Whitelist in Mimecast

If you're using Mimecast's services, you can whitelist CyTech to allow our simulated phishing test emails and training notifications through to your end users.

Below you'll find instructions for several different policies you'll need to add to your Mimecast console to allow the use of CyTech's various services. The policies below are in a suggested order for the highest probability of success for your phishing security tests.

Each Mimecast policy section has a description of the policy's purpose regarding CyTech's phishing security test features.

If you run into issues whitelisting CyTech in your Mimecast services, we recommend reaching out to Mimecast for specific instructions. You can also contact our Support team whenever you need assistance.

Anti-Spoofing Policy

Follow the steps below to allow CyTech to send emails appearing to come from an email address at your domain, on your behalf.

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **Anti-Spoofing** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings, see Mimecast's Configuring an Anti-Spoofing Policy article.
7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter our IP ranges. **Note:** Contact CyTech for the list of IPs.

Image not found or type unknown

Be sure to save the policy. This should allow the simulated phishing templates appearing to come from your organization's domain, to successfully reach your users' inboxes. We suggest setting up a test campaign to yourself or a small group of people to ensure the policy works as intended, before sending a campaign to all of your users.

Permitted Senders Policy

To successfully whitelist our phishing and training-related emails when using Mimecast, you should Create a new Permitted Sender policy to allow our phishing and training-related emails through to your users' inbox.

Important: Do not edit your default Permitted Sender policy. A new one must be created.

Follow the steps below to allow CyTech emails to arrive successfully in your users' inboxes.

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **Permitted Senders** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings see Mimecast's Configuring a Permitted Senders Policy article.
7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter the appropriate IP ranges for your CyTech account's location.

Note: Contact CyTech for the list of IPs.

Image not found or type unknown

Be sure to save the policy. We suggest setting up a test campaign to yourself or a small group of people to ensure the policy works as intended, before sending a campaign to all of your users.

Attachment Protection Bypass Policy

If you'd like to use attachments in your simulated phishing tests, follow the steps below to increase the likelihood that emails with attachments from CyTech will successfully arrive in your users' inboxes. Mimecast may still prevent the delivery of attachments. Set up a test after creating this policy to ensure your desired attachment goes through.

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **Attachment Protection Bypass** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings, see Mimecast's Configuring Attachment Protection Bypass Policies article.

7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter the appropriate IP ranges for your CyTech account's location.

Note: Contact CyTech for the list of IPs.

Image not found or type unknown

Be sure to save this new policy. After allowing time for this new rule to propagate, we recommend setting up a phishing campaign to yourself, or a small group to test out the various attachment types.

URL Protection Bypass Policy

Mimecast's URL Protection service scans and checks links in emails upon delivery. This can sometimes result in false positives for your phishing security tests. Follow the steps below to create a URL Protection Bypass policy for accurate phishing security test results.

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **URL Protection Bypass** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings, see Mimecast's Configuring a URL Protection Bypass Policy article.
7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter the appropriate IP ranges for your CyTech account's location.

Note: Contact CyTech for the list of IPs.

Image not found or type unknown

Be sure to save the policy. We suggest setting up a test campaign to yourself or a small group of people to ensure the policy works as intended, before sending a campaign to all of your users.

Impersonation Protection Bypass Policy

If you’re sending whaling/phishing emails purporting to come from users/domains that look like they are internal to your organization, you'll want to create an Impersonation Protection Policy in your Mimecast console.

Impersonation Protection Bypass Policy

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **Impersonation Protection Bypass** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings, see Mimecast's Configuring an Impersonation Protection Bypass Policy article. **Note:** In the **Select Option** field under **Options**, select the impersonation protection definition you want to be bypassed. If you have multiple definitions you would like to bypass, you will need to create a separate Impersonation Protection Bypass Policy for each one.
7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter the appropriate IP ranges for your CyTech account's location.

Note: Contact CyTech for the list of IPs.

Image not found or type unknown

Be sure to save the policy. We suggest setting up a test campaign to yourself or a small group of people to ensure the policy works as intended, before sending a campaign to all of your users.

Attachment Management Bypass Policy

If you'd like to use attachments in your simulated phishing tests, follow the steps below to prevent attachments from being stripped from emails, potentially resulting in skewed test results.

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **Attachment Management Bypass** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings, see Mimecast's Configuring Attachment Management Bypass Policies article.
7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter the appropriate IP ranges for your CyTech account's location.

Note: Contact CyTech for the list of IPs.

