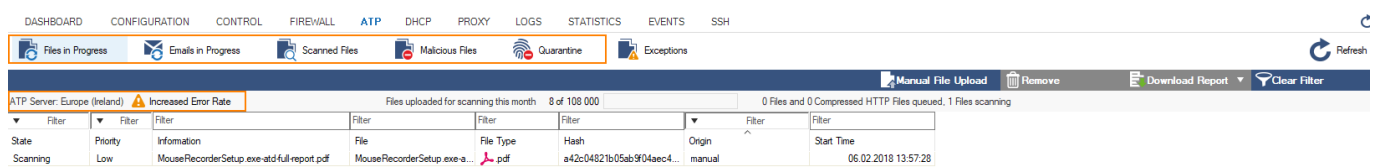


ATP Tab

<https://campus.barracuda.com/doc/79463246/>

The **ATP** tab both displays results and processes file scanning via Advanced Threat Protection (ATP). Before you can use the **ATP** tab, you must enable ATP in the firewall settings. For more information, see [Advanced Threat Protection \(ATP\)](#).


The location of the ATP server and its status is displayed on top of the data table for every ribbon bar menu except the menu **Exceptions**:



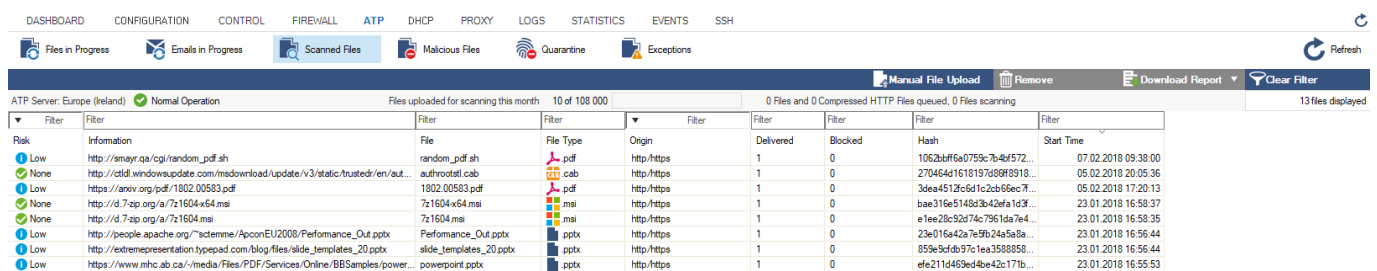
There are four options available for the status:

ATP Server:  Initializing

ATP Server: Europe (Ireland)  Normal Operation

ATP Server: Europe (Ireland)  Increased Error Rate

ATP Server: Europe (Ireland)  Unable to Submit Files



The information displayed on the **ATP** page is listed in the following columns:

- **Risk** – Displays the risk classification.
- **Information** – Displays the URL of the scanned file.
- **File** – Displays the scanned file entry.
- **File Type** – Displays the scanned file type.
- **Origin** – Displays the source of the scanned file.

- **Delivered** – Displays the number of file deliveries.
- **Blocked** – Displays the number of blocks for this file.
- **Start Time** – Displays the time the scan was started.

To access the information on the files scanned by ATP, click the service bar icons top of the page:

