

Configure Cloud Gateway Gold Configuration

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Related Products](#)

[Policy Quarantines](#)

[Cloud Gateway Gold Configuration](#)

[Before You Begin](#)

[Basic Configuration](#)

[Security Services](#)

[System Administration](#)

[Additional Configuration \(Optional\)](#)

[CLI Level Changes](#)

[Host Access Table \(Mail Policies > Host Access Table \(HAT\)\)](#)

[Mail Flow Policy \(Default Policy Parameters\)](#)

[Incoming Mail Policies](#)

[Outgoing Mail Policies](#)

[Other Settings](#)

[Dictionaries \(Mail Policies > Dictionaries\)](#)

[Destination Controls \(Mail Policies > Destination Controls\)](#)

[Content Filters](#)

[Incoming Content Filters](#)

[Outgoing Content Filters](#)

[Cisco Live](#)

[Additional Information](#)

[Cisco Secure Email Gateway Documentation](#)

[Secure Email Cloud Gateway Documentation](#)

[Cisco Secure Email and Web Manager Documentation](#)

[Cisco Secure Product Documentation](#)

[Related Information](#)

Introduction

This document describes an in-depth analysis of the Gold Configuration provided for Cisco Secure Email Cloud Gateway.

Prerequisites

Requirements

Cisco recommends that you know these topics:

- Cisco Secure Email Gateway or Cloud Gateway, both UI and CLI administration
- Cisco Secure Email Email and Web Manager, UI level administration
- Cisco Secure Email Cloud customers can request CLI access; please see: [Command Line Interface \(CLI\) Access](#)

Components Used

The information in this document is from the gold configuration and best practice recommendations for Cisco Secure Email Cloud customers and administrators.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Related Products

This document is also applicable with:

- Cisco Secure Email Gateway on-premises hardware or virtual appliance
- Cisco Secure Email and Web Manager on-premises hardware and virtual appliance


Policy Quarantines

Quarantines are configured and maintained on the Email and Web Manager for Cisco Secure Email Cloud customers. Please log in to your Email and Web Manager to view the quarantines:

- ACCOUNT_TAKEOVER
- ANTI_SPOOF
- BLOCK_ATTACHMENTS
- BLOCKLIST
- DKIM_FAIL
- DMARC_QUARANTINE
- DMARC_REJECT
- FORGED_EMAIL
- INAPPROPRIATE_CONTENT
- MACRO
- OPEN_RELAY
- SDR_DATA
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE

- URL_MALICIOUS

Cloud Gateway Gold Configuration

 **Warning:** Any changes to configuration(s) based on the best practices as provided in this document need to be reviewed and understood before you commit your configuration changes in your production environment. Please consult your Cisco CX Engineer, Designated Service Manager (DSM), or Account Team before configuration changes.

Before You Begin

The Gold Configuration for Cisco Secure Email cloud customers is the best practice and zero-day configuration for both the Cloud Gateway and the Cisco Secure Email and Web Manager. Cisco Secