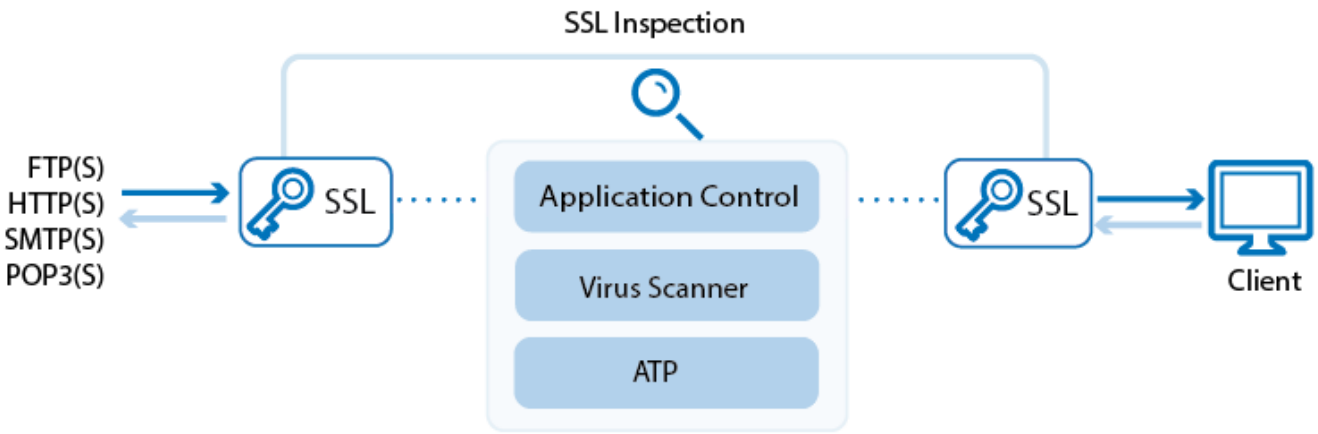
How to Configure ATP in the Firewall

https://campus.barracuda.com/doc/73698002/

Configure when and which types of files are uploaded to the Barracuda ATP Cloud. You can also configure if users will receive files immediately or have to wait until the file analysis is completed to continue with the download. Users who downloaded files with a risk factor higher than the defined risk threshold are placed in quarantine. Create access rules to define what is blocked for the infected users and/or IP addresses.



Before You Begin

- Configure a **System Notification Email** address. For more information, see How to Configure System Email Notifications.
- Enable virus scanning in the firewall for web, mail, and/or FTP traffic. For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic, How to Configure Virus Scanning for Mail Traffic, and How to Configure Virus Scanning in the Firewall for FTP Traffic.
- Verify that all file types you want to scan with ATP for HTTP and SMTP connections are also listed in the scanned MIME types of the Virus Scanner. For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic.

Step 1. Enable ATP in the Firewall and Configure Scan Policies

Enable ATP and configure the ATP scan policies for HTTP, HTTPS, SMTP, SMTPS, POP3, and POP3S connections. Depending on the policy, the user will have to wait for scanning to complete before the file is forwarded. FTP traffic is always scanned with the **Deliver before scan complete** policy.

1. Go to **FIREWALL > Settings**.
2. In the **Advanced Threat Protection** section, enable **Advanced Threat Protection**.
3. Select the **Global Scan Policy**:
   - **Deliver first, then scan** – The user receives the file or email immediately. If malware is

found, the quarantine policy applies.
  - **Scan first, then deliver** – The user is redirected to a scanning page. If no malware is found during the scan, the download starts.
4. Select the **Block Threats** policy:
   - **High only** – Files classified as high risk are blocked.
   - **High and Medium only** – Files classified as high or medium risk are blocked.
   - **High and Medium and Low** – Files classified as high, medium, or low risk are blocked. Only files with classification **None** are allowed.
5. Configure automatic blacklisting for HTTP and HTTPS traffic:
   - From the **Quarantine Policy** drop-down list, select the policy for automatic blacklisting:
     - **No automatic blacklisting** – No connections are blocked.
     - **User** – All connections by the infected user are blocked regardless of the source IP address.
     - **IP** – All connections by the infected source IP address are blocked regardless of the user.
     - **User AND IP** – All connections originating from the infected source IP address and the infected user are blocked. If a different user logs into the infected computer, all connections are allowed because only one criteria, the source IP address, matches. If the username for the connection is unknown, only the IP address is blocked.
     - **User OR IP** – All connections coming from the infected source IP address and/or the infected user are blocked. If a different user logs into the infected computer, all connections are blocked because the source IP is blocked. If the infected user logs into a different workstation, connections are blocked because the infected user is blocked.
6. Click **Save**.