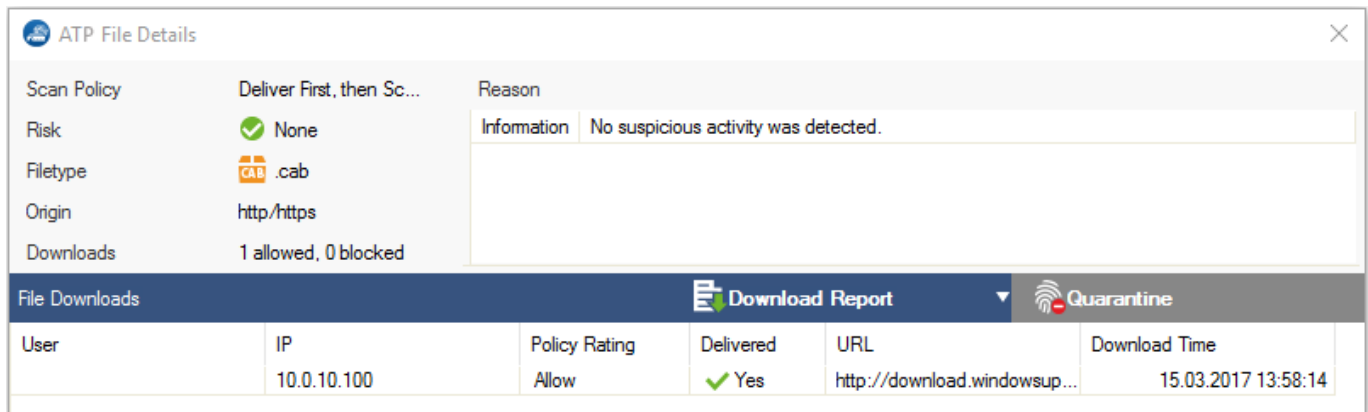
- **Files in Progress** – Clicking this icon displays all files that are selected for the scan process.
- **Emails in Progress** – Clicking this icon displays all emails that are selected for the scan process.
- **Scanned Files** – Clicking this icon queries the ATP list and displays all files scanned by ATP.
- **Malicious Files** – Clicking this icon displays all files blocked by ATP.
- **Quarantine** – Clicking this icon displays the users and IP addresses whose connections were redirected to the quarantine and shows the time since the address was put into quarantine.
- **Exceptions** – Clicking this icon displays all files that are exempted from scanning due to whitelisting or from forwarding due to blacklisting.

Filter Options


To filter the list according to specific criteria (such as risk, URL, or file type), use the fields on top of each column. Click the **Clear Filter** icon on the top right of the ribbon bar to remove the criteria entered.

Managing Threat Information

Double-clicking a file opens the **ATP File Details** window where you can view additional information on the file:



The screenshot shows the 'ATP File Details' window with the following information:

Scan Policy	Deliver First, then Sc...	Reason
Risk	✓ None	Information No suspicious activity was detected.
Filetype	 .cab	
Origin	http/https	
Downloads	1 allowed, 0 blocked	

Below the details is a ribbon bar with 'File Downloads', 'Download Report', and 'Quarantine' options. A table below the ribbon bar shows the following data:

User	IP	Policy Rating	Delivered	URL	Download Time
	10.0.10.100	Allow	✓ Yes	http://download.windowsup...	15.03.2017 13:58:14

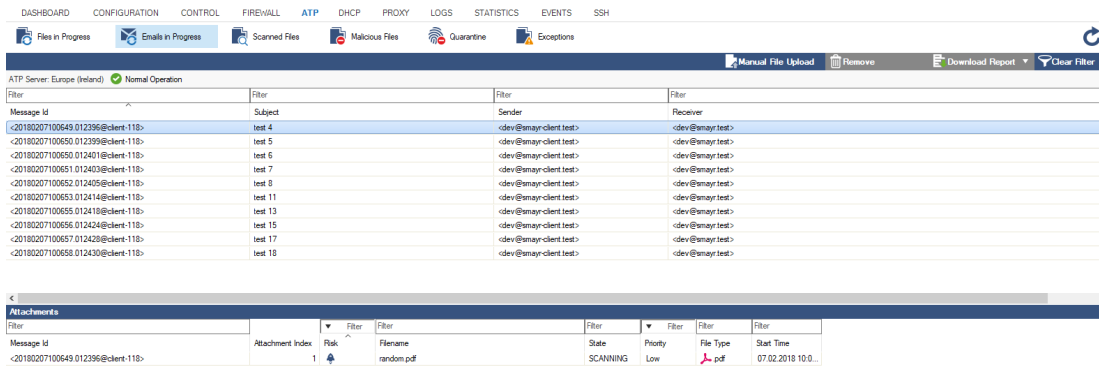
- **Scan Policy** – Displays the scanning policy that applies to the file.
- **Risk** – Shows the risk classification. The **Reason** section on the right displays further details on

the blocking reason.

- **Filetype** - The file type.
- **Origin** - The path of the scanned file.
- **Downloads** - Shows the number of downloads for this file and the action that was performed by ATP.

