How to Configure ATP in the HTTP Proxy

https://campus.barracuda.com/doc/41116326/Configure when and which types of files are uploaded to the Barracuda ATP Cloud for traffic passing through the HTTP proxy service. Users will receive downloaded files immediately. When files with a risk factor higher than the define risk threshold are detected, the associated users and/or IP addresses are placed in quarantine. Create access rules to define what is blocked for the infected users and/or IP addresses. Files whitelisted in the Malware Protection configuration of the HTTP Proxy are never scanned by ATP.

In this article:

Before you Begin

- You must have a Malware and an Advanced Threat Detection license subscription. For more information, see Licensing.
- Verify that you have configured a **System Notification Email** address. For more information, see How to Configure the System Email Notification Address.
- Verify that you have enabled malware protection for the HTTP proxy. For more information, see How to Configure Malware Protection in the HTTP Proxy.
- Verify that all file types you want to scan with ATP are not listed in the Virus Scan Exceptions. For more information, see How to Configure Malware Protection in the HTTP Proxy.

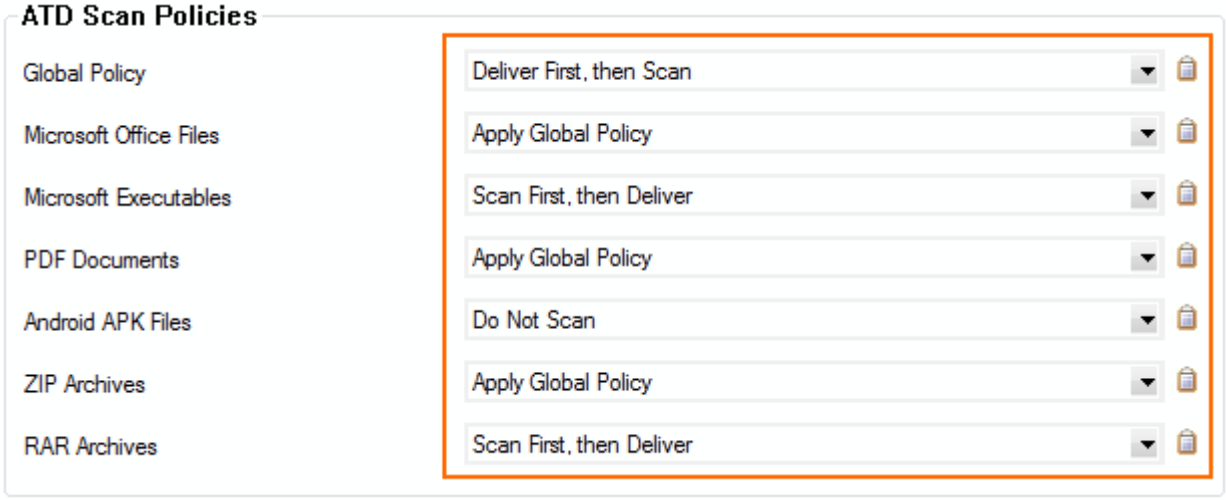
Step 1. Configure ATP Scan Policy and Risk Threshold

Configure the ATP scan policy to determine if the user will have to wait for scanning to complete before the file is forwarded.

1. Open the **Virus Scanner Settings** page (**Config > Full Config > Virtual Servers > *your virtual server* > Virus Scanner**).
2. Click **Lock**.
3. In the left menu, click **ATD**.
4. In the **ATD Scan Policy** section, select the **Global Policy: Deliver First, then Scan** – The user receives the file immediately. If malware is found the quarantine policy applies.
   Scan First, then Deliver does not work with the HTTP Proxy.
5. If needed set the individual scan policies for each file type:
   - **Apply Global Policy (default)**
   - **Do Not Scan** – This file type is not scanned and immediately forwarded to the user.

- **Deliver First, then Scan** – The user receives the file immediately. If malware is found the quarantine policy applies.
- **Scan First, then Deliver** – The user is redirected to a scanning page. After the scan is complete the download starts.

