How to Configure ClamAV Virus Scanning

https://campus.barracuda.com/doc/96026340/

To configure ClamAV virus scanning, you can define settings for the following features:

- Archive Scanning – Define the settings for compressed scanning archives.
- Malware Detection – In addition to viruses, ClamAV can also detect malware, spyware, or bandwidth wasters. Specify which of these threats that the engine should scan for.
- Engine-Specific Options – Specify scanning, phishing detection, and data loss prevention settings for ClamAV.
- HTTP Multimedia Streaming – Because the Virus Scanner service downloads an entire file before scanning and delivering it, some audio or video streams cannot be accessed. To enable content streaming, disable virus scanning for specific DNS domains.

Before You Begin

Before configuring ClamAV virus scanning, activate the Virus Scanner service. For more information, see How to Enable the Virus Scanner.

Configure Archive Scanning

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Assigned Services** > **Virus-Scanner** > **Virus Scanner Settings**.
2. In the left menu, select **ClamAV**.
3. Click **Lock**.
4. Set **Scan Archives** to **yes** to enable the archive scan.
5. In the **ClamAV Archive Scanning** section, define the following archive scanning settings:
    - **Max. Scan Size (MB)** – The maximum amount of data to be scanned for each file. Specifying a maximum size prevents the virus scanner from being overloaded. Archive and other container files are recursively added and scanned up to this value.

      > If a maximum scan size is not entered or the limit set too high, this may result in severe damage to the system.

    - **Max. File Size (MB)** – The maximum size for files to be scanned. Files that exceed this limit will not be scanned. If a limit is not required, enter 0 (zero).
    - **Max. Nesting Depth** – The maximum nesting level for the archives. If a limit is not required, enter 0 (zero).
    - **Max. File Count** – The maximum number of files that can be stored in an archive. If a limit is not required, enter 0 (zero).
    - **Block Encrypted Archives** – To block encrypted archives, select **yes**.

      > If the archive contains file types like.zip,.rar,.exe,.iso,.tar,.tgz,.cab,.msi,.btn, etc., it

> is possible that one of these files is encrypted (virus scanner message: *Encrypted archives are blocked*). In this case, the virus scanner will block the whole archive.
> To disable blocking of encrypted archives, select *no*.

6. In the **ClamAV Possibly Unwanted Applications (PUA)** section, specify the types of malware that the engine should scan for.
7. In the **ClamAV Misc. Scanning Options** section, specify the types of files that should be scanned. You can also enable heuristic and HTML scanning.
8. In the **ClamAV Email Scanning** section, select whether or not to scan URLs found in mails.
9. In the **ClamAV Phishing Protection** section, specify the following settings to detect phishing attacks:
    - **Use Phishing Signatures** – To enable signature based phishing detection, select ***yes***.
    - **Always block SSL Mismatch** – To block SSL mismatches in URLs (even if a URL is not in the database), select ***yes***.
    - **Always Block Cloak** – To block all cloaked URLs (even if a URL is not in the database), select ***yes***.
10. In the **ClamAV Data Loss Prevention (DLP)** section, specify the following settings to detect possible private data theft:
    - **Min. Credit Card Count** – The minimum amount of credit card numbers that can be stored in a file before the file is detected.
    - **SSN Format** – To enable the DLP module to scan for valid social security numbers, select ***yes***.
    - **Min. SSN Count** – The minimum amount of social security numbers that can be stored in a file before the file is detected.
11. Click **Send Changes** and **Activate**.

Configure HTTP Multimedia Streaming

To enable content streaming, disable virus scanning for specific DNS domains.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. In the left menu, select **Content Scanning**.
3. Click **Lock**.
4. In the **Scan Exceptions** table, add an entry for each DNS domain that should not be scanned.
    1. Enter a name for the entry and click **OK**.
    2. In the **Allowed MIME types** table, add an entry for each MIME type that should not be scanned.

        > To determine the MIME type for a file, enable the debug log and check the **cas** log files.
        > To enable the debug log, go the **Virus Scanner Settings - Basic Setup** page. In the **Debug Log Level** field, enter 1.

    3. In the **Domain** field, enter the domain name.
5. Click **Send Changes** and **Activate**.