The **File Downloads** section displays further details on the file, such as download origin and user, URL, and download time.

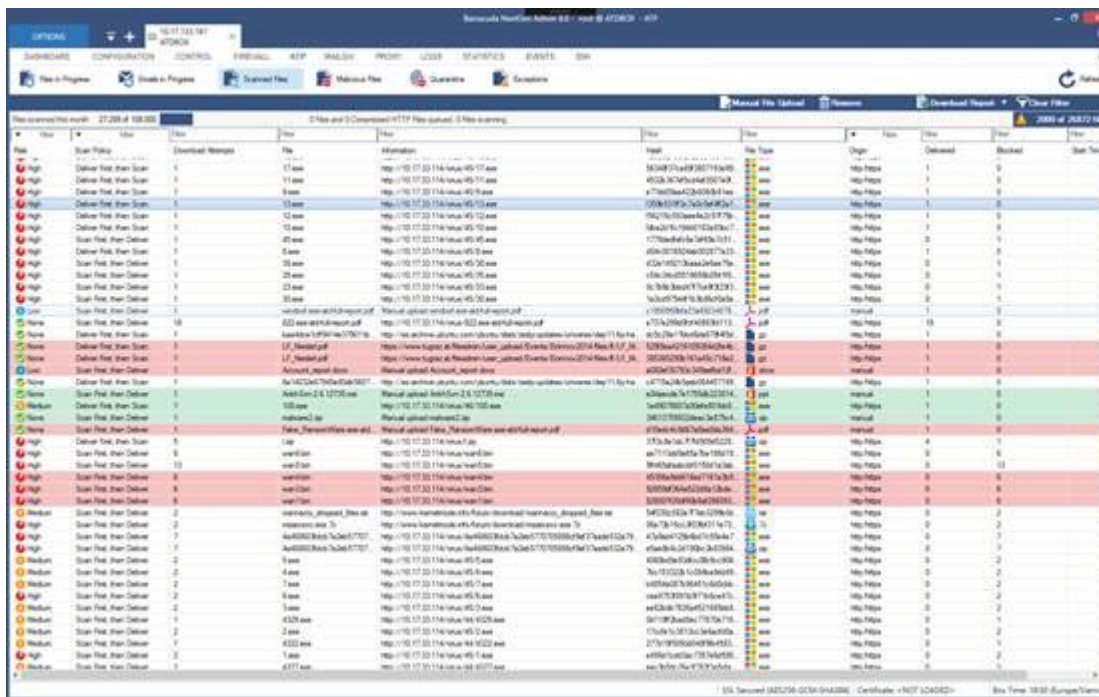
The **Emails in Progress** page displays emails that have attachments that are currently scanned. This applies only to the option Scan First Then Deliver.



Message Id	Subject	Sender	Receiver
<20180207100649.012396@clert-118>	test 4	<dev@amay-client-test>	<dev@amay-test>
<20180207100650.012399@clert-118>	test 5	<dev@amay-client-test>	<dev@amay-test>
<20180207100650.012401@clert-118>	test 6	<dev@amay-client-test>	<dev@amay-test>
<20180207100651.012403@clert-118>	test 7	<dev@amay-client-test>	<dev@amay-test>
<20180207100652.012405@clert-118>	test 8	<dev@amay-client-test>	<dev@amay-test>
<20180207100653.012414@clert-118>	test 11	<dev@amay-client-test>	<dev@amay-test>
<20180207100655.012418@clert-118>	test 13	<dev@amay-client-test>	<dev@amay-test>
<20180207100656.012424@clert-118>	test 15	<dev@amay-client-test>	<dev@amay-test>
<20180207100657.012428@clert-118>	test 17	<dev@amay-client-test>	<dev@amay-test>
<20180207100658.012430@clert-118>	test 18	<dev@amay-client-test>	<dev@amay-test>

Message Id	Attachment Index	Risk	Filename	State	Priority	File Type	Start Time
<20180207100649.012396@clert-118>	1	1	random.pdf	SCANNING	Low	pdf	07.02.2018 10:0...

The **Scanned Files** page displays all files scanned by ATP. Whitelisted files are highlighted in green, and blacklisted files in light red.