Step 2. Configure Advanced Scan Settings

If needed, set the individual scan policies for each file type:

1. Go to **FIREWALL > Settings**.
2. In the **Advanced Threat Protection** section, select **Show** next to **Advanced Options**.
3. In the **General** section, configure the following settings:
   - **Encrypted Archives handling** – Specify what happens if encrypted archives were detected. Default: **Report only**
   - **Max. Archive size** – Maximum allowed archive size. Default: `1024`. Set to `0` to disable.
   - **Large Archives handling** – Specify what happens if **Max. Archive size** is exceeded. Default: **Report only**
   - **Send Notification E-mails** – **To system settings Address** sends a notification mail for every malicious file found by ATP.
   - **ATP Report Page size** – Select the page format for ATP reports.
4. If needed, set the individual HTTP and HTTPS scan policies for each file type:
   - **Apply Global Policy (default)** – This file type is scanned according to the policy

configured in the basic ATP settings.
- **Do not scan** – The file 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.

5. Click **Save**.

After specifying the ATP settings, click **Save** to save your configuration changes.

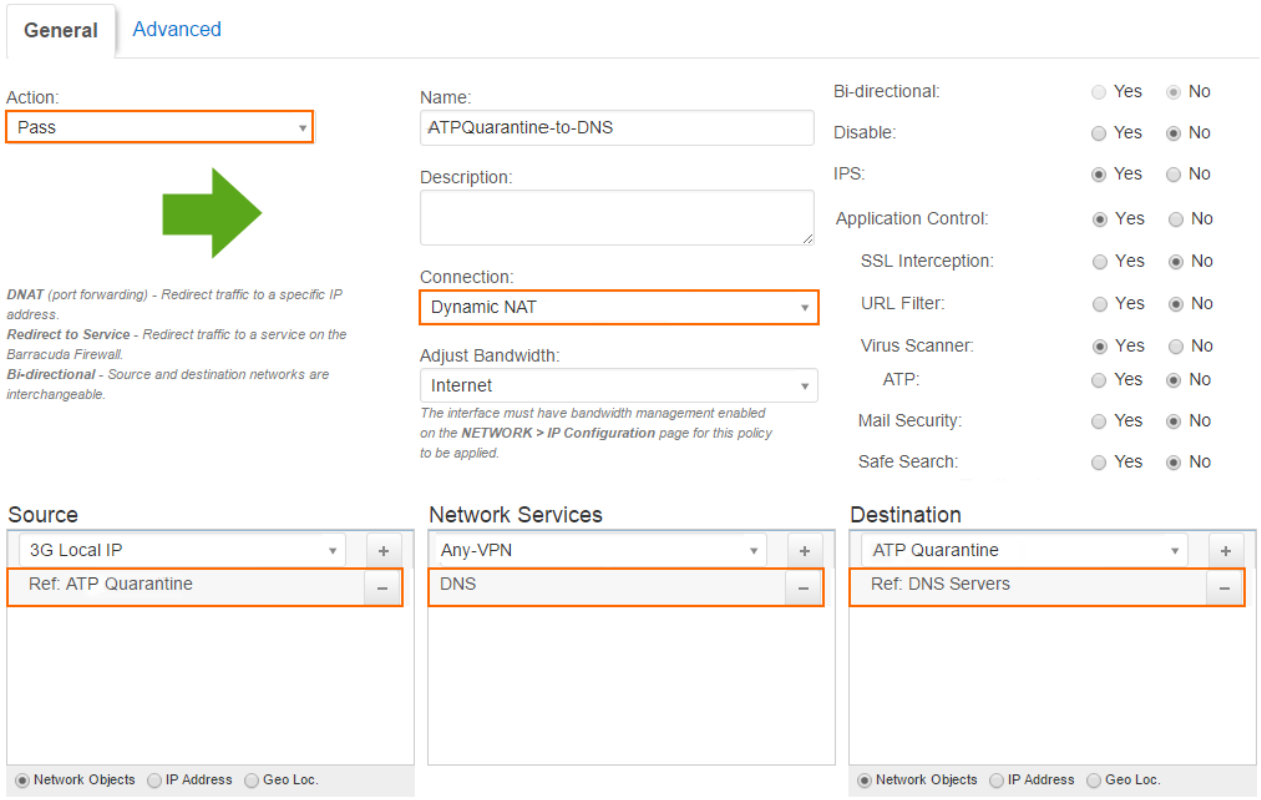
Step 3. Create Two Quarantining Access Rules

To block users and/or IP addresses, you must create access rules using the **ATP User Quarantine** network object. Place the Block rules before any other access rules handling traffic for these IP addresses and/or users. Enable **HTTP Block Page** to redirect HTTP traffic from quarantined users or IP addresses to the custom quarantine block page. You must allow DNS queries from quarantined users to display the HTTP block page. Non-HTTP traffic is simply blocked or denied.

Create a new access rule to allow DNS queries:

1. Go to **FIREWALL > Acces Rules**.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

Action	Connection	Service	Source	Destination
Allow	Select a connection object to allow you to connect to the DNS server.	**DNS**	Select **ATP Quarantine** network object.	Enter the IP addresses of your DNS servers.

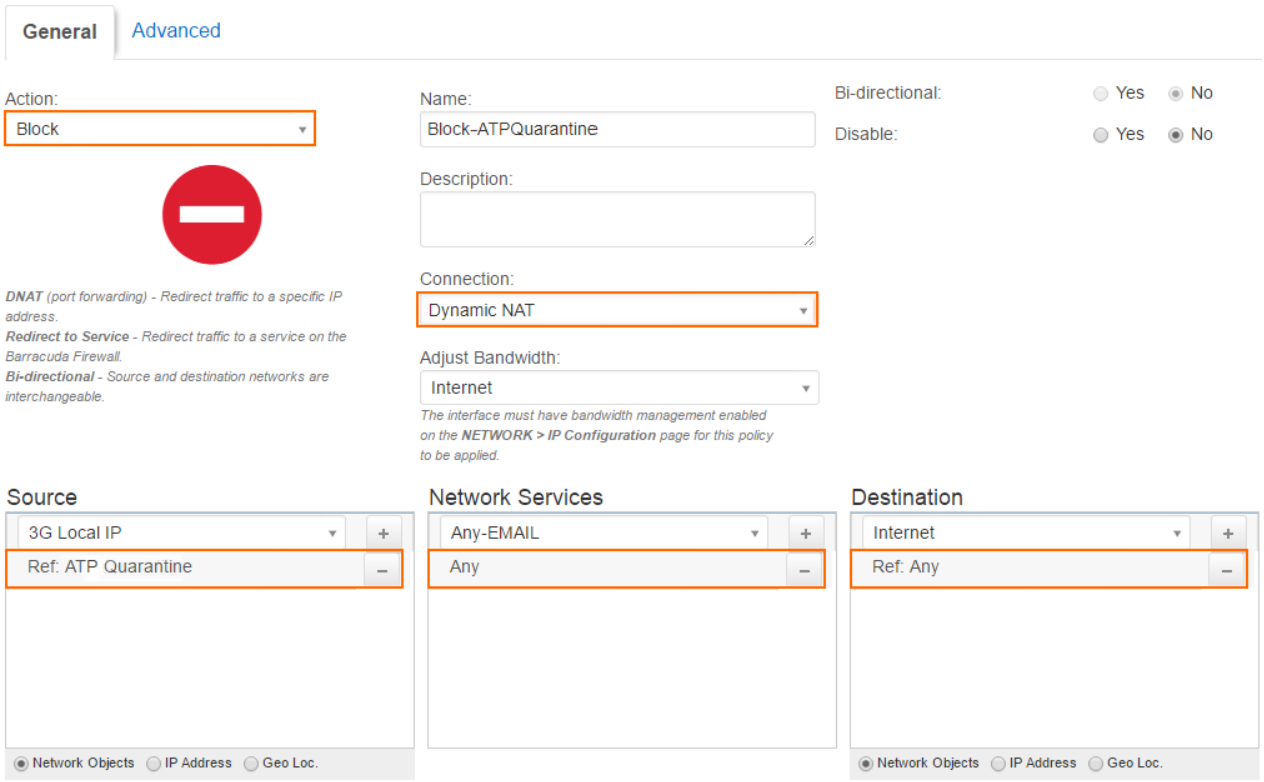


5. Click **Save**.
6. Place the access rule so that no rule before it matches the same traffic.

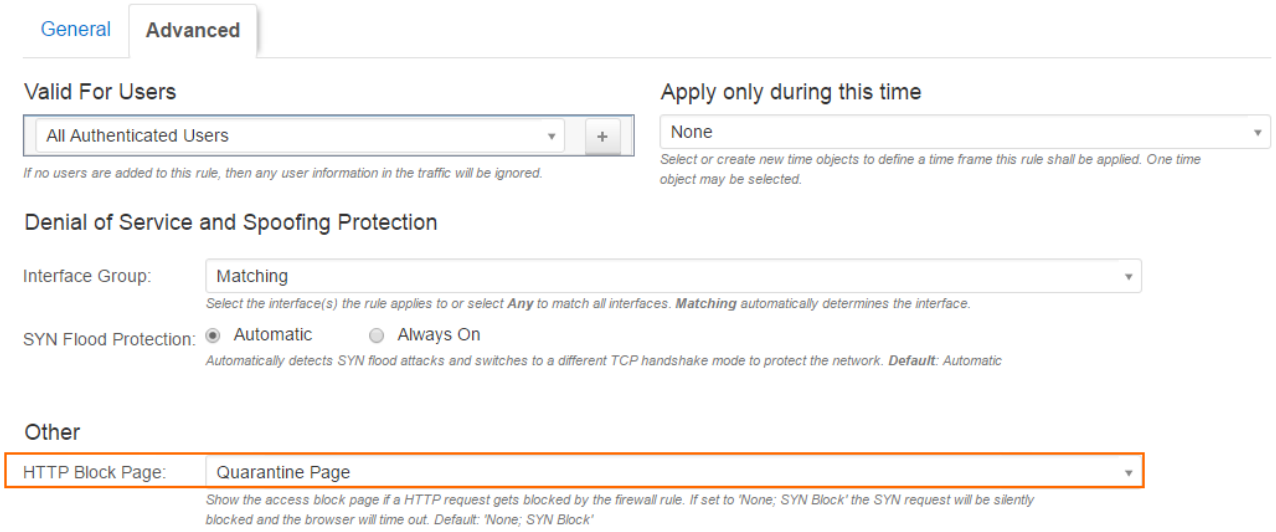
Create a second access rule:

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

Action	Connection	Service	Source	Destination
Block	Select a connection object to allow you to connect to the DNS server.	Select **Any**.	Select **ATP Quarantine** network object.	Select **Any (0.0.0.0/0)** network object.

