Exempt IP or Email Addresses from the ESA Bounce Configuration

Contents

[Introduction](#)

[Exempt IP Addresses/Domains/Email Addresses from ESA Bounce Configuration](#)

[Outbound Mail](#)

[Inbound Mail](#)

[Related Information](#)

Introduction

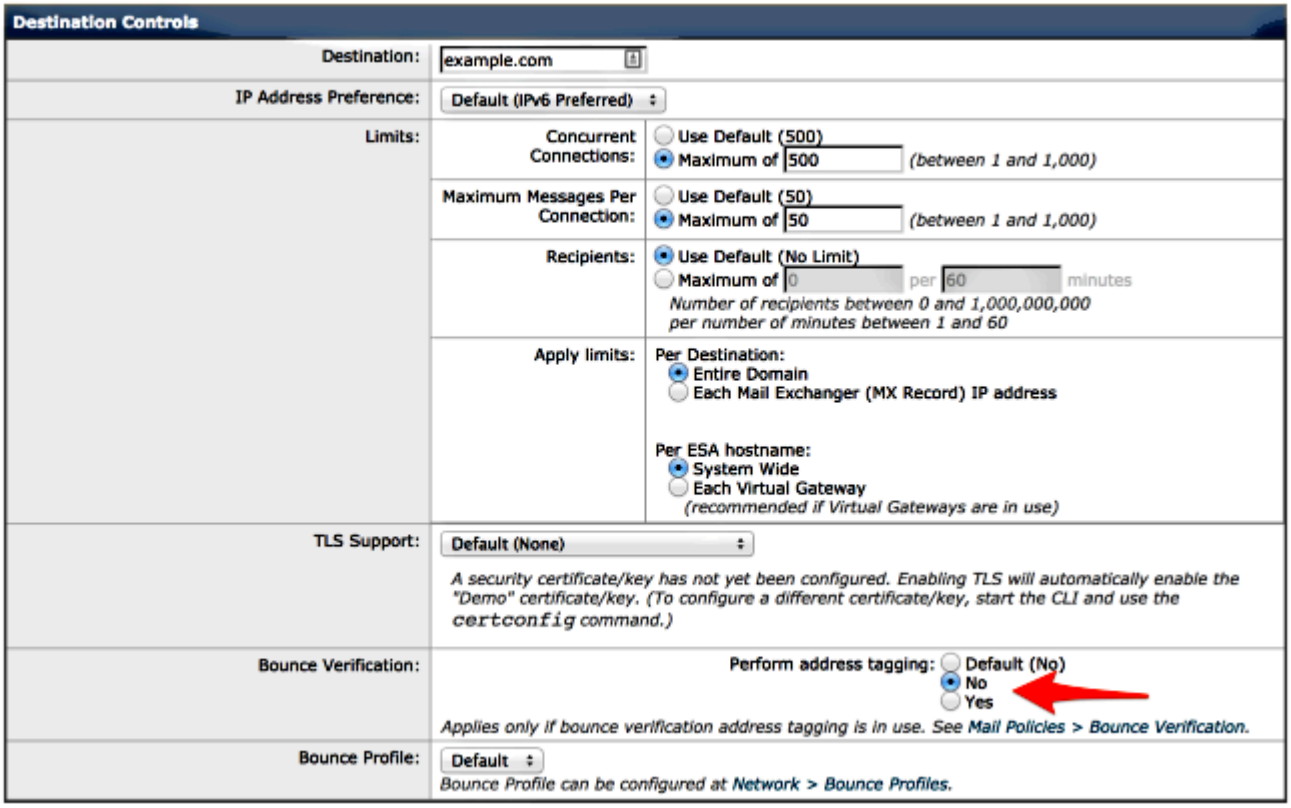
This document describes how to configure inbound and outbound mail to exempt IP addresses, domains, or email addresses for Cisco ESA.

Exempt IP Addresses/Domains/Email Addresses from ESA Bounce Configuration

You can specify recipient domains on which to disable Bounce Verification when the Email Security Appliance (ESA) delivers to those domains. You need to configure both outbound and inbound mail.

Outbound Mail

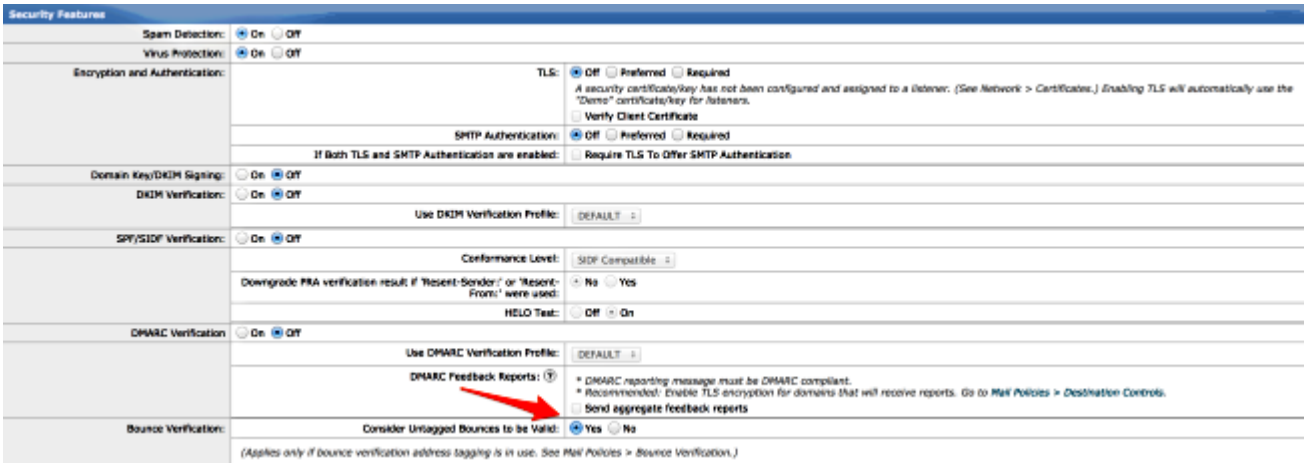
1. Navigate to **Mail Policies > Destination Controls**.
2. Select **Add destination...**
3. Call the new destination **example.com**.
4. In the settings, set **Bounce Verification** to **No**.
5. **Submit** and **Commit** changes.



Note: For outbound mail, you can only refer to the destination domain and not an IP address or email address.

Inbound Mail

1. From **Mail Policies > Mail Flow Policies**, use an exisiting Mail Flow Policy or create a new Mail Flow Policy, and set the **Bounce Verification/Consider Untagged Bounces to be valid** to **Yes**.
2. From **Mail Policies > Hat Overview**, add the domain to a Sender Group that uses the modified or created Mail Flow Policy.



Notes: Failure to configure your inbound mail can cause your ESA to drop valid bounce messages for messages.

Notes: To verify that Bounce Verification is disabled for this domain, you can enable domain debug logs and tail the logs to verify.

Related Information

- Cisco Email Security Appliance - End-User Guides
- Technical Support & Documentation - Cisco Systems