-on security service to the firewall, similar to Gateway Anti-Virus.

Topics:

- [Supported platforms](#)
- [Overview](#)
- [File upload maximums](#)
- [Licensing Capture ATP](#)
- [Configuring Capture ATP settings](#)
- [Viewing Capture ATP status](#)
- [Uploading a file for analysis](#)
- [Viewing threat reports](#)
- [About Dell](#)

## Supported platforms

Dell SonicWALL Capture ATP is supported on the following Dell SonicWALL network security appliances running SonicOS 6.2.6 and higher:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 / TZ500W
- TZ400 / TZ400W
- TZ300 / TZ300W
- SOHO W

# Overview

Capture Advanced Threat Protection (ATP) is sold as an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV).

Capture ATP helps a firewall identify whether a file is malicious or not by transmitting the file to the cloud where the Dell 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. This is done in real time while the file is being processed by the firewall.

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

Before you can enable Capture ATP you must first get a license, and you must enable the Gateway Anti-Virus (GAV) and Cloud Anti-Virus Database services. You can choose the settings for GAV, such as protocols to scan for files, or IPs to exclude from scanning, and they will also apply to the Capture ATP service.

All files that are submitted to Capture ATP for analysis are first subjected to preprocessing. Files can be rejected or passed based on preprocessing. If preprocessing determines a file to be malicious or benign, the file will not be analyzed by Capture ATP.

If a file is not determined to be malicious or benign by the GAV service during the Capture preprocessing process, the file is submitted to Capture ATP for analysis.

If the file does not appear in the **Capture ATP > Status** page, that means that the file was not analyzed by Capture ATP, but was passed or rejected based on the Capture preprocessing process. Only files that have been analyzed by Capture ATP are listed in the log table on the **Status** page.

The **Block all files until a verdict is returned** option ensures that no packets get through until the file is completely analyzed and it is determined to be either malicious or benign. This option only applies to HTTP/HTTPS downloads. 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 permanently. Once a file is blocked permanently, there is no way to recover it or analyze it again.

Capture ATP provides a file analysis report (threat report) with detailed threat behavior information. If the **Block all files until a verdict is returned** option is not enabled, the threat report provides information necessary to respond to a threat or infection.

When a file is determined to be malicious, threat intelligence is incorporated into the other Dell security services, such as GAV and Cloud Anti-Virus, so that other firewalls will benefit within 48 hours.

All files are sent to the Capture ATP cloud over an encrypted connection. Dell SonicWALL does not keep the files. All file types, whether they are malicious or benign are removed from the Capture ATP server after they are analyzed, except for executable files that contain malware. Executable files that are determined to be malicious are sent to the Dell SonicWALL threat research facility for further analysis, but they are also removed after a certain time period.

The Dell SonicWALL privacy policy can be accessed at:

<https://www.mysonicwall.com/privacypolicy.aspx>

## File upload maximums

The file upload maximums differ depending on the Dell SonicWALL appliance platform. Maximums exist for:

- The number of files per hour that can be uploaded to the Capture ATP service for analysis
- The number of files that can be analyzed at the same time

### Per hour and concurrent file upload maximums

Appliance platform	Max files per hour	Max concurrent files
SuperMassive 9600	9000	50

Appliance platform	Max files per hour	Max concurrent files
SuperMassive 9400	4500	50
SuperMassive 9200	3000	50
NSA 6600/5600	1500	25
NSA 4600/3600/2600	900	15
TZ 600/500 series	300	5
TZ 400/300 series	50	3
SOHO Wireless		

## Licensing Capture ATP

This section describes how to license and activate the Capture ATP feature on your Dell SonicWALL appliance.

The Capture ATP license requires that the Gateway Anti-Virus service is also licensed. You must enable Gateway Anti-Virus and Cloud Anti-Virus before you can enable Capture ATP.

Currently, only Beta licenses are available for Capture ATP.

Topics:

- [Activating a Beta Capture ATP license](#)
- [Enabling SonicOS services](#)
- [Disabling Gateway Anti-Virus or Cloud Anti-Virus](#)

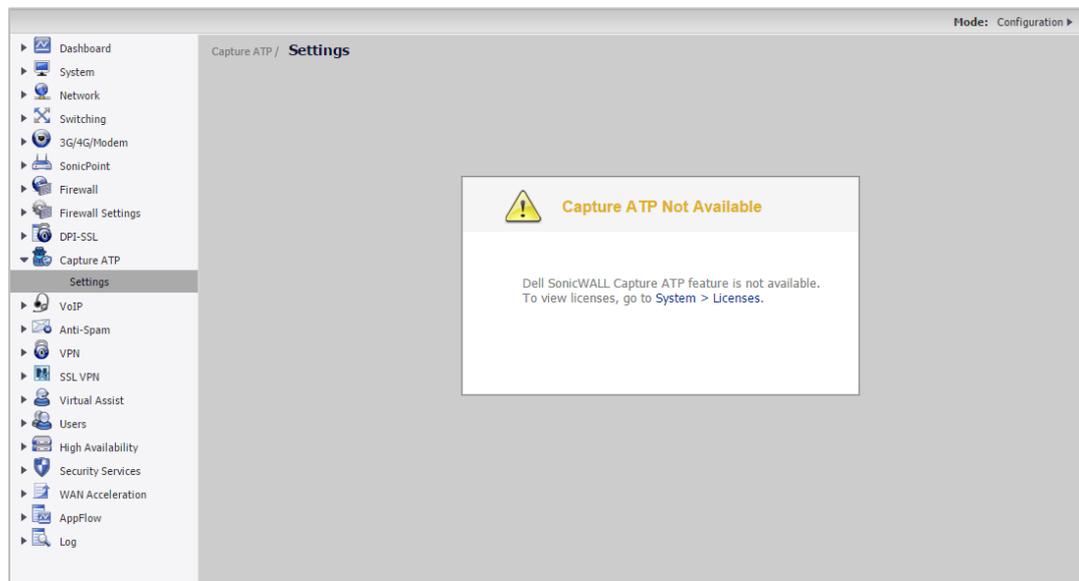
# Activating a Beta Capture ATP License

This procedure describes how to activate a Beta Capture ATP license.

## To activate a Beta Capture ATP license on your firewall:

- 1 Submit the serial number of the appliances you would like to activate by completing the survey at <https://www.surveymonkey.com/r/Sonicwall-Beta-SonicOS626>.
- 2 After you complete the survey, you will be notified by Email when the Capture ATP license has been activated for your appliance.

When Capture ATP is not licensed, the left-hand navigation panel only shows the **Settings** page, which directs you to go to the **System > Licenses** page where you can view system licenses and initiate licensing for Capture ATP.