Image not found or type unknown

Be sure to save the policy. We suggest setting up a test campaign to yourself or a small group of people to ensure the policy works as intended, before sending a campaign to all of your users.

Greylisting Bypass Policy

You may want to set up this policy if want to prevent Mimecast from preventing emails from being deferred. Below are instructions on how to add this policy.

1. Log in to your Mimecast Administration Console.
2. Click the **Administration toolbar** button.
3. Select the **Gateway | Policies** menu item.
4. Select **Greylisting** from the list of policies displayed.
5. Select the **New Policy** button.
6. Select the appropriate policy settings under the **Options**, **Emails From**, **Emails To**, and **Validity** sections. For more information on these settings, see Mimecast's Configuring Greylisting Policies article.
7. Select the **Policy Override** check box.
8. In the **Source IP Ranges** field (shown below), enter the appropriate IP ranges for your CyTech account's location. **Note:** Contact CyTech for the list of IPs.
9. Click **Save and Exit** to save the changes.

Image not found or type unknown

Preventing Mimecast from Re-Writing Phishing Links

If you'd like to prevent Mimecast from re-writing the links in the Phishing tests you send, you can do so by adding CyTech's phish link domains as Permitted URLs in Mimecast. You can find a list of our phish link domains in the **Phishing** tab of your KSAT console under **Domains**. Our support team can provide a list of our phish link domains.

Keep in mind, we don't recommend creating an exception for this unless you also have exceptions for other senders already in place. Otherwise, seeing ***anything*** other than a rewritten Mimecast URL will be a red flag for users and may skew your results.

For more information on disabling link rewriting on permitted URLs, see Mimecast's Targeted Threat Protection: Managed URLs article.

DNS Authentication Bypass Policy (Optional)

If you are having issues with our emails being sent to your spam folder or being quarantined, you may want to set up this additional policy. First, you'll need to set up the inbound definition and then you can create the policy. Below are instructions on how to add this policy.

DNS Authentication - Inbound Definition Setup

1. Log in to your Mimecast Administration Console.
2. Select the **Gateway | Policies** menu item.
3. Click the **Definitions** drop-down menu and select the **DNS Authentication - Inbound** option.
4. Select **New DNS Authentication - Inbound Checks**.
5. Create a name for the definition and leave all options unchecked.
6. Click **Save and Exit** to save your changes.

DNS Authentication - Inbound Policy Setup

1. Log in to your Mimecast Administration Console.
2. Select the **Gateway | Policies** menu item.
3. Click the **DNS Authentication - Inbound** policy.
4. Select **New Policy**.
5. Specify the following settings listed in the image below:Image not found or type unknown
6. Enter the CyTech IP ranges into the **Source IP ranges** field.
7. Check the **Policy Override** option.
8. Click **Save and Exit** to save the changes.

CyberGraph Policy (Optional)

If you’re having issues with Mimecast removing CyTech’s email trackers, you can set up this policy. Mimecast’s CyberGraph Policy will prevent email trackers from being removed. To set up the CyberGraph policy, follow the steps below:

1. Log in to your Mimecast Administration console.
2. Navigate to **Services** > **CyberGraph**.
3. Click **Create New Policy**.
4. Enter a Name for the policy, such as “CyTech CyberGraph Policy”.
5. (Optional) Enter a **Description** for the policy.
6. In the **Dynamic Banners** field, select **Disabled**.
7. In the **Trackers** field, select **Disabled**.
8. In the **User Reporting** field, select **Disabled**.
9. Click **Next**.
10. In the **Applies To** section, set the **From** field to **Everyone**. Then, set the **To** field to **Everyone**.

11. In the **Source IP Ranges** field, enter CyTech’s IP addresses. **Note:** Contact CyTech for the list of IPs.
12. Click **Next**. You’ll be taken to the **Summary** page to confirm your settings are correct.
13. In the **Policy Status** field, click **Enabled**.
14. Click **Create New Policy**.

Image not found or type unknown

Troubleshooting

Note: After following the steps in this article, we recommend that you set up a test phishing campaign containing one or two users to make sure your whitelisting was successful.

If your whitelisting was unsuccessful, we recommend that you reach out to Mimecast for additional help.

If you're experiencing issues with false positives and the **Journaling** feature is enabled for your Mimecast account, you may need to add our phishing domains to your **Managed URLs.** For more information, see Mimecast's Targeted Threat Protection: Managed URLs article. For a list of our phishing domains, please contact our support team.

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

Revision #1
Created 5 December 2024 08:48:14 by David Napoleon Romanillos
Updated 5 December 2024 08:55:59 by David Napoleon Romanillos