File Name	Scan Policy	Download Message	File	Attention	File Type	Origin	Action	Status
17.exe	High	17.exe	http://192.168.1.104/scan/45-17.exe	Malicious	exe	http://192.168.1.104/scan/45-17.exe	Block	Blacklisted
15.exe	High	15.exe	http://192.168.1.104/scan/45-15.exe	Malicious	exe	http://192.168.1.104/scan/45-15.exe	Block	Blacklisted
13.exe	High	13.exe	http://192.168.1.104/scan/45-13.exe	Malicious	exe	http://192.168.1.104/scan/45-13.exe	Block	Blacklisted
12.exe	High	12.exe	http://192.168.1.104/scan/45-12.exe	Malicious	exe	http://192.168.1.104/scan/45-12.exe	Block	Blacklisted
10.exe	High	10.exe	http://192.168.1.104/scan/45-10.exe	Malicious	exe	http://192.168.1.104/scan/45-10.exe	Block	Blacklisted
8.exe	High	8.exe	http://192.168.1.104/scan/45-8.exe	Malicious	exe	http://192.168.1.104/scan/45-8.exe	Block	Blacklisted
5.exe	High	5.exe	http://192.168.1.104/scan/45-5.exe	Malicious	exe	http://192.168.1.104/scan/45-5.exe	Block	Blacklisted
3.exe	High	3.exe	http://192.168.1.104/scan/45-3.exe	Malicious	exe	http://192.168.1.104/scan/45-3.exe	Block	Blacklisted
25.exe	High	25.exe	http://192.168.1.104/scan/45-25.exe	Malicious	exe	http://192.168.1.104/scan/45-25.exe	Block	Blacklisted
23.exe	High	23.exe	http://192.168.1.104/scan/45-23.exe	Malicious	exe	http://192.168.1.104/scan/45-23.exe	Block	Blacklisted
30.exe	High	30.exe	http://192.168.1.104/scan/45-30.exe	Malicious	exe	http://192.168.1.104/scan/45-30.exe	Block	Blacklisted
random.pdf	Low	random.pdf	http://192.168.1.104/scan/45-random.pdf	Whitelisted	pdf	http://192.168.1.104/scan/45-random.pdf	Allow	Whitelisted

The **Exceptions page** displays two tables. The upper table with the name **Whitelisted Files** displays files that are exempted from scanning regardless if they are a risk or not. The lower table with the name **Blacklisted Files** displays files that are blacklisted. These files will not be scanned and not be forwarded regardless if they are a risk or not.

DASHBOARD CONFIGURATION CONTROL FIREWALL **ATP** MAILGW PROXY LOGS STATISTICS EVENTS SSH

Files in Progress Emails in Progress Scanned Files Malicious Files Quarantine **Exceptions**

Whitelisted Files

	Filter	Filter	Filter	Filter	Filter	Filter	Filter
Risk	Information	File	File Type	Origin	Deliv...	Block...	Start Time
✔ N...	Email data not displayed. File is not malicious.	text.txt.33	pdf	smtp	1	0	27.06.2017 17:19:14

Blacklisted Files

	Filter	Filter	Filter	Filter	Filter	Filter	Filter
Risk	Information	File	File Type	Origin	Deliv...	Block...	Start Time
✔ N...	Email data not displayed. File is not mal...	text.txt.35	pdf	smtp	1	0	27.06.2017 17:19:14
✔ N...	Email data not displayed. File is not mal...	text.txt.37	pdf	smtp	1	0	27.06.2017 17:19:14

Available Actions

For instant scanning and process management, the links section on the top right of the page provides the following options:

- **Manual File Upload** - Opens the file browser from where you can select a file to be scanned. For more information, see [How to Manually Upload Files to ATP](#).
- **Remove** - Removes a selected entry from the file list.
- **Download Report** - Downloads the scan report to a file.

Figures

1. atp_status_for_ribbon_menu.png
2. atp_status_0.png
3. atp_status_1.png
4. atp_status_2.png
5. atp_status_3.png
6. atp_page_with_status.png
7. atp_details.png
8. emails_in_progress_with_atp_status.png
9. atp_scan.png
10. atp_exceptions_file_overview.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.