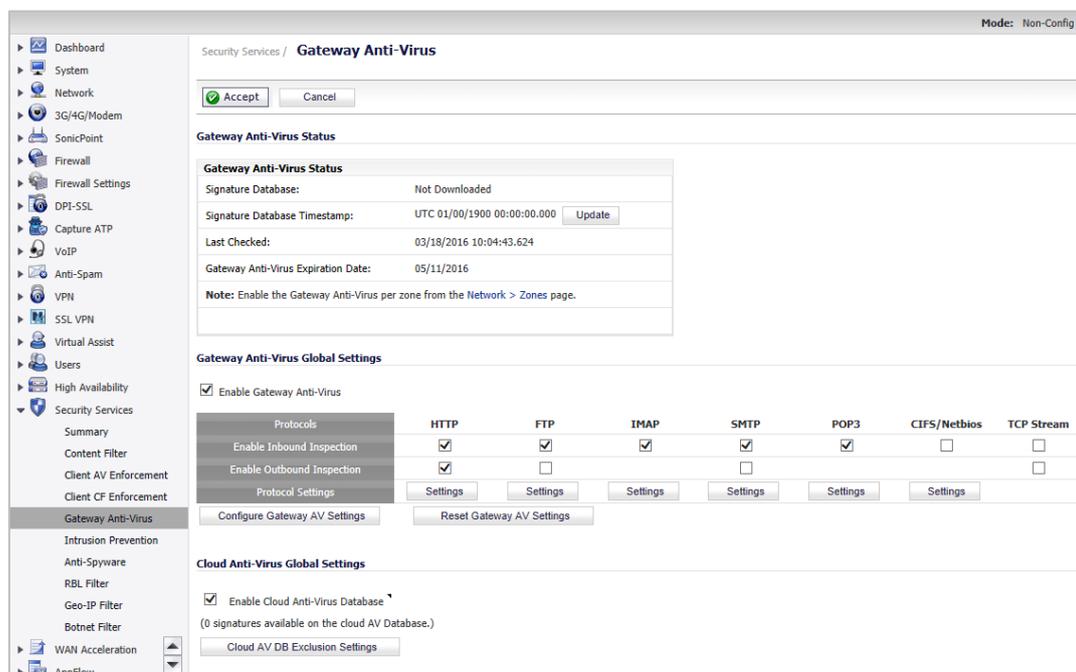


# Enabling SonicOS services

Before you can enable Capture ATP, the Gateway Anti-Virus and Cloud Anti-Virus Database services must be enabled in SonicOS.

*To enable the Gateway Anti-Virus and Cloud Anti-Virus Database services:*

- 1 On the firewall, go to the Security Services > Gateway Anti-Virus page.



- 2 Ensure that the checkboxes for **Enable Gateway Anti-Virus** and **Enable Cloud Anti-Virus Database** are checked.

You can also choose the protocols that are used to scan for malicious files. The GAV protocol settings will apply to both GAV and Capture ATP services. You can also use GAV settings to select or define address objects to exclude from GAV and Capture ATP scanning.

If a file is determined not to be malicious or benign by GAV during preprocessing, the file is submitted to Capture ATP for analysis, and if Capture ATP determines that the file is malicious, it creates a detailed threat analysis report that can be accessed from the **Capture ATP > Status** page.

- (Optional) To configure the GAV protocol settings, click **Configure Gateway AV Settings** and select the settings you want in the **Gateway AV Settings** dialog.

**Gateway AV Settings**

- Disable SMTP Responses
- Disable detection of EICAR test virus
- Enable HTTP Byte-Range requests with Gateway AV
- Enable FTP 'REST' requests with Gateway AV
- Do not scan parts of files with high compression ratios
- Block files with multiple levels of zip/gzip compression
- Enable detection-only mode

**HTTP Clientless Notification**

- Enable HTTP Clientless Notification Alerts

**Message to Display when Blocking**

This request is blocked by the Firewall Gateway Anti-Virus Service

**Gateway AV Exclusion List**

- Enable Gateway AV Exclusion List
- Use Address Object  
--Select an address object--
- Use Address Range

From Address	To Address	Configure
No Entries		

Add... Delete All

- (Optional) If you want to use an exclusion list to prevent certain items from being scanned, select the checkbox for **Enable Gateway AV Exclusion List**.
- To exclude certain address objects from scanning, select the **Use Address Object** radio button and click on the drop-down menu to select the address objects you want to add to the **Gateway AV Exclusion List**.
- (Optional) To exclude any items from Cloud Anti-Virus filtering, click **Configure Cloud AV DB Exclusion Settings** in the main **Gateway Anti-Virus** page.

**Cloud AV Exclusions List**

Cloud AV Signature ID:

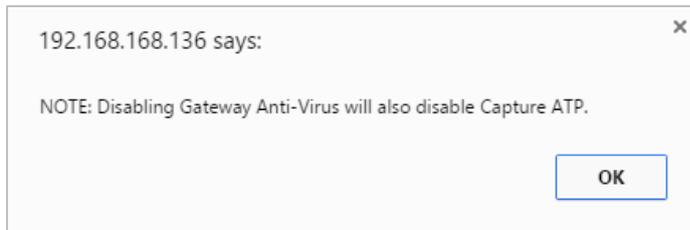
List:

- 1002067
- 5777326
- 5973803
- 9851466

- In the **Cloud AV Exclusions List** dialog, type or paste each signature ID to be excluded into the **Cloud AV Signature ID** field and then click **Add** to add it to the List.
- Optionally adjust the List by using the **Update**, **Remove**, or **Remove All** buttons.
- When finished, click **OK**.

## Disabling Gateway Anti-Virus or Cloud Anti-Virus

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



Capture ATP will stop working if either Gateway Anti-Virus or Cloud Anti-Virus is disabled. For example, if Gateway Anti-Virus is not enabled, the 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 Security Services > Gateway Anti-Virus page where you can enable it.

Capture ATP / **Settings**

Accept  Cancel

---

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

**Basic Setup Checklist**

- ✔ Capture ATP is Enabled until 09/04/2016. [\(disable it\)](#)
- ✘ You must enable Gateway Anti-Virus Database for Capture ATP to function. [\(manage settings\)](#)
- ✔ Cloud Anti-Virus Database is enabled. [\(manage settings\)](#)
- i Inspected Protocols [\(manage settings\)](#)

Direction	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP Stream
Inbound	✔	✔	✔	✔	✔	✘	✘
Outbound	✘	✘	n/a	✘	n/a	n/a	✘

# Configuring Capture ATP settings

Topics:

- [Basic setup checklist](#)
- [Bandwidth management](#)
- [Custom blocking behavior](#)

## Basic setup checklist

The [Capture ATP > Settings](#) page can appear in either enabled or disabled mode.