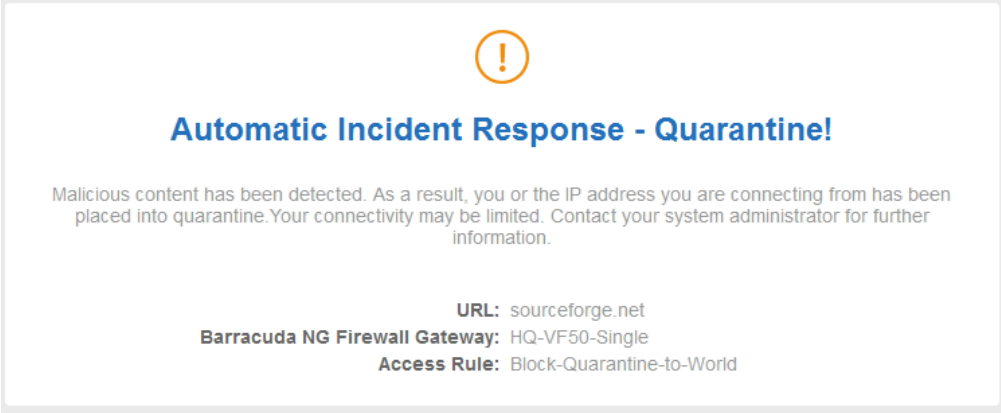


5. In the **Add Access Rule** window, click the **Advanced** tab.
6. In the **Other** section, set **HTTP Block Page** to **Quarantine Page**.



7. Click **Save**.
8. Place the access rule directly below the rule allowing DNS queries from the quarantine so that no rule before it matches the same traffic.

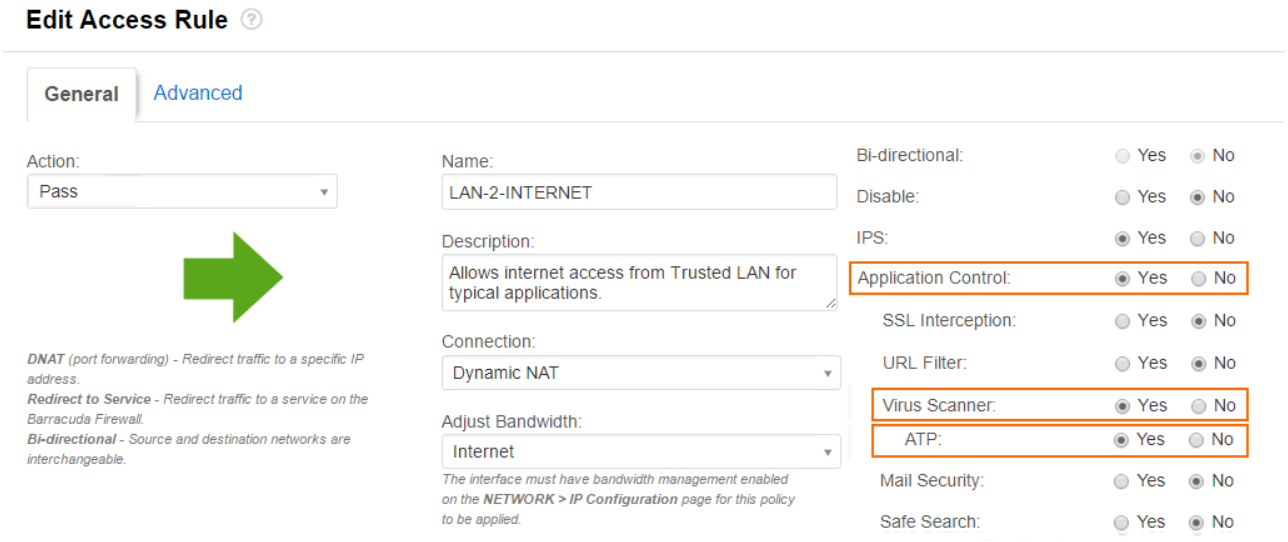
Quarantined users or users connecting via HTTP from quarantined IP addresses are automatically redirected to the customizable quarantine page. For more information, see How to Configure Custom Block Pages and Texts.



Step 4. Edit Access Rules to Use ATP

Enable ATP by editing the access rules handling traffic you want to be scanned. E.g., LAN-2-INTERNET

1. Go to **FIREWALL > Access Rules**.
2. Create or edit an access rule.
3. Edit the access rule handling the traffic you want analyzed by ATP.
4. On the **General** page, select the following options:
   - **Application Control** – required.
   - **SSL Interception** – optional.
   - **Virus Scanner** – required.
   - **ATP** – required.



