

---

## IP Blocking and IP Exemption

<https://campus.barracuda.com/doc/6553643/>

If you are not already in the Barracuda Web Security Service Manager interface, click **Barracuda Web Security Service** at the top of your Barracuda Cloud Control login screen. The Barracuda Web Security Service Manager interface appears. Click the **CONFIGURATION** tab.

Specify IP Blocking and IP Exemption settings by selecting the desired Barracuda Web Security Service Connector on the **Gateway** tab, then selecting the **Policy** tab.

### Configuring IP-based Exemptions

---

If you want to exempt certain clients or sub-networks from all filtering (including spyware filtering), you can select **Add New IP and Port Exemption** and specify the source IP address for those clients under **IP and Port Exemptions**. For example, if you want to exempt an executive's client machine from all filtering, you can do so using the IP address of the client. Similarly, if you want to exempt certain external devices (such as trusted servers outside the protected network) from all filtering, you can specify the destination IP address and specific port under **IP and Port Exemptions**. Be sure to **Enable** your settings before you **Save Changes**.

Exempted IP addresses will bypass the following block filters:

- Content filtering
- IM blocking
- All types of download blocking

When prompted to sync the Barracuda Web Security Service Connector, click **Sync**.

### Configuring IP-based Blocking

---

If you want to block certain clients or sub-networks from all access, you can use the Add New IP and Port Blocking and specify the source IP address for those clients under IP and Port Exemptions. For example, if you want to block traffic from a suspicious client machine or email servers or internal web servers, you can do so using the IP address of the client. Similarly, if you want to block certain external devices, you can specify the destination IP address and specific port under IP and Port Exemptions. Note that when the Barracuda Web Security Service Connector is deployed as a forward proxy, IP block/exempt rules based on request destination are not applied. You can use this page to configure clients or targeted servers to bypass scanning or filtering. To avoid accidentally specifying a broader than intended exemption range, be sure to apply the proper subnet mask. Be sure to **Enable**

your settings before you **Save Changes**.

When prompted to sync the Barracuda Web Security Service Connector, click **Sync**.

© Barracuda Networks Inc., 2019 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.