When Capture ATP is enabled, the [Capture ATP > Settings](#) page appears in enabled mode.

Dell SonicWALL Network Security Appliance Wizards | Help | Logout

Mode: Configuration ▶

Capture ATP / **Settings**

### Basic Setup Checklist

- ✓ Capture ATP service is enabled until May 4, 2017. ([disable.it](#))
- ✓ Gateway Anti-Virus is enabled. ([manage.settings](#))
- ✓ Cloud Anti-Virus Database is enabled. ([manage.settings](#))

**i** Inspected protocols. ([manage.protocols](#))

Direction	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP Stream
Inbound	✓	✓	✓	✓	✓	✗	✗
Outbound	✗	✗	n/a	✗	n/a	n/a	✗

### 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, .gz, .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 (*unlimited*)

Restrict to  kb

### Custom Blocking Behavior

Files which are not blocked by other Security Services, will be sent to Capture ATP for analysis. Indicate if the firewall should block the file while awaiting a verdict.

Allow all files by default  
Less secure. You will be alerted via email when files have been determined to be malicious after they were allowed onto your network.

Block all files until a verdict is returned  
More secure, but will slow down the download of some legitimate files and may require users to retry the download.

**Note: Only applies to HTTP and HTTPS file downloads**

The Capture ATP > Settings page has three main sections:

- Basic Setup Checklist
- Bandwidth Management
- Custom Blocking Behavior (aka: Block all files until a verdict is returned)

When Capture ATP is disabled, the Capture ATP > Settings page appears in disabled mode.

Accept Cancel

**Capture ATP is not currently running. See the Setup Checklist below for troubleshooting.**

**Basic Setup Checklist**

- ❗ Capture ATP subscription is valid until May 4, 2017 but the service is not currently enabled. ([enable it](#))
- ✅ Gateway Anti-Virus is enabled. ([manage settings](#))
- ✅ Cloud Anti-Virus Database is enabled. ([manage settings](#))
- ℹ Inspected protocols. ([manage protocols](#))

Direction	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP Stream
Inbound	✅	✅	✅	✅	✅	❌	❌
Outbound	❌	❌	n/a	❌	n/a	n/a	❌

**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, .gz, .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 (*unlimited*)
- Restrict to  kb

**Custom Blocking Behavior**  
Files which are not blocked by other Security Services, will be sent to Capture ATP for analysis. Indicate if the firewall should block the file while awaiting a verdict.

- Allow all files by default  
Less secure. You will be alerted via email when files have been determined to be malicious after they were allowed onto your network.
- Block all files until a verdict is returned  
More secure, but will slow down the download of some legitimate files and may require users to retry the download.

Note: Only applies to HTTP and HTTPS file downloads

If the user has manually disabled the Capture ATP service, or if there are licensing issues, the banner displays this message:

**Capture ATP is not currently running. See the Setup Checklist below for troubleshooting.**

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

The **Basic Setup Checklist** lists the setup tasks and displays any error states that may be present.

Basic Setup Checklist							
✓	Capture ATP service is enabled until May 4, 2017. ( <a href="#">disable it</a> )						
✓	Gateway Anti-Virus is enabled. ( <a href="#">manage settings</a> )						
✓	Cloud Anti-Virus Database is enabled. ( <a href="#">manage settings</a> )						
ⓘ	Inspected protocols. ( <a href="#">manage protocols</a> )						
Direction	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP Stream
Inbound	✓	✓	✓	✓	✓	✗	✗
Outbound	✗	✗	n/a	✗	n/a	n/a	✗

The **Basic Setup Checklist** is always visible and displays four setup tasks:

- [Service status](#)
- [Gateway Anti-Virus status](#)
- [Cloud Anti-Virus Database status](#)
- [Inspected protocols](#)

If there are any red warning icons, Capture ATP will not run properly, and the **Capture ATP > Settings** page will appear in disabled mode.

## Service status

The first line in the **Basic Setup Checklist** is the Service Status, which indicates the overall state of the service and can change automatically. The following table describes the messages that can appear in the **Basic Setup Checklist**.

Icon	Message	Link	Action
Green check	Capture ATP service is enabled until renewal_date.	<b>disable it</b>	Clicking the <b>disable it</b> link turns off Capture ATP and changes the page to disabled mode. This action does not require that the user press the <b>Accept</b> button to apply this change.
Red warning	Capture ATP subscription is valid until renewal_date but the service is not currently enabled.	<b>enable it</b>	Clicking the <b>enable it</b> link turns on Capture ATP and changes the page to enabled mode. This action does not require that the user press the <b>Accept</b> button to apply this change.
Red warning	Capture ATP subscription expired on renewal_date.	renew it	Clicking the renew it link takes the user to MySonicWALL to renew the service.

## Gateway Anti-Virus status

The second line in the **Basic Setup Checklist** is the Gateway Anti-Virus Status, which indicates the state of the Gateway Anti-Virus service.

Icon	Message	Link	Action
Green check	Gateway Anti-Virus is enabled.	manage settings	Clicking <b>manage settings</b> takes the user to the <b>Security Services &gt; Gateway Anti-Virus &gt; Gateway Anti-Virus Global Settings</b> page.
Red warning	You must enable Gateway Anti-Virus for Capture ATP to function.	manage settings	Clicking <b>manage settings</b> takes the user to the <b>Security Services &gt; Gateway Anti-Virus &gt; Gateway Anti-Virus Global Settings</b> page.

## Cloud Anti-Virus Database status

Icon	Message	Link	Action
Green check	Cloud Anti-Virus Database is enabled.	manage settings	Clicking <b>manage settings</b> takes the user to the <b>Security Services &gt; Gateway Anti-Virus &gt; Cloud Anti-Virus Global Settings</b> page.
Red warning	You must enable the Cloud Anti-Virus Database for Capture ATP to function.	manage settings	Clicking <b>manage settings</b> takes the user to the <b>Security Services &gt; Gateway Anti-Virus &gt; Cloud Anti-Virus Global Settings</b> page.

## Inspected protocols

Icon	Message	Link	Action
Black information	Inspected protocols.	manage protocols	Clicking <b>manage protocols</b> takes the user to the <b>Security Services &gt; Gateway Anti-Virus &gt; Gateway Anti-Virus Global Settings</b> page.
Red warning	No applicable traffic is being inspected. Capture will never be invoked.	manage protocols	Clicking <b>manage protocols</b> takes the user to the <b>Security Services &gt; Gateway Anti-Virus &gt; Gateway Anti-Virus Global Settings</b> page.