5. Click **Save**.

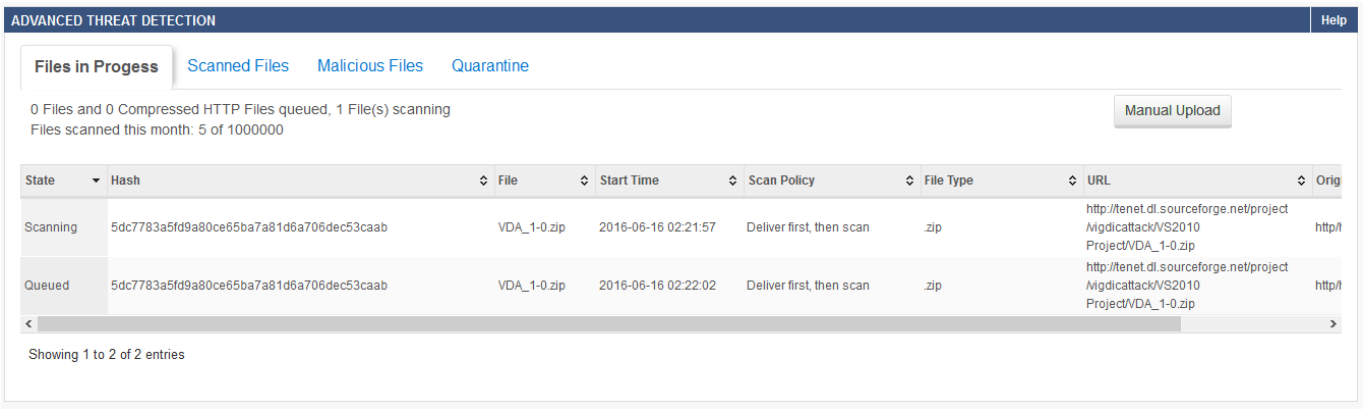
All traffic handled by access rules with **ATP** enabled are now scanned by the ATP service. Blocked files are listed on the **BASIC > Recent Threats** page. To view scan results, go to **BASIC > ATP**.

File Scanning on the ATP Page

The **ATP** page displays results and processes file scanning via Advanced Threat Protection. Use the global filter settings to adjust the amount of displayed files. To access the information on the files scanned by ATP, click the tabs.

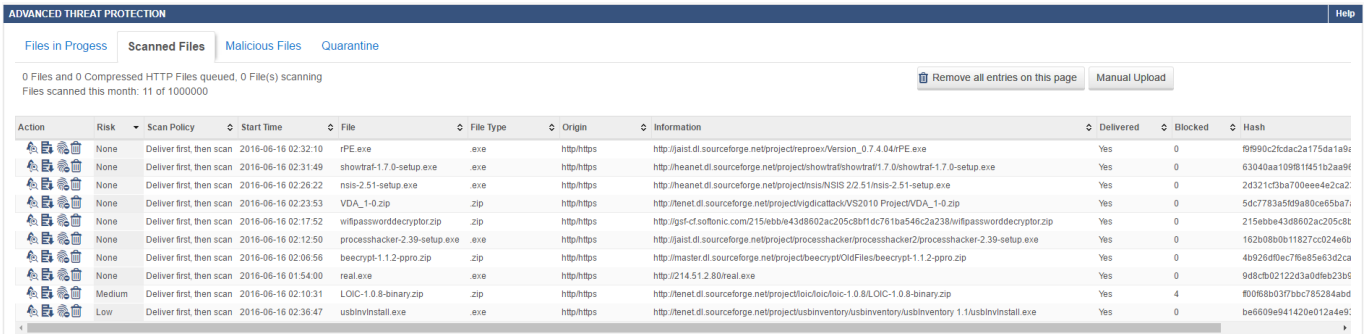
Files in Progress Tab

This tab displays all files that are currently scanned or waiting in the queue. The information displayed on this page is listed in columns. The **State** column shows the ATP scan status.



Scanned Files Tab

Clicking this tab queries the ATP list and displays all files that were scanned by ATP.



