How to Set Threat Policies

https://campus.barracuda.com/doc/73720988/

This article covers how to configure malware prevention policies using the **THREAT POLICY** page. Threat policies are used to specify how you want to handle files determined to be *clean*, *suspicious*, or *malicious*. For details on these terms, what the Malware Prevention feature is, and how it works, see Malware Prevention With Barracuda Content Shield.

> Note that the Malware Prevention feature (MPC) was no longer sold as part of BCS Plus after December 21, 2021. If you purchased your subscription before that date, and if you installed the MPC agent on endpoint machines, then this article applies.

To configure *content filter* policies, see How to Configure DNS Filtering and Policies and How to Configure Advanced Filtering Policies .

Using the Malware Prevention Feature

Malware Prevention can be enabled or disabled at the top of the **THREAT POLICY** page using the **Malware Prevention** toggle. When enabled, threat policies you configure on the page sync with client machines running the Barracuda Content Shield (BCS) agent every 5 minutes, and the file scanner runs on the client machine:

- Whenever the user accesses a file
- Upon installation, performing a full system scan
- Based on the (optional) frequency you configure using the **Schedule Full Scan** setting

> **Important**: The MPC is disabled by default because the endpoint machine may appear to experience some latency while the MPC scanner performs an initial scan on the endpoint drive(s). Knowing this allows the administrator to prepare users for this potential latency when the MPC is first enabled, perhaps enabling the feature during off-peak hours.

If you disable **Malware Prevention** on the **THREAT POLICY** page, threat policies will not be applied on the endpoint machines. The **Status** tab on the BCS agent interface on the clients will show *Content Protection Disabled.* Web content filtering will still apply to web traffic per policy.

Setting Threat Policies by Account

To configure Threat Policies for an account, on the **Accounts** page, click **Manage** for that account,

then do the following:

1. Click **THREAT POLICY** in the left navigation menu.
2. Set **Malware Prevention** to *Enabled*.
3. Schedule regular scans (optional) using the **Schedule Full Scan** feature:
    1. Click **Schedule**, or, if you have previously scheduled a scan, click on the displayed schedule. For example, *Daily at 3:00 PM*.
    2. In the popup, set **Enable Schedule Scan** to *ON*.
    3. Select **Frequency** using the drop-down for *Daily*, *Weekly*, *Bi-Weekly*, or *Monthly*. For *Weekly*, *Bi-Weekly*, or *Monthly*, select the appropriate day or month of the year. Set the time zone in the next drop-down.
    4. Click **Schedule**.
    5. To disable scheduled scans, click the box showing the current schedule. For example, *Daily at 3:00 PM*. In the popup, set **Enable Schedule Scan** to *OFF*. Click **Schedule** to save.

        To run a scan immediately on endpoints, click **RUN NOW**.
4. Under **Scan Policy**, select an **Action for Suspicious Files**:
    - *Quarantine* (Recommended) – Places suspicious files into quarantine for later review. For best protection, set **Action for Suspicious Files** to *Quarantine* so that an administrator can review suspicious files later and decide if the file should be released or deleted from the end user's device. See Quarantine for details.
    - *Allow* – Allows download, but reports on suspicious files detected.
5. Under **File Types**, select file types you want scanned.
6. Under **Encrypted and Password Protected Files**, set *Allow* or *Quarantine* policies.

    Important notes on encrypted and password protected files:
    - The BCS malware scanner may be unable to access a file due to password protection or file encryption. If this option is set to *Allow*, such a file may be downloaded by a user.
    - To ensure the greatest security in dealing with password-protected and encrypted files, Barracuda Networks recommends setting **Encrypted Files** and **Password Protected Files** to **Quarantine**.
    - Encrypted zip archives containing malware are allowed to be copied from a removable drive to another drive on the endpoint, but will be caught by the on-access scanner if/when a user unzips/extracts the files.
7. Under **Removable Drives**, set **Scan Removable Drives** to *YES* to have all removable drives scanned by the service, or *NO* to scan removable drives only when they are accessed. Note that suspicious/malicious files found on removable drives will be *quarantined in place*, rather than moving them off of the removable drive to the Quarantine folder. The user is protected by preventing access to the quarantined files. These files remain intact and can be accessed by a system that is not running BCS Plus.
8. Under **Custom Exclusions**, you can specify either a filename or full path to a file for exclusion from scanning.
    1. Click **+Add Exclusion.**
    2. In the popup, select either *File* or *Path* from the **Exception Type** drop-down.
    3. Enter the value of the filename or path per the example syntax shown in the text box.

To exclude processes (for example, explorer.exe) from scanning, use the EXEMPTION POLICIES page.

Your Threat Policies for this account are now configured. See also Threat Logs.