The **Inspected protocols** line also contains a table that shows the direction and the type of protocol being inspected.

- A green checkmark indicates that the protocol is being inspected.
- A gray X indicates that the protocol is not being inspected.
- N/A indicates that inspection is not applicable to this protocol in this direction.

## Bandwidth management

The Bandwidth Management section enables you to select the types of files that can be submitted to Capture ATP and to specify the maximum file size that can be submitted to Capture ATP.

**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 , .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

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 (1024Kb)**. The default size is the size specified by the License Manager.

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 License Manager limit.

## Custom blocking behavior

The Custom Blocking Behavior section allows you to customize the **Block all files until a verdict is returned** feature.

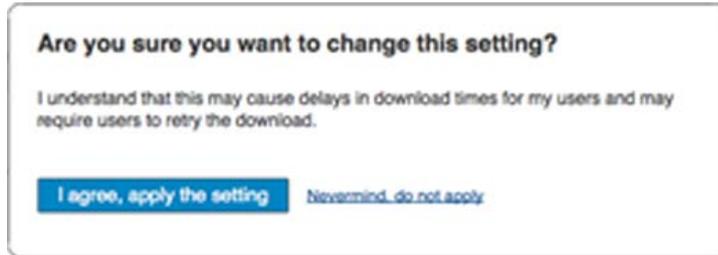
**Custom Blocking Behavior**  
Files which are not blocked by other Security Services, will be sent to Capture ATP for analysis. Indicate if the firewall should block the file while awaiting a verdict.

- Allow all files by default**  
Less secure. You will be alerted via email when files have been determined to be malicious after they were allowed onto your network.
- Block all files until a verdict is returned**  
More secure, but will slow down the download of some legitimate files and may require users to retry the download.

**Note: Only applies to HTTP and HTTPS file downloads**

Block all files until a verdict is returned is OFF by default.

The **Block all files until a verdict is returned** feature is potentially very confusing, and should only be invoked under very specific conditions. If you select this feature, a warning dialog appears.



Clicking the **I agree, apply the setting** button selects the **Block all files until a verdict is returned** option. You also must click the **Accept** button for the change to take effect.

Clicking the **Nevermind, do not apply** link, closes the dialog and leaves **Allow all files by default** selected.

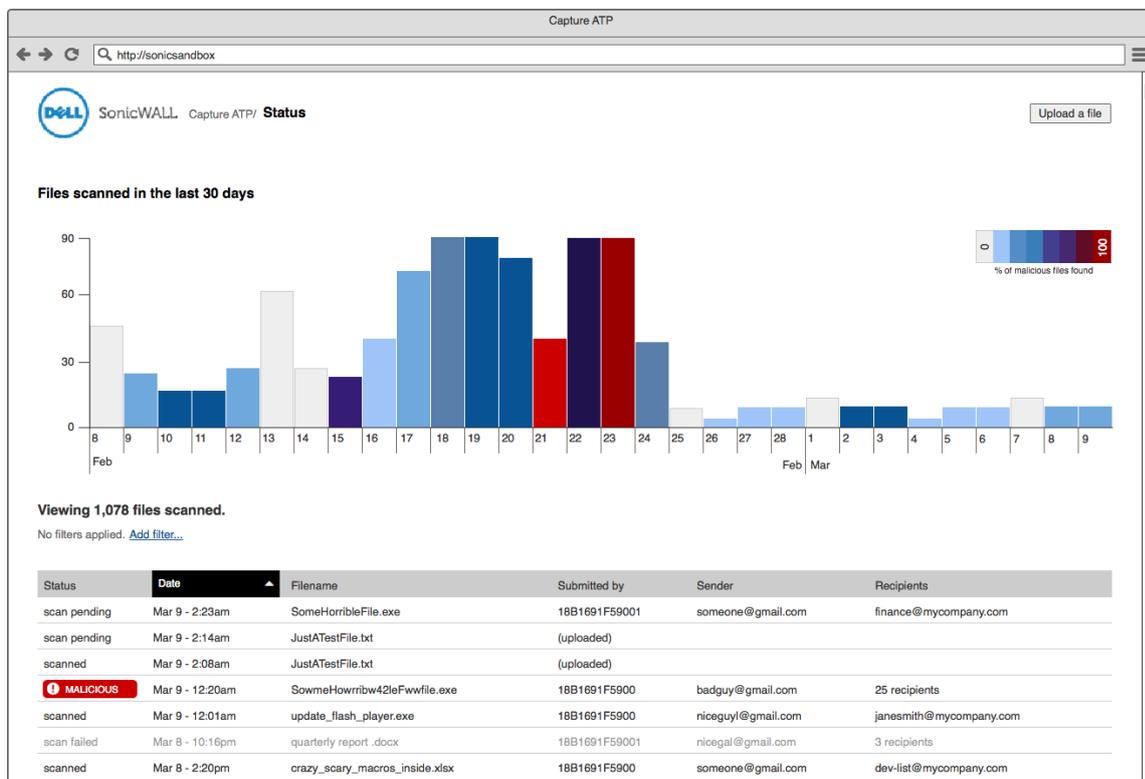
## Viewing Capture ATP status

Topics:

- [Viewing the graph and log table](#)
- [Filtering the log table](#)

## Viewing the graph and log table

The **Capture ATP > Status** page displays a graph and a log table that provide information for each file that has been scanned. Files can be uploaded to Capture ATP for scanning from this page by clicking the **Upload a file** button.

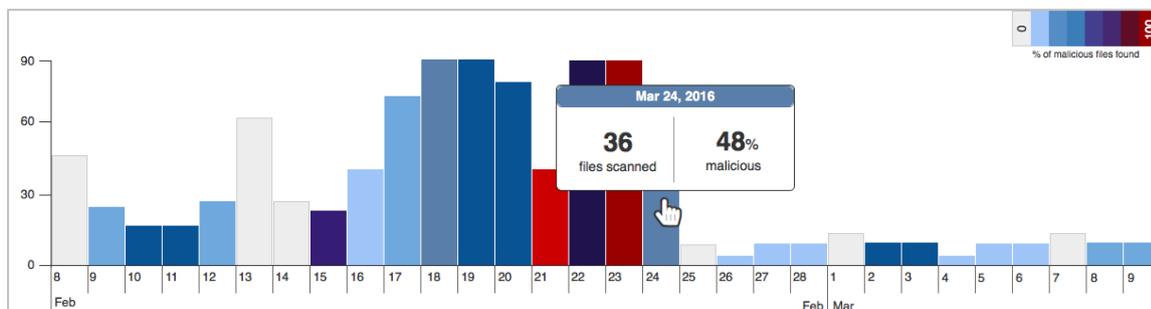


The graph shows the number of files scanned for each day. The X axis represents time and shows only the last 30 days. Each tick is one day. The Y axis represents the number of files scanned.

