How to Update Virus Patterns Manually

https://campus.barracuda.com/doc/79463091/

In the **Virus Scanner - Update Handling** settings, pattern updates are scheduled or disabled according to the **Update Every (min)** and **Disable Update** settings. You can override these settings to manually execute or disable the pattern updates.

For security reasons, manual pattern update execution and disabling are restricted to the administrator's role:

- On stand-alone Barracuda CloudGen Firewalls, access is permitted for the **Manager** and **Security** roles. For more information, see Managing Access for Administrators.
- On Barracuda Firewall Control Centers, access is permitted through the **Virus Scanner Module** section of the admin role settings on the **Administrative Roles** page (**Config** > **Multi-Range** > **Global Settings**).

1. Go to **CONTROL > Server**.
2. To trigger an immediate virus scanner update:
   1. In the **Service Status** section of the window, select and then right-click the virus scanner service.
   2. Select **Update Pattern**.
3. To disable virus scanner pattern updates:
   1. In the **Service Status** section of the window, select and then right-click the virus scanner service.
   2. Select **Disable Pattern Update**.
   3. In the **Disable Virus Scanner Update** window, configure the following settings to specify how long the pattern updates should be disabled:
      - **Disable permanently** – To disable virus pattern updates permanently, select this check box.
      - **hours/minutes/seconds** – To disable virus pattern updates temporarily, specify in these fields how long to disable the updates.

   The **Info** column for the Virus Scanner service is then updated to state how long the pattern updates are disabled.

   When you disable pattern updates, the **Disable Pattern Update** option is renamed as **Enable Pattern Update**. To re-enable the pattern updates, right-click the Virus Scanner service and select **Enable Pattern Update**.

© 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.