Advanced Threat Protection Configuration

https://campus.barracuda.com/doc/46895388/

The Barracuda Web Security Gateway leverages Advanced Threat Protection (ATP) to provide for safe use of online applications and tools without exposure to web-borne ransomware and other threats.

Traditional signature-based antivirus solutions are no longer sufficient to defend against new breed of malware attacks. This has resulted in the emergence of heuristic-based antivirus solutions and advanced threat protection solutions with sandboxing capabilities. Advanced Threat Protection (ATP) is a subscription-based service that detects and notifies the administrator of advanced malware, zero-day exploits, and targeted attacks that are not detected by the Barracuda Web Security Gateway virus scanning features. The ATP service analyzes files downloaded from the internet in a secured cloud based sandbox environment.

- In order to scan files transmitted over HTTPS protocol, you must enable SSL Inspection and configure it to inspect the domain from which the file is sent. See Using SSL Inspection With the Barracuda Web Security Gateway, or go to **ADVANCED > SSL Inspection** in the web interface and click **Help**. Also make sure to whitelist the domain range ***cudasvc.com** to allow necessary connections to the ATP service.
- ATP scan time varies based on file content. When the ATP option **Scan First, Then Deliver** is selected, because ATP sandbox analysis covers every possible scenario, scan time can take up to 4 hours in certain cases.

ATP Subscription

You can subscribe to the ATP service just as you do with Energize Updates. Your ATP subscription either expires when your Energize Updates subscription does, or before. In order to purchase an ATP subscription, you must have a valid Energize Updates subscription. Subscription status for ATP is shown on the **BASIC > Dashboard** page.

How ATP Works

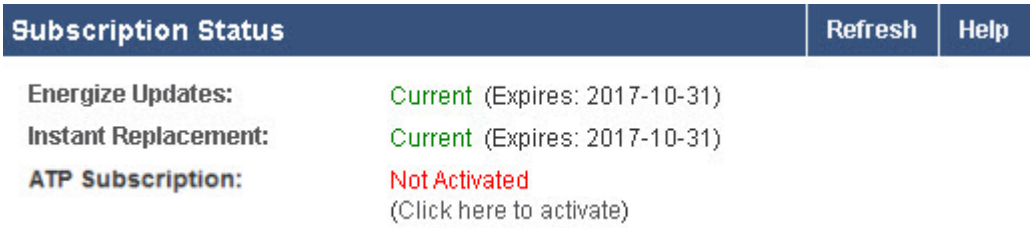
ATP analyzes attachment files (based on file types you specify on the **BASIC > Virus Checking** page) in the Barracuda ATP cloud and assigns a risk score. Infected files are sandboxed and deemed malicious by ATP when the service is enabled. Additionally, when you subscribe to the ATP service, you can view infected traffic on the **BASIC > ATP Log** page. The log provides the option to manually export a file in CSV format.

File Types Scanned by the Barracuda ATP Cloud:

- **Microsoft Office files** – doc, docx ,ppt, pps, pptx, ppsx, xls, xlsx
- **OpenOffice** – rtf, open office document extensions
- **Microsoft executables** – exe, msi, class, wsf
- **macOS executables**
- **PDF documents** – pdf
- **Android APK files** – apk
- **ZIP Archives** – 7z, lzh, bz, bz2, chm, cab, zip
- **RAR Archives** – rar4 and rar5
- **TAR Archives** – tar
- **GZ Content** – Content compressed with gzip
- **Javascript** – Manual scan

How to Get and Use ATP:

1. Subscribe by clicking on **Click here to activate** on the **BASIC > Dashboard** page as shown below.



2. Go to the **BASIC > Virus Checking** page. Set **Advanced Threat Protection (ATP)** to either:
   - **Deliver First, Then Scan –** The downloaded file is delivered to the user while ATP scans the file. If the file is then determined to be infected, an alert is sent to the **Threat Alerts Email Address** defined on the **BASIC > Administration** page**.**
   - **Scan First, Then Deliver** –
     - If the file for download is scanned within 1 second and a virus is detected, the user is served a standard block page indicating that the file has been blocked for that reason.
     - If the scan takes longer than 1 second, the user is served a block page with a message indicating that the file is still undergoing scanning. This page provides a button for the user to click to open another tab in the browser, which shows 'still under scan' status until the scan is complete. This new tab auto-refreshes and, once the scan is complete, will show if the file is either clean or blocked. The file will be delivered if clean. If the file is not clean, it will be blocked and the user alerted. If the user does not click the button to retrieve the file within 4 hours, the page times out and the user will need to download the file again. The original block page

served will automatically return to original browsing page.

> Note that blocking or allowing password protected files is affected both by the configured allow/block policy for encrypted archives, and by ATP. However, though ATP does try well known passwords to attempt scanning password protected files, the service usually cannot scan such files due to password protection, and returns a code stating that the file cannot be scanned. Such a file may be downloaded by a user, and because the scan status is undetermined, it is not listed in the ATP Log when ATP is configured for **Scan First, Then Deliver**. To ensure the greatest security in dealing with password-protected files, Barracuda recommends setting **Block Encrypted Archives** to **Yes**.

   - You can also select **No** to disable ATP scanning while keeping your subscription active.
3. Configure scanned file types and MIME types as shown on the page. Click **Help** for details.
4. Optionally set **Block Encrypted Archives** to **Yes** if you want to block downloading of password-encrypted archives such as .zip and .rar as viruses. Barracuda recommends setting to **Yes** as explained in the note above.
5. Click **Save**.

File Types Scanned by ATP

On the **BASIC > Virus Checking** page, you can select any of the following file types to scan with ATP, as well as specifying MIME types:

- archives
- ms_office
- pdf
- win_exe

ATP Statistics and Logs

You can view statistics on files scanned and determined to be infected by the ATP service on the **DASHBOARD** page, with more detail available on the **BASIC > ATP Log** page.

- **Status** - Possible values are:
  - **Clean** - No infection was detected.
  - **Scanning** - The attachment is undergoing scanning by ATP.
  - **Suspicious** - The scan is complete but the outcome of the scan is not definitive.
  - **Infected** - The ATP scan is complete and the infected file was blocked if the scan completed before delivery of the file. If not, the admin will receive an alert at the **Threat Alerts Email Address**.
  - **Error** - Indicates network issues in connecting with the ATP service, or the file type was

not supported.

- **Filename** - Name of the file being scanned or that was scanned by ATP. The maximum file name length supported for logging is 100 characters; anything longer than that will be truncated.
- **Username** - The user who downloaded the file.
- **IP Address** - IP address of the machine or network from which the threat was initiated.
- **URL** - The URL of the site from which the treat was initiated. The maximum URL length supported for logging is 2083 characters; anything longer than that will be truncated.
- **Scan Completed** - Date and time the ATP scan completed.
- **Report** - Click to print a report of ATP scan results.

Figures