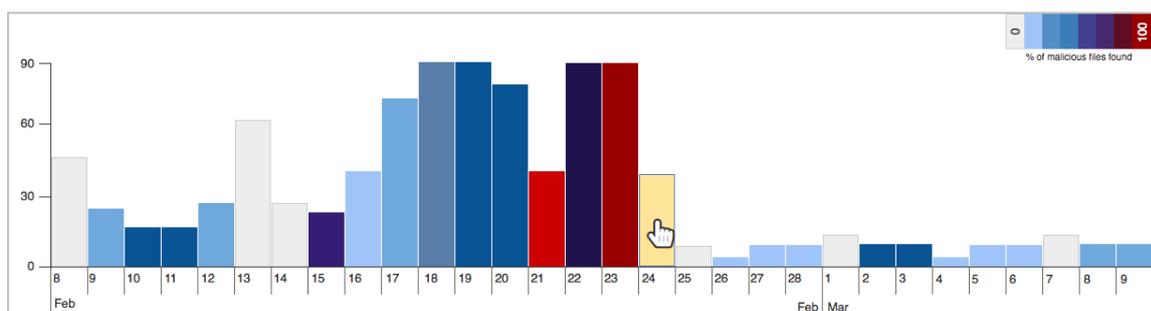
The percentage of malicious files found is represented by the color of each bar in the graph. The key shows the percentage that each color represents. Zero means no malicious files were found.

Below the graph, the log table shows information for each file that has been scanned. You can customize what is displayed in the log table, by clicking the **Add filter...** link. The graph, log table, and filters are bound, and any interactions on one will affect the others.

When you hover over a bar, a popup shows the actual numbers of files scanned and malicious files found.



You can click on a single bar in the graph to set the filter for the log table to show the details of that bar only.



Viewing 36 files of 1,078 total scanned.

Date: Feb 24, 2016 [Add filter...](#)

Status	Date	Filename	Submitted by	Src	Dest
scan pending	Mar 9 - 2:23am	SomeHorribleFile.exe	18B1691F59001	0.0.0.0:80	0.0.0.0:80
scanned	Mar 9 - 2:08am	JustATestFile.txt	(uploaded)		
<b>MALICIOUS</b>	Mar 9 - 12:20am	<b>SowmeHowrribw42leFwrfwfile.exe</b>	<b>18B1691F5900</b>	<b>0.0.0.0:80</b>	<b>0.0.0.0:80</b>
scan failed	Mar 9 - 12:01am	(unknown)	18B1691F5900	0.0.0.0:80	0.0.0.0:80
file not supported	Mar 8 - 11:13pm	JustATestFile.txt	(uploaded)		

The log table allows you to scroll through the list of scanned files. If a scan fails, that row is dimmed. If a **malicious** file is found, that row is bolded. Clicking on any row opens the threat report. For more information about threat reports, see [Viewing Threat Reports](#).

The heading for this page is dynamic and may appear in two states:

- When no filters are applied - Viewing *n* files scanned.
- When filters are applied - Viewing *n* files of *n* total scanned.

The columns for the log table are:

- The **STATUS** column displays these states:
  - scan pending - the scan is still in progress
  - scanned - the scan has completed, but no judgement is confirmed yet

- scan failed - the scan has failed
- MALICIOUS - the scan has completed, and the judgement is malicious (the word MALICIOUS is displayed in small caps in a red tag with a warning symbol)
- The Date column displays the date that the file was scanned.
- The Submitted by column displays the user ID number of the user who submitted the file to Capture ATP.
- The Src column displays the source IP address where the file originated.
- The Dest column displays the destination IP address where the file was sent.

The columns can be sorted as follows:

- The default sort order is reverse chronological order in the date column.
- A sorted column has a black background with an arrow indicating the direction of the sort.
- Clicking the header of a column sorts that column and toggles it in ascending or descending order.
- Hovering on the header of a column reveals whether that column can be sorted (arrows are hidden until hover)
- The selected sort order is persistent as filters are added or removed.

## Filtering the log table

You can filter the entries in the log table by adding a filter that only displays certain criteria for a certain column, such as what the status, date, or src is, etc.

*To add a filter to the log table:*

- 1 On the Capture ATP > Status page, click the Add filter... link. The filter builder bar appears.



- 2 Select the criteria you want from the drop-down menus:
  - a From the first drop-down menu, select the column name, such as Status.
  - b From the second drop-down menu, select the operator: is or is not
  - c From the third drop-down menu, select the appropriate criteria for the selected column.
- 3 Click add. The filter builder bar disappears, and a filter tag is created.



**i** | **NOTE:** Only one type of filter can be applied to the log table at a time.

The add filter... link reappears after the filter is added and the table results are updated immediately.

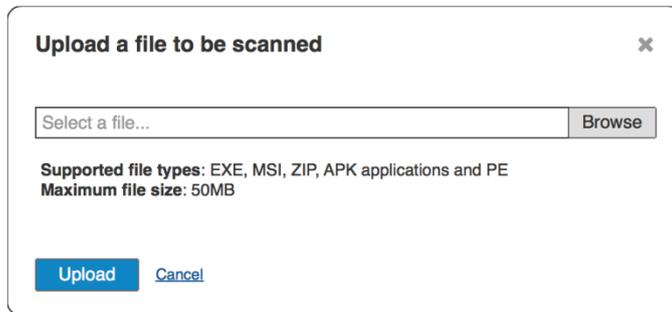
If you press x, the filter builder bar disappears and the filter is not applied to the log table.

# Uploading a file for analysis

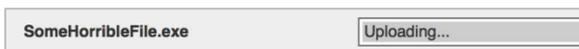
You can upload files to be scanned using the **Upload File** button on the **Capture ATP > Status** page.

*To upload a file for scanning:*

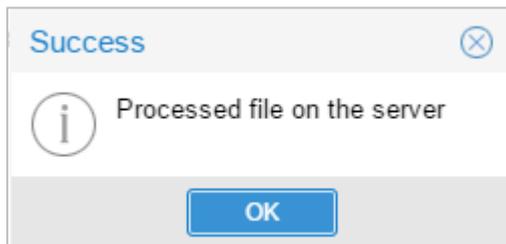
- 1 On the **Capture ATP > Status** page, click the **Upload File** button. The **Upload** dialog appears.



