

Whitelist in Trend Micro

If you're utilizing Trend Micro's services, you can whitelist CyTech to allow our simulated phishing test emails and training notifications through to your end users. If you run into issues whitelisting CyTech in your Trend Micro services, we recommend reaching out to Trend Micro for specific instructions. You can also contact our Support team whenever you need assistance.

Whitelisting by Domain in Trend Micro

The whitelisting process is broken down into 5 sections. Each section has its own steps for configuration and must be completed to successfully whitelist CyTech.

Note: If you are experiencing false positives, you can try to resolve the issue by whitelisting our phish link domains and our landing page domains.

Advanced Spam Protection

1. Navigate to the **Advanced Threat Protection** tab > **Add**.
 2. Select the policy to create based on the service:
 - Exchange
 - OneDrive
 - SharePoint
 - Box
 - Dropbox
 - Google
 3. On the left, select **Advanced Spam Protection**.
 4. Check the **Enable Advanced Spam Protection** option.
 5. Select the **Approved/Blocked Sender List** section.
 6. Check the box next to the **Enable the approved sender list** option.
 7. Enter ***@CyTech.com** in the text field and click the **Add >** button.
Image not found or type unknown
 8. Select the **Rules** configuration section.
 9. Under the **Apply to:** drop-down menu, select the **Incoming messages** option.
 10. For Detection **Level:**, select the **Medium** option.
Image not found or type unknown
-

Malware Scanning

11. On the left, select **Malware Scanning**.

12. Select the **Rules** configuration section.
 13. Under the **Apply to:** drop-down menu, select the **All messages** option.
 14. Under **Malware Scanning**, select **Scan all files** and check the box next to **Scan message body** and **Enable IntelliTrap**.
Image not found or type unknown
 15. Select the **Action** configuration section.
 16. For **Action:**, select the **Trend Micro recommend actions** option from the drop-down menu.
 17. For **Notification:**, select the **Notify** option from the drop-down menu.
Image not found or type unknown
-

File Blocking

18. On the left, select **File Blocking** and select Enable File Blocking. We recommend keeping File Blocking on because you cannot limit this option to CyTech messages. Turning off File Blocking could allow potentially malicious attachments through to your users.
Image not found or type unknown
-

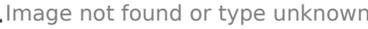
Web Reputation

19. On the left, select **Web Reputation**.
20. Check the **Enable Web Reputation** option.
21. Select the **Rules** configuration section.
22. Under the **Apply to:** drop-down menu, select the **All messages** option.
23. For **Security Level:**, select the **Medium** option.
Image not found or type unknown
24. Select the **Approved/Blocked URL List** section.
25. Check the box next to the **Enable the approved URL list** option.
26. Check the box next to the **Add internal domains to the approved URL list** option.
27. Enter the phish link root domains enabled in your KSAT console.
28. Then, click the **Add >** button. **Note:** You can click the **Import** button to import URLs in batches.

Image not found or type unknown

Virtual Analyzer

29. On the left, select **Virtual Analyzer**.
30. Check the **Enable Virtual Analyzer** option.
31. Click the **Save** button.
Image not found or type unknown

Once all steps in each section are completed, your new policy will appear under the **Advanced Threat Protection** tab.

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

Whitelisting by Email Header in Trend Micro Security

To whitelist by email header in Trend Micro Cloud App Security (CAS), follow the steps below.

1. Log in to your KSAT console.
2. Click the email address in the top-right corner of the page, then select **Account Settings**.
3. Navigate to **Phishing > Phishing Settings**.
4. Under **Phishing Email Headers**, select the **Enable PST Header Token** check box.
5. Copy your unique **PST Token** and save it somewhere you can easily access.
6. In a separate window, log in to your Trend Micro CAS account.
7. Navigate to **ATP Policy | Exchange Online > Web Reputation**.
8. In the **Approved Header Field List** section, select the **Enable the approved header field list** check box.
9. In the **Name** field, enter "X-CYTECHTOKEN".
10. In the **Value** field, paste your PST Token that you copied earlier.
11. Click **Add >**.
12. Click **Save**.

Whitelisting Trend Micro Hosted Email Security

Trend Micro Hosted Email Security does not allow emails from non-registered domains regardless of whether or not they were added to the Allowed Senders list. For more information, see the [Blocked message details](#) article from Trend Micro.

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

Revision #1

Created 5 December 2024 09:26:20 by David Napoleon Romanillos

Updated 5 December 2024 09:41:45 by David Napoleon Romanillos