

## How to Configure Office 365 for Inbound and Outbound Mail

<https://campus.barracuda.com/doc/39822576/>

This article addresses configuring Office 365 with the Barracuda Email Security Gateway as your inbound and/or outbound mail gateway.

**See also:** [Step 3 - Initial Configuration](#)

Office 365 addresses and user interfaces can change, so please refer to Microsoft documentation for details on configuration. To prepare your Barracuda Email Security Gateway deployment to connect with Office 365, see [Prerequisites for your email server environment in Set up connectors to route mail between Office 365 and your own email servers](#).

You can specify the Barracuda Email Security Gateway as an *inbound mail gateway* through which all incoming mail for your domain passes before reaching your Office 365 account. The Barracuda Email Security Gateway filters out spam and viruses, and then passes the mail on to the Office 365 mail servers. Use the **Inbound Configuration** instructions below to configure.

You can likewise specify the Barracuda Email Security Gateway as the *outbound mail gateway* through which all mail is sent from your domain via your Office 365 account to the recipient. As the outbound gateway, the Barracuda Email Security Gateway processes the mail by filtering out spam and viruses and applying any outbound policies (blocking, encrypting, etc.) before final delivery. By using the configuration described in *Outbound Configuration* below, you instruct the Office 365 mail servers to pass all outgoing mail from your domain to the Barracuda Email Security Gateway.

### Inbound Configuration

To restrict all mail sent to your organization to only that which is sent from the Barracuda Email Security Gateway:

1. Create a connector for MS Exchange in Office 365. You will need the IP address of the Barracuda Email Security Gateway. Once you configure the connector, any Internet mail that does not originate from this IP address range will be rejected by Office 365.
2. Optionally add the requirement for TLS encryption. If you do so, then all mail from your partner organization sent from the IP address or address range you specify must be sent using TLS. Any mail that does not meet this restriction will be rejected.

For further details about configuring Office 365 with connectors, see [Set up connectors for secure mail flow with a partner organization](#) in Microsoft documentation.

---

## Outbound Configuration

---

To restrict all mail leaving your organization to only that which is sent from the Barracuda Email Security Gateway:

1. Create a connector for MS Exchange in Office 365 for outbound mail. You will need the IP address of the Barracuda Email Security Gateway. Before you set up a new connector, check any connectors that are already listed here for your organization. For more information, see [Set up connectors to route mail between Office 365 and your own email servers](#) in Microsoft documentation. The outbound mail gateway will be the IP address of the Barracuda Email Security Gateway.
2. Log into the Barracuda Email Security Gateway web interface as **admin**. Go to the **BASIC > Outbound** page and follow instructions under *Simple configuration of outbound relay of mail* to configure outbound mail, or follow the same instructions in [How to Route Outbound Mail from the Barracuda Email Security Gateway](#).

© Barracuda Networks Inc., 2020 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.