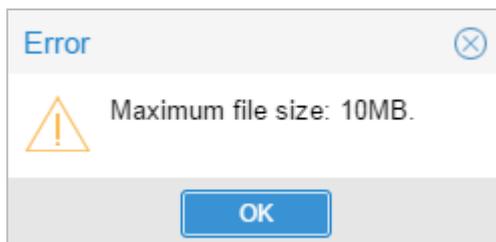
- 2 Click the **Browse** button and locate and select the file you want to scan. The progress of the upload is shown in an inline status bar at the top of the page.



If the upload completes successfully, this message is shown.



If upload fails, this error message is shown.



The message remains on screen for 15 seconds, and then disappears.

## Viewing threat reports

When you click on any row in the logs table on the **Capture ATP > Status** page, the **Capture ATP** threat report appears in a new browser window. The report format varies depending on whether a full analysis was performed or the judgment was based on preprocessing.

Topics:

- [Launching the threat report from the logs table](#)
- [Viewing the threat report header](#)

- Viewing the threat report footer
- Viewing the static file information
- Viewing threat reports from preprocessing
- Viewing threat reports from a full analysis

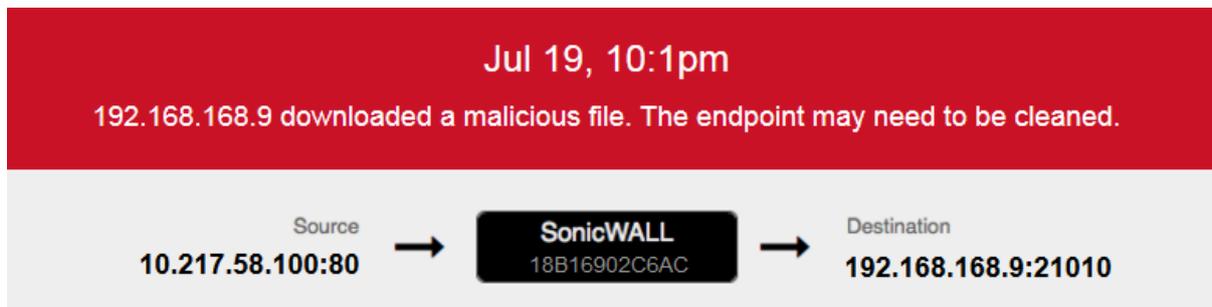
## Launching the threat report from the logs table

You can launch a threat report by clicking on any row in the logs table on the Capture ATP > Status page. Hovering your mouse pointer over a row highlights it, and you can click anywhere in the row to launch the threat report in a new browser window.

An exception exists for archives which do not contain any supported file types. In this case, no threat report is launched.

## Viewing the threat report header

The report header is very similar among the various threat reports. This section describes the header components and variations.



### Colored banner:

- The colored banner is red for a malicious file, and blue for a clean file.
- The top entry displays the date and time that the file was submitted to Capture ATP for analysis.
- Below the date and time, a summary of the result is displayed.

### Lower banner:

- The lower part of the banner contains the connection information.
- On the left is the IP address (IPv4) and port number of the connection source. This is the address from which the file was sent.
- In the middle is the firewall identified by its serial number or friendly name.
- On the right is the IP address (IPv4) and port number of the connection destination. This is the address to which the file is being sent.

## Viewing the threat report footer

The report footer is very similar among the various threat reports.



The **File Identifiers** are displayed at the left side of the footer. The following file identifiers are displayed, one per line:

- MD5
- SHA1
- SHA256

On the right side of the footer, the following information is displayed:

- **Serial Number** – This is the serial number of the firewall that sent the file. This is not displayed if the file was manually uploaded.
- **Capture ATP Version** – This is the software version number of the Capture ATP service running in the cloud.
- **Report Generated** – This is the timestamp in UTC format of when the report was generated.

## Viewing the static file information

The static file information is displayed on the left side of the threat report, and is similar across all types of reports.



The file information includes:

- File size in kilobits (kb)
- File type
- File name as it was intercepted by the firewall

# Viewing threat reports from preprocessing

There are varying amounts of data on a preprocessor threat report, based on whether the file was found to be malicious or clean.

Preprocessor threat report for a malicious file:

**Mar 30, 12:30am**  
172.17.0.146 downloaded a malicious file. The endpoint may need to be cleaned.

Source: 37.59.43.72:80 → SonicWALL 18B1691F5900 → Destination: 172.17.0.146:60669

**32kb PE32 executable (GUI) Intel 80386**  
filename\_of\_some\_badthing73992.exe

- virus scanners detected malware
- vendor reputation passed
- domain reputation passed
- embedded code found

**Analysis Summary**  
This file was supplied by a reputable vendor on a reputable domain. However embedded code was detected and 43 of the 62 virus scanners identified it as known malware. It was therefore judged malicious.

**43 of 62 virus scanners detected known malware**

Win32.Expiro.Gen.3	Win32/Expiro	Virus.Win32.Expiro.p (v)	Win32.Expiro.Gen.3
Win32.Expiro.Gen.3	Win32/Expiro5.Gen	Virus/Win32.Expiro.nr	Virus.Expiro.Win32.42
Win32.Xpirat-A	W32/Expiro.nr	Win32.Expiro.Gen.3	Virus.Win32.Expiro.p (v)
W32.FamVT.ExpiroPC.PE	W32.Expiro.NR	Win.Trojan.Expiro-1795	Virus.Expiro.2414
Virus.Win32.Expiro.SR	W32/Expiro.BG	Win32.Expiro.80	PE_EXPIRO.AR
Win32/Expiro.AY	Win32.Expiro.Gen.3 (B)	W32/Expiro.BG	PE_EXPIRO.AR
Win32.Expiro.Gen.3	W32/Expiro.W	Win32.Expiro.Gen.3	W32/Expiro-S
Virus.Win32.Expiro	Virus ( 0040f4dc1 )	Virus ( 0040f4dc1 )	PE.Trojan.Win32.Expiro.b1075356111
Virus.Win32.Expiro.nr	W32/Expiro.gen.p	BehavesLike.Win32.Salityjc	Win32/Expiro.AO
Win32.Expiro.Gen.3	Virus/Win32/Expiro.CD	Virus.Win32.Expiro.civwed	W32/Expiro.O
Expiro.YJ	Virus.Win32.Expiro.aab	W32.Xpiro.F	

**File Identifiers**  
MD5: 19213ad9a1e356c064065b3d26bc6871  
SHA1: c018e40f411864e6577e5b5a19ca13d9b366bbc9  
SHA256: 9f143d3dd282664dbc7df2de4dbb95e3c5ce9b2475f8109cee562b9765345d4f

Serial Number 18B1691F5900  
Capture ATP Version 0.1  
Report Generated on 2016-07-21 T 02:56 UTC

The above threat report format is seen when the virus scans reveal malware in the file.

