

How to Enable the Virus Scanner

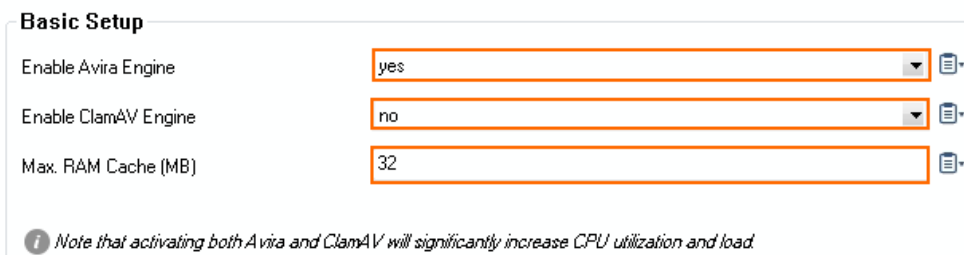
<https://campus.barracuda.com/doc/96026337/>

The Virus Scanner service supports two virus scanning engines: Avira and ClamAV. Although it is possible to use both virus scanning engines, it is not recommended because this can result in high system load. A Malware or Web Security subscription is required. The virus scanner can be integrated with the following services:

- Firewall
- HTTP Proxy
- Mail Gateway
- FTP Proxy

Enable and Configure the Virus Scanner

1. Go to **Configuration > Configuration Tree > Box > Assigned Services > Virus-Scanner > Virus Scanner Settings.**
2. Click **Lock.**
3. Enable the virus engine(s):
 - **Avira** - Set **Enable Avira Engine** to **yes**.
 - **ClamAV** - Set **Enable ClamAV Engine** to **yes**. (To display the ClamAV configuration, expand the **Configuration Mode** menu on the left and select **Switch to Advanced**. If the option is missing, open the Firewall Admin settings and select **Show Expert Settings**. For more information, see [Barracuda Firewall Admin Settings](#).)
 - **Enable ATP Engine - (Advanced Configuration Mode)** Enable this setting to use ATP scanning. For more information, see [Advanced Threat Protection \(ATP\)](#).
4. (optional) Adjust the **Max. RAM Cache (MB)** to your preferences. Files exceeding the cache size are stored on the hard drive. Increase to cache more files in memory and reduce the I/O load on the firewall.



Basic Setup	
Enable Avira Engine	yes
Enable ClamAV Engine	no
Max. RAM Cache (MB)	32

Note that activating both Avira and ClamAV will significantly increase CPU utilization and load.

5. In the left menu, click **Update Handling**.
6. Set **Disable Updates During Working Hours**:
 - **Yes** - The firewall will not perform a virus scanner pattern update during the defined working hours because the virus scanning service does not respond to scan queries while it is re-initialized with new patterns.
 - **No** - Virus scanning patterns are installed immediately after they are available.
7. (optional) Enter **Update Every (mins)** to change the update frequency.

8. To download the updates via a proxy:

- **Proxy Settings** – If the virus scanner requires an HTTP proxy to reach the update servers, configure the parameters in this section.

General Update Settings

Disable Update	no	▼	📄
Disable Update During Working Hours	yes	▼	📄
Working Hours Start	07:00	▼	📄
Working Hours End	19:00	▼	📄
Update Every [mins]	60		📄

Proxy Settings

Connection Method	Like-System-Settings	▼	📄
-------------------	----------------------	---	---

Switch to the advanced view if you need to configure an explicit proxy server.

9. Click **Send Changes** and **Activate**.

Next Steps

- Configure the Avira virus scanning settings. For more information, see [How to Configure Avira Virus Scanning](#).
- Configure the ClamAV virus scanning settings. For more information, see [How to Configure ClamAV Virus Scanning](#).

Figures

1. virus_scanner_00.png
2. virus_scanner_01.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.