6. In the **ATD Threats** section, select the **Block Threats** policy:
   - **High Only** – File classified as high risk are blocked.
   - **High and Medium (Default)** – Files classified as high or medium risk are blocked.
   - **High, Medium and Low** – Files classified as high, medium or low risk are blocked. Only files with classification **None** are allowed.



7. Set **Send Notification Emails** to:
   - **No** – No notification emails are sent when malware is found.
   - **To System Notification Email (Default)**– A notification email is sent to the system notification email address. For more information, see How to Configure the System Email Notification Address.
   - **To Explicit Address** – Enter the **Explicit Email Address** and **Explicit SMTP Server** the Barracuda NG Firewall will use to send the notification emails.
8. (optional) Set the **ATD Data Retention** (in days). These values determine how long files are kept on the system before they are deleted.
9. Click **Send Changes** and **Activate**.

Step 2. Enable ATP in the Firewall, Configure Automatic Quarantine Policy and Quarantine for the HTTP Proxy

You must enable ATP in the security policy of the forwarding firewall and enable the quarantine for the HTTP proxy.

1. Open the **Security Policy** page (**Config > Full Config > Virtual Servers > *your virtual server* > Firewall**).
2. Click **Lock**.
3. In the **Advanced Threat Detection** section click **Enable ATD in the firewall**.

4. Select the **Automatic Blacklist Policy**:
   - **No auto quarantining** – No connections are blocked.
   - **User only** – All connections by the infected user are blocked regardless of the source IP address.
   - **User@IP (AND)** – All connections originating from the infected source IP address and the infected user are blocked.
   - **User, IP (OR)** – All connections coming from the infected source IP address and/or the infected user are blocked.
5. Set the checkbox for **Enable Quarantine for HTTP Proxy**.

6. Click **Send Changes** and **Activate**.

Step 3. Create an Automatic Quarantining Access Rule

To block users and/or IP addresses you must create access rules using the **ATD User Quarantine** network object. Place the Deny or Block rules before any other access rules handling traffic for these IP addresses and/or users.

Example Access Rule to Deny Internet access to Infected Users

- **Action** – Select **Deny**.
- **Source** – Select **ATD User Quarantine** network object.
- **Destination** – Select **Any (0.0.0.0/0)** network object.
- **Service** – Select **Any**.

Example Access Rule to Block Access to Quarantines IP address

- **Action** – Select **Deny**.
- **Source** – Select **Any (0.0.0.0/0)** network object.
- **Destination** – Select **ATD User Quarantine** network object.
- **Service** – Select **Any**.

Quarantine Management

Manually Placing a User and/or IP Address in Quarantine

If you are not using automatic quarantine policy, the administrator can also place a user in quarantine manually.

1. Open the **ATD** page (**Firewall > ATD**).
2. Click the **Scanned Files** tab.
3. Double click the malicious file. The **ATD File Details** widow opens.
4. In the **File Download** section select the user in the list.
5. Click **Quarantine**. The **Select Quarantine Policy** window opens.
6. Select the **Quarantine Policy:**
   - **Block only Users** – Place the user in quarantine, but not the source IP address.
   - **Block only IP Addresses** – Place the IP address in quarantine, but not the user.
   - **Block User @ IP (logic AND)** – Place user@IP address in quarantine. Both user and IP address have to match.
   - **Block User, IP (logic OR)** – Place the user and IP address in quarantine. Either user or IP address have to match.
7. Click **OK**.

The user and/or IP address are now in quarantine network object (Click the **Quarantine** tab to verify). Create an access rule using the ATD User Quarantine network object to block connection to and from the infected users and/or IP addresses.

Removing a User and/or IP Address from Quarantine

1. Open the **ATD** page (**Firewall > ATD**).
2. Click the **Quarantine Tab**.
3. Right click the user or IP address you want to remove from quarantine.
4. Click **Remove from Quarantine**.

The user and/or IP address is removed from the quarantine network object.

Download a Scan Report

You can download a short or long version of scan report.

1. Open the **ATD** tab (**Firewall > ATD**).
2. Double click the scanned file.
3. Click **Download Report** and select the report type:
   - **Summery Report**
   - **Full Report**

Figures

1. atd02.png
2. atd_proxy01.png