

Barracuda Outlook Add-In Overview 6 and Above

<https://campus.barracuda.com/doc/12196995/>

This guide applies to the Barracuda Email Security Gateway 300 and higher, version 6.0 and higher. The Barracuda Outlook Add-in is compatible with:

- Microsoft Outlook 2007 and Outlook 2010, and 2013 32-bit and 64-bit versions.
- Microsoft Outlook 2016 if you are running version 7.1.1.003 or higher. If so, see [Barracuda Outlook Add-In Deployment Guide version 7 and Above](#).

If you are running version 6.0.0.028 or later of the Barracuda Email Security Gateway firmware, you must upgrade your Barracuda Outlook Add-in to version 6.0.21 or later (see the **USERS > User Features** page).

If both per-user quarantine and per-user Bayesian are enabled, the administrator can install an add-in, or choose to allow users to download an add-in, that provides the user with the following tools:

- **Classify messages as *Spam* or *Not Spam*** directly from their MS Outlook client. This classification helps train the user's personal Bayesian database, and results in higher accuracy for the Barracuda Email Security Gateway. Users must have a quarantine account on the Barracuda Email Security Gateway to use the Barracuda Outlook add-in. For information about automatically or manually creating quarantine accounts for users, see [Creating and Managing Accounts](#). Note that all feedback is stored in a per-user Bayesian database on the system. This mechanism prevents users from compromising the global Bayesian database, and results in more specific scoring due to learning about a user's personal mail preferences.
- **Message encryption.** The user can click a button in the MS Outlook client to encrypt the message contents before sending it. Any messages encrypted using the add-in will appear in the Barracuda Email Security Gateway Message Log with a **Reason** of *Outlook Add-In*. Email encryption is performed by the Barracuda Email Encryption Service, the same way encryption is performed when configured on the Barracuda Email Security Gateway. The difference is that, with the add-in installed on the user's machine, their outgoing email can be encrypted inside the network, securing email exchanged among people in the organization. See [Encryption of Outbound Mail](#) for more information about configuring email encryption.
- **Sender whitelisting.** The user can decide who should be on their whitelist.

For instructions on the installation and configuration of the Barracuda Outlook Add-In for the Windows environment, please see the [Barracuda Outlook Add-In Deployment Guide](#).

Getting the Add-In

It is up to the administrator of the Barracuda Email Security Gateway to decide whether or not users should be given access to this add-in. If the admin wishes to provide the add-in, download capability can be activated for the users under the **USERS > User Features** page. Users will then be able to download and install the add-in from a link on the login screen.

If the administrator chooses to only provide the add-in to a small subset of users, the add-in deployment kit can be downloaded from the **USERS > User Features** page in the **Mail Client Plugins** section and distributed to the necessary users. The add-in is downloaded in a zip file containing .msi files, and is available in both 32 and 64-bit versions.

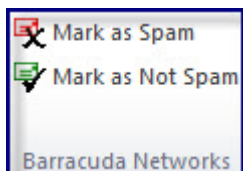
Using the Add-In

Spam / Not Spam Classification

Once installed, the add-in makes itself available to the user through the toolbar inside MS Outlook. Two icons are provided that perform the necessary “Spam” or “Not Spam” classification functionality:

- A red envelope with an “X” in the lower right corner to classify messages as spam.
- A green envelope with a checkmark to classify messages as not-spam.

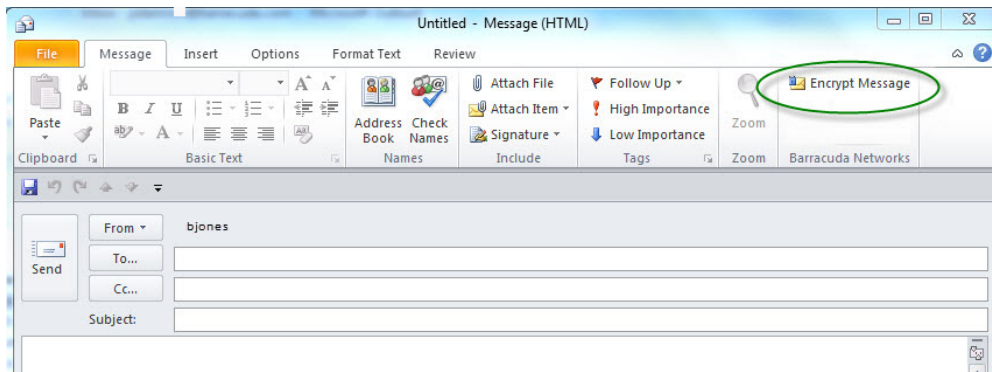
Figure 1: Users can mark messages as Spam or Not Spam using icons in their mail client



Select one or more items from the message window and click on the **Mark as Spam / Mark as Not Spam** icon to submit the messages to the Barracuda Email Security Gateway for classification. For convenience, the toolbar icons are also provided when a mail message is opened in a new window for viewing. If desired, the message can be classified immediately from that window.

Please note that Bayesian learning is only effective when the differences between “Spam” and “Not Spam” are known to the system. Therefore it is important to make sure that both types of messages are classified from user desktops. This add-in is designed to make that classification process as easy as possible. However, it is up to each user to make sure the items they classify from the add-in are really considered spam or not spam as it will affect the scoring of future messages coming onto the system for them.

Figure 2: Users can encrypt a message



Encryption

With the Barracuda Email Security Gateway 5.1 or later, when the user opens the New Message window in Microsoft Outlook, the **Encrypt Message** icon will appear within the window as shown in Figure 2, providing the option to encrypt the message contents before sending it. When the user sends an encrypted message using the Barracuda Outlook Add-In, the recipient will receive a notification email from the Barracuda Message Center that includes a link the recipient can click to retrieve their message. The Barracuda Message Center provides a web client much like any web mail client that the recipient can log into to view and manage encrypted messages. Note that the **Encrypt Message** icon can be disabled through GPO.

For more information about the Barracuda Email Encryption Service, see [Encryption of Outbound Mail](#).

TLS Secure Transmission

The Barracuda Outlook Add-In supports TLSv1.1 and TLSv1.2.

Figures

1. SPamNotSpamIcons.jpg
2. EncryptAddIn.jpg

© 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.