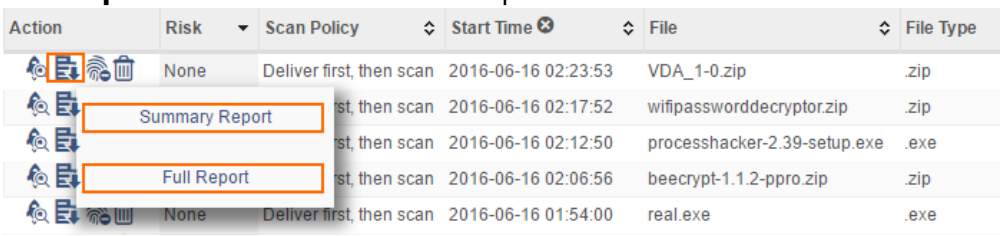
The **Action** column provides a set of icons, offering the following options:

- **Details** – Opens the **ATP File Details** window.
- **Download** – Offers the option to download a scan report.
- **Move to Quarantine** – Moves the file to the **Quarantine** page.
- **Delete Entry** – Deletes the file entry.

Download a Scan Report

Scanned files are displayed on the **Scanned Files** page. You can download a basic or detailed version of the scan report.

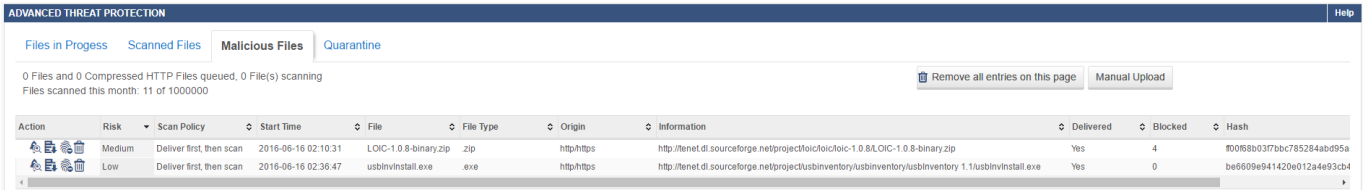
1. Go to **BASIC > ATP**.
2. Select the scanned file.
3. From the **Action** menu, select the **Download Report** icon.
4. Select the report type:
   - **Summary Report** – Download a basic summary report
   - **Full Report** – Download a detailed report



5. Save the report to your desired location.

Malicious Files Tab

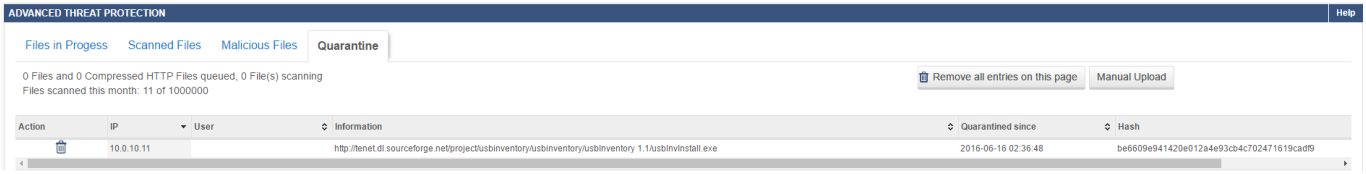
This tab displays all files that were blocked by ATP.



The **Action** column provides the same options as on the **Scanned Files** tab. If you want to remove a file from the list, click the trash can icon and choose the action **Delete Entry** to delete the file entry. To remove all files, select **Remove all entries on this page**.

Quarantine Tab

Displays all files that are quarantined due to the **Quarantine Policy**.



If you want to remove a file from the quarantine, click the trash can icon and choose the action **Remove from Quarantine**. To remove all files from the list, select **Remove all entries on this page**.

Quarantined users and/or IP addresses are also shown on the **BASIC > Status** page.

Manual File Upload

If you want to manually check a local file using ATP, you can upload the file to the ATP Cloud. After the file has been scanned, you are mailed a report with the scan results.

For more information, see How to Manually Upload Files to ATP.

Figures

1. virus_scanning_https_traffic_ATP.png
2. atd_quarantine_01.png
3. atd_quarantine_02.png
4. atd_quarantine_03.png
5. atd_quarantine_block_page.png
6. atd_rule.png
7. atd_fp.png
8. atd_sf.png
9. atd_report.png
10. atd_mf.png
11. atd_qu.png
12. atd_qustat.png