

# Block or allow inbound email



Owned by Former user (Deleted) ...

Last updated: May 15, 2024 by James Fernandez • 3 min read • 14 people viewed

Use the procedures below to create policies that block or allow inbound email. Policies can be made for individual email addresses, entire domains, IP ranges, or specific message content. Start by logging into [Barracuda](#) with the credentials found in Keeper.

Procedures:

[By email address or domain](#)

[By IP address/range](#)

[By message content](#)

[Domain-level policies](#)

## By email address or domain

✗ NEVER whitelist a client's own domain name. Spoofing a client's domain is a common phishing tactic.

⚠ Do not allow OR block generic public domains such as *gmail.com* or *yahoo.com*.

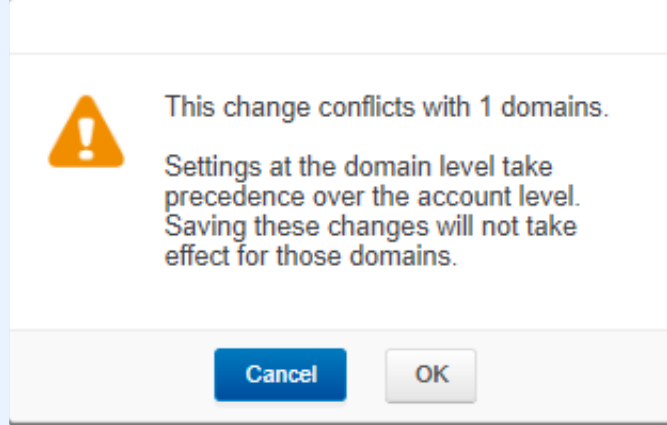
1. Click **Email Gateway Defense** on the left, then select the client from the drop-down at the top
2. Click **Inbound Settings** > **Sender Policies**
  - a. These are "account-level" policies and are meant to apply to all the client's domains (see the [Domain-level policies](#) section below)
3. Enter the sender's email address or domain (e.g., *fiserv.com*)
  - a. Do not use wildcards! Asterisks are not supported. Barracuda will treat domains with an implied wildcard (e.g., entering *domain.com* is the same as entering *\*@domain.com*)
  - b. If you're creating a policy for a subdomain, create a policy for the main domain as well (e.g., *training.knowbe4.com* & *knowbe4.com*)
4. Select **Block** to block, or **Exempt** to allow ("exempt" from spam scoring, intent analysis, content filters, and SPF checks)
5. Enter your ticket number in the comment

### 6. Click **Add**



Did you receive this warning?

This means the account-level policy you just created will not apply to domains that have their own domain-level policies. You will have to proceed with the [domain-level policies](#) section to create the same policy for those domains explicitly.



This change conflicts with <#> domains.

## By IP address/range

**i** Try to avoid blocking entire ranges of IP addresses. Legitimate senders can sometimes fall into a given range.

1. Click **Email Gateway Defense** on the left, then select the client from the drop-down at the top
2. Click **Inbound Settings > IP Address Policies**
  - a. These are "account-level" policies and are meant to apply to all the client's domains (see the [Domain-level policies](#) section below)
3. Enter the IP address and subnet mask. A mask of 255.255.255.255 indicates a single IP address
  - a. If you need to convert from CIDR notation, use a subnet calculator like [IP Address Guide](#)
4. Select **Block** to block, or **Exempt** to allow ("exempt" from spam scoring and all other block lists)
5. Enter your ticket number/short description and click **Add**

### **≡** Best Practice

If you exempt a sender's (such as KnowBe4's) IP range, you will also need to exempt their domain.

## By message content

**i** Create content policies to allow or deny emails based on the content of the subject, headers, body, attachments, or sender/recipient address.


**⚠** These are [Regular Expressions](#) which could potentially have major unintended consequences if written incorrectly. Use a tester like [RegEx 101](#) to validate your expressions and avoid adding these policies if you're not confident in what you're doing.

1. Click **Email Gateway Defense** on the left, then select the client from the drop-down at the top
2. Click **Inbound Settings > Content Policies**
  - a. These are "account-level" policies and are meant to apply to all the client's domains (see the [Domain-level policies](#) section below)

3. Add your expression in the Message Content Filter section of the page
4. Select **Block** to block, **Allow** to allow, or **Quarantine** to have the user decide
5. Select whether to find pattern matches in the subject, headers, body, attachments, or sender/recipient addresses, then click **Add**

## Domain-level policies






Generally, an account-level policy will apply to all of a client's domains. Domains with flag icons, however, have their own policies which **override** the account-level policies. Once you've added a domain-level policy, the domain will become flagged and you will have to manage its policies in addition to the account-level policies going forward.

	Settings	Domain Options	
cti...	<a href="#">Edit</a>	<a href="#">Manage</a>	<a href="#">Remove</a>
ma...	<a href="#">Edit</a>	 <a href="#">Manage</a>	<a href="#">Remove</a>
tail...	<a href="#">Edit</a>	<a href="#">Manage</a>	<a href="#">Remove</a>

A "flagged" domain with it's own policies

1. Click **Email Gateway Defense** on the left, then select the client from the drop-down at the top
2. Click **Domains** to look for any "flagged" domains
3. Click **Manage** to enter the configuration for the flagged domain
4. Click the **Inbound Settings** tab
5. Follow the guidance above to add your Sender Policies/IP Address Policies/Content Policies specific to this domain
6. Click **Return to domain management** to repeat for any additional flagged domains

### Related articles

-  [Block or allow inbound email](#)
-  [Convert on-prem AD-synced user to cloud-only](#)
-  [O365 Compromised Account](#)
-  [Whitelist YouTube](#)
-  [Whitelist Facebook](#)

barracudas spam x barracuda x whitelist x email x filter x spam x spamfilter x kb-how-to-article x

+ Add label