## Preprocessor threat report for a clean file:

Capture ATP Report | SonicWALL

http://sonicsandbox.sonicwall.com

SonicWALL | Capture ATP Report

Email to... Export

Mar 30, 12:30am

SonicWall 18B1691F5900 submitted a file to Capture ATP for analysis. It was not found to be malicious.

Source: 37.59.43.72:80 → SonicWALL 18B1691F5900 → Destination: 172.17.0.146:60669

32kb  
PE32 executable (GUI)  
Intel 80386

filename\_of\_some\_badthing73992.exe

62  
virus scanners passed

✓  
vendor reputation passed

?  
domain reputation inconclusive

✓  
embedded code check passed

**Analysis Summary**  
This file was supplied by Adobe, a reputable vendor.  
Since there was also no embedded code and is not known malware, it was not judged as malicious.

**File Identifiers**  
MD5: 19213ad9a1e356c064065b3d26bc6871  
SHA1: c018e40f411864e6577e5b5a19ca13d9b366bbc9  
SHA256: 9f143d3dd282664dbc7df12de4d8b95e3c5cee9b2475f8109cee562b9765345d4f

Serial Number 18B1691F5900  
Capture ATP Version 0.1  
Report Generated on 2016-07-21 T 02:56 UTC

A clean threat report like the one shown above is seen in either of the following two cases:

Case one:

- Virus scans are inconclusive or all good.
- The file matches domain or vendor allow lists.

Case two:

- Virus scans are inconclusive or all good.
- No embedded code is present in the file.

See the following topics for more information about preprocessor reports:

- [Analysis summary and status boxes in preprocessor reports](#)
- [Malware names in preprocessor reports](#)

## Analysis summary and status boxes in preprocessor reports

Preprocessor threat reports contain an Analysis Summary section on the left side, which summarizes the findings based on the four phases of analysis during preprocessing.

**Analysis Summary**

This file was supplied by a reputable vendor on a reputable domain.

However embedded code was detected and 43 of the 62 virus scanners identified it as known malware.

It was therefore judged malicious.

The results from the four phases of preprocessing are displayed in the status boxes.



virus scanners detected malware



vendor reputation passed



domain reputation passed



embedded code found

62

virus scanners passed



vendor reputaiton passed



domain reputation inconclusive



embedded code check passed

Each phase results in a true or false outcome. The following table shows what happens in the process depending on the result of each phase of the preprocessing.

### Four areas of preprocessor analysis

Preprocessor phase result	Virus scanners detect malware?	Vendor reputation - on Allow list?	Domain reputation - on Allow list?	Embedded code found in the file?
True	<b>Malicious</b>	Non-malicious	Non-malicious	Continue analysis
False	Continue analysis	Continue analysis	Continue analysis	<b>Non-malicious</b>

Some phase results trigger an immediate judgment of either **Malicious** or **Non-malicious**, as indicated in the above table. Otherwise, that phase ends with the “Continue analysis” state.

If all phases of preprocessing result in the “Continue analysis” state, the file is sent to the cloud for full analysis by Capture ATP.

- i **NOTE:** The vendor reputation filter is only applicable to PE files, and the domain reputation might not be available for files delivered over SMTP. In these cases, the “Continue analysis” state is the phase result.

## Malware names in preprocessor reports

If the virus scanners detect known malware in the file, all virus names are listed in the content area of the report.

43 of 62 virus scanners detected known malware			
Win32.Expiro.Gen.3	Win32/Expiro	Virus.Win32.Expiro.p (v)	Win32.Expiro.Gen.3
Win32.Expiro.Gen.3	Win32/Expiro5.Gen	Virus/Win32.Expiro.nr	Virus.Expiro.Win32.42
Win32:Xpirat-A	W32/Expiro.nr	Win32.Expiro.Gen.3	Virus.Win32.Expiro.p (v)
W32.FamVT.ExpiroPC.PE	W32.Expiro.NR	Win.Trojan.Expiro-1795	Virus.Expiro.2414
Virus.Win32.Expiro.SR	W32/Expiro.BG	Win32.Expiro.80	PE_EXPIRO.AR
Win32/Expiro.AY	Win32.Expiro.Gen.3 (B)	W32/Expiro.BG	PE_EXPIRO.AR
Win32.Expiro.Gen.3	W32/Expiro.W	Win32.Expiro.Gen.3	W32/Expiro-S
Virus.Win32.Expiro	Virus ( 0040f4dc1 )	Virus ( 0040f4dc1 )	PE:Trojan.Win32.Exprio.bl1075356111
Virus.Win32.Expiro.nr	W32/Expiro.gen.p	BehavesLike.Win32.Sality.jc	Win32/Expiro.AO
Win32.Expiro.Gen.3	Virus:Win32/Expiro.CD	Virus.Win32.Expiro.clnvwd	W32/Expiro.O
Expiro.YJ	Virus.Win32.Expiro.aab	W32.Xpiro.F	

# Viewing threat reports from a full analysis

Full analysis threat reports provide the same set of information for both malicious and non-malicious files, although the banner color is different.

**Mar 30, 12:30am**  
172.17.0.146 downloaded a malicious file. The endpoint may need to be cleaned.

Source: 37.59.43.72:80 → SonicWALL 18B1691F5900 → Destination: 172.17.0.146:60669

**32kb**  
PE32 executable (GUI)  
Intel 80386  
filename\_of\_some\_badthing73992.exe

**62** virus scanners  
**2** reputation databases  
**3** detonation engines  
**6** live detonations

**Why live detonations were needed**

- Not a known malware
- Embedded code found
- Not a known reputable vendor
- Not a known reputable domain
- All other results inconclusive. File sent to detonation engines for further analysis.

**Summary of actions once detonated**

Engine	time	libraries	files	registries	processes	mutexes	functions	connection	download full details
<b>Engine Alpha</b>									
100 Windows XP Pro	130s	9	73		6	37	1	7	XML, Screenshots, PCAP
92 Windows 7	124s	9	85	1	5	36	1	12	XML, Screenshots, PCAP
<b>Engine Beta</b>									
12 Windows Phone	130s	9	73		6	37	1	7	XML, Screenshots, PCAP
0 Android	timeout								XML, Screenshots, PCAP
<b>Engine Gamma</b>									
100 Windows XP Pro	130s	9	73		6	37	1	7	XML, Screenshots, PCAP
63 Windows 7	124s	9	89	1	5	36	1	1	XML, Screenshots, PCAP

**File Identifiers**  
MD5: 19213ad9a1e356c064085b3d26bc6871  
SHA1: c018e40f411864e6577e5b5a19ca13d9b368bbc9  
SHA256: 9f143d3dd282664dbc7d12de4dbb95e3c5ee9b2475f8109cee562b9765345d4f

Serial Number 18B1691F5900  
Capture ATP Version 0.1  
Report Generated on 2016-07-21 T 02:56 UTC

This Threat Report format is used when the following conditions occur:

- Virus scans are inconclusive or all good.
- Embedded code is present in the file.
- The file does not match domain or vendor allow lists.

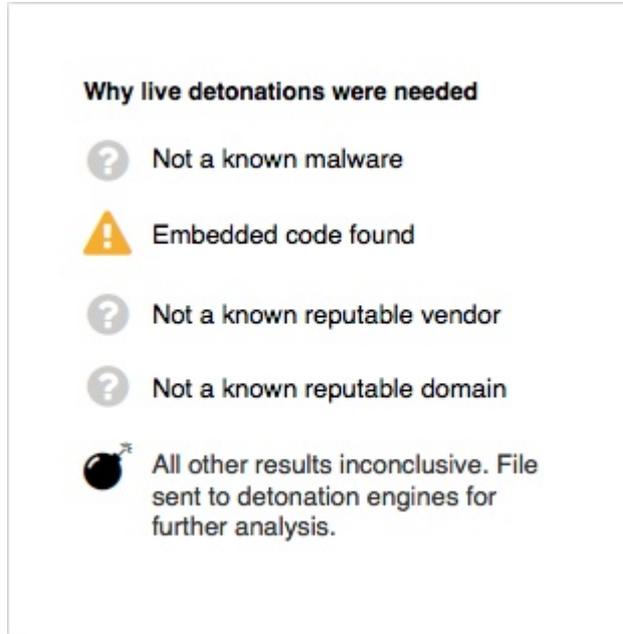
See the following topics for more information about full analysis reports:

- [Why live detonations were needed](#)
- [Status boxes in a full analysis threat report](#)
- [Analysis engine results tables](#)

## Why live detonations were needed

The left side of the full analysis threat report displays a summary of the preprocessing results as an explanation of why live detonations were needed. The term *live detonations* is used to indicate that one or more analysis engines and multiple environments were used to analyze the file in the cloud servers.

The set of preprocessing results which lead to full analysis of the file is shown below:



## Status boxes in a full analysis threat report

The status boxes in full analysis threat reports display status from preprocessing results as well as information about the analysis performed in the cloud servers.



### Virus scanners:

- This is the number of Anti-Virus vendors used, regardless of the judgment from each.
- SonicWALL Gateway Anti-Virus and Cloud Anti-Virus each count as one.
- Additional virus scanners from many AV products and online scan engines are included in the total.

### Reputation databases:

- One is the vendors allowed list.
- One is the domains allowed list.

### Detonation engines:

- This is the number of analysis engines used to analyze the file.

- One is the SonicWALL analysis engine.
- Additional analysis engines from third-party vendors are included in the count.

**Live detonations:**

- This is the total number of environments used across all analysis engines.
- The environment is comprised of the analysis engine and the operating system on which it was run.

## Analysis engine results tables

Under the status boxes, the full analysis threat report displays multiple tables showing the results from each analysis engine.

		Summary of actions once detonated							See everything the engines saw			
Engine Alpha		time	libraries	files	registries	processes	mutexes	functions	connection	download full details		
100	Windows XP Pro	130s	9	73		6	37	1	7	XML	Screenshots	PCAP
92	Windows 7	124s	9	89	1	5	36	1	12	XML	Screenshots	PCAP
Engine Beta		time	libraries	files	registries	processes	mutexes	functions	connection	download full details		
12	Windows Phone	130s	9	73		6	37	1	7	XML	Screenshots	PCAP
0	Android	timeout								XML	Screenshots	PCAP
Engine Gamma		time	libraries	files	registries	processes	mutexes	functions	connection	download full details		
100	Windows XP Pro	130s	9	73		6	37	1	7	XML	Screenshots	PCAP
63	Windows 7	124s	9	89	1	5	36	1		XML	Screenshots	PCAP

The engines are designated by names from the Greek alphabet, such as Alpha, Beta, Gamma, etc.

Each row represents a separate environment, and indicates the operating system in which the engine was executed.

The overall score from the analysis in each environment is displayed in a highlighted box to the left of the operating system. The color of the box indicates whether the score triggered a malicious or non-malicious judgment:

- A score in a red box indicates a malicious judgment
- A score in a grey box indicates a non-malicious judgment

For each environment, the columns provide the analysis duration and a summary of actions once detonated:

- **Time** – The time taken by the analysis, using ‘s’ for seconds, ‘m’ for minutes, and **timeout** if the analysis did not complete.
- **Libraries** – Cumulative count of malware libraries that were read during the analysis.
- **Files** – Cumulative count of files that were created, read, updated or deleted during the analysis.
- **Registries** – Cumulative count of OS registries that were read during the analysis.
- **Processes** – Cumulative count of processes that were created during the analysis.
- **Mutexes** – Cumulative count of mutual exclusion objects that were used during the analysis to lock a resource for exclusive access.
- **Functions** – Cumulative count of functions executed during the analysis.
- **Connection** – Cumulative count of network connections that were created during the analysis.

You can click any cell in the **Summary of actions** table to jump to the full data available further down in the report. Blank cells are not clickable.

The last column provides access to the full details of the analysis by the different engines:

- **XML** — Clicking here lets you open or save an XML file which contains all the detailed data behind the above counts.
- **Screenshots** — Clicking here lets you open or save a zip file of all the screenshots produced by the analysis.
- **PCAP** — Clicking here lets you open or save a packet capture file in libpcap format with details about the connections opened during the analysis.

# About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit <http://www.software.dell.com>.

## Contacting Dell

For sales or other inquiries, visit <http://software.dell.com/company/contact-us.aspx> or call 1-949-754-8000.

## Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <http://support.software.dell.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to <http://software.dell.com/trials>.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

 **NOTE:** Please DO NOT CONTACT SUPPORT about Beta software/firmware. For product functionality feedback and questions for Beta releases, send Email to [sandboxbeta@sonicwall.com](mailto:sandboxbeta@sonicwall.com).

Copyright © 2016 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and SonicWALL are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

## Patents

For more information about applicable patents, go to <http://software.dell.com/legal/patents.aspx>.

## Legend

 **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.

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

---

Last updated: 7/25/2016

232-00xxxx-xx Rev 06