# Whitelist in Barracuda

If you're utilizing Barracuda's Email Security Gateway, you can whitelist CyTech to allow our simulated phishing test emails and training notifications through to your end-users.

The instructions below are for a third-party software. If you run into issues whitelisting CyTech in Barracuda, we recommend reaching out to Barracuda for specific instructions. You can also contact our support team whenever you need assistance.

## Whitelisting by IP in Barracuda in Email Security Gateway

These instructions were gathered and summarized–based on Barracuda's knowledgebase. For more information on how to whitelist in Barracuda, check out the Barracuda Email Security Service - Configuring Inbound Email video.

**If you are using Barracuda's Email Security Service (cloud), follow these steps to whitelist Barracuda by IP address:**

1. Log in to your Barracuda Cloud Control.
2. Go to **Email Security** > **Inbound Settings** > **IP Address Policies**.
3. In the **IP Blocking / Exemption** section, use the top line to enter one of our IP addresses. This process will need to be repeated for each IP address. **Note:** Contact CyTech for the list of IPs.
4. In the Netmask field, type *255.255.255.255*. **Note:** Barracuda does not allow for IP address ranges, so the first IP range should be 147.160.167.0 with a netmask of 255.255.255.192. Entering the IP range this way will cover the entire range. The single addresses will have a netmask of 255.255.255.255.
5. Set the **Policy** field to **Exempt**.
6. If you'd like, add a note in the **Comment** field. For example, CyTech Simulated Phishing IP Address.
7. Click **Add** to whitelist the IP address.
8. Repeat steps 2 through 7 for each of the CyTech IP addresses.

**If you are using Barracuda's Email Security Gateway (on-premises), follow these steps to whitelist Barracuda by IP address:**

1. Log in to your Barracuda Email Security Gateway web interface.
2. Go to the **BLOCK/ACCEPT > IP Filters** page.

3. In the **Allowed IP/Range** section, use the top line to enter one of our IP addresses. This process will need to be repeated for each IP address. **Note:** Contact CyTech for the list of IPs.
4. In the Netmask field, type *255.255.255.255*.

**Note:** Barracuda does not allow for IP address ranges, so the first IP range should be 147.160.167.0 with a netmask of 255.255.255.192. Entering the IP range this way will cover the entire range. The single addresses will have a netmask of 255.255.255.255.

1. Set the **Policy** field to **Exempt**.
2. If you'd like, add a note in the **Comment** field. For example, CyTech *Simulated Phishing IP Address*.
3. Click **Add** to whitelist the IP address.
4. Repeat steps 2 through 7 for each of the CyTech IP addresses.

# Barracuda Intent Analysis

You may need to whitelist us in Barracuda's Intent Analysis feature to prevent the URLs in simulated phishing tests from being altered and potentially resulting in skewed phishing test results. See the Intent Analysis - Inbound Mail article from Barracuda explaining this process.

**If you are using Barracuda's Email Security Service (cloud), follow these steps to whitelist Barracuda's Intent Analysis:**

1. Log in to your Barracuda Cloud Control.
2. Navigate to **Email Security** > **Inbound Settings** > **Anti-Phishing.**
3. Under the **Intent** section, add CyTech's hostnames. Make sure the **Policy** drop-down menu is set to **Ignore**.

**If you are using Barracuda's Email Security Gateway (on-premises), follow these steps to whitelist Barracuda's Intent Analysis:**

1. Log in to your Barracuda Email Security Gateway web interface.
2. Navigate to **Email Security Gateway** > **Basic** > **Spam Checking**.
3. Under the **Intent Analysis** section, add CyTech's hostnames to the **URI Exemptions**: text box field.

# Barracuda Sender Authentication

If you'd like to spoof your own domain in simulated phishing tests, you can exempt Trusted Forwarder IP addresses from SPF checks. See the How to Configure Sender Policy Framework article from Barracuda for more information.

**If you are using Barracuda's Email Security Service (cloud), follow these steps to whitelist Barracuda's Sender Authentication:**

1. Log in to your Barracuda Cloud Control.
2. Navigate to **Email Security** > **Inbound Settings** > **Sender Authentication.**
3. In the Use Sender Policy Framework center enter our IP addresses in the SPF exemptions table.

**If you are using Barracuda's Email Security Gateway (on-premises), follow these steps to whitelist Barracuda's Sender Authentication:**

1. Log in to your Barracuda Email Security Gateway web interface.
2. Navigate to **Email Security** > **Block/Accept** tab and select Sender Authentication.
3. Under **Sender Policy Framework (SPF) Configuration** section, select **Yes**.
4. Add the CyTech IP addresses to the exemption list.

**Note:** After following this article, we recommend setting up a test phishing campaign for 1-2 users to ensure your whitelisting was successful. As a last resource, we suggest reaching out to your service provider for assistance.

## Barracuda Advanced Threat Protection (ATP)

If you are using Barracuda's Advanced Threat Protection (ATP) and have experienced false clicks or false attachment opens, you can set up exemptions. Setting up exemptions allows you to bypass PDF scanning for phishing test emails from CyTech's IP addresses.

To set up exemption addresses to bypass **ATP PDF Scanning:**

1. Log in to your Barracuda Email Security Gateway web interface.
2. Select the **ATP Settings** tab.
3. Enter the IP address(es) and Subnet Mask(s). **Note:** Contact CyTech for the list of IPs.
4. Click **Add**.

## Barracuda Sentinel Allow Senders

Using Barracuda Sentinel’s **Allow Senders** list allows CyTech emails to bypass your organization’s current whitelisting rules. See Barracuda’s How to Allow Senders article for more information.

**To add specific senders to your Allow Senders list:**

1. Log in to your Barracuda admin console.
2. Click **Dashboard** in your console menu.
3. Click the **Settings** icon, which should appear as a gear.
4. Click **Allowed Senders**.

5. Enter one email address or domain name into the **Sender Email or Domain** field.

**Note:** Barracuda Sentinel will only allow you to enter one email address or domain name at a time for security reasons. You can repeat steps 5 through 7 for as many email addresses or domains you wish to add.

1. You can add a comment to your email address or domain name if you wish.
2. Click **Save**.

You can also delete or edit the email addresses and domain names from the **Allowed Senders** page using their respective icons.

*If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.*

---

Revision #1
Created 5 December 2024 07:52:40 by David Napoleon Romanillos
Updated 5 December 2024 08:12:47 by David Napoleon Romanillos