How to Set Threat Policies

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

Using Malware Prevention

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 Suite 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
- After rebooting, scanning only files that have been touched since the last scan

Threat policies are used to specify how you want to handle files determined to be *clean*, *suspicious*, or *malicious*. A file is *suspicious* if the service was unable to definitively determine a file to be clean or malicious; for example, the service may not be able to access a password-protected or encrypted file, and therefore cannot determine if the file is a real threat. A file is *malicious* if Barracuda Content Shield has scanned the file and has designated that file as a threat that should not be accessed by users. **Malicious files are quarantined by default.**

> If you disable **Malware Prevention** on the **Threat Policy** page, threat policies will not be applied on the client machines. The **Status** tab on the Barracuda Content Shield Suite interface on the clients will show *Content Protection Disabled.* Web content filtering will still apply to web traffic per policy.

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

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.

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. Under **Scan Policy**, select an **Action for Suspicious Files**:
   - *Quarantine* (Recommended) – Places suspicious files into quarantine for later review. See Quarantine for details.
   - *Allow* – Allows download, but reports on suspicious files detected.
3. Under **File Types**, select file types you want scanned.
4. Under **Encrypted and Password Protected Files**, set *Allow* or *Quarantine* policies.

   Barracuda Content Shield tries well-known passwords to attempt scanning password-protected files; however, the service 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 recommends setting **Encrypted Files** and **Password Protected Files** to **Quarantine**.
5. 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. If you set this option to *YES,* you can specify exceptions in the **Custom Exclusions** section, described in the next step.

   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.
6. Finally, under **Custom Exclusions**, click **ADD EXCLUSION** to specify any files, paths, or processes, using the drive letter/path or process/application name, that you want to exclude from scanning. For a process exclusion, enter the executable name (example: explorer.exe) or the full path (C:\Program Files\explorer.exe). To edit or remove an exclusion you created, on the right side of the table, click the More Options icon (⋮) and select the action you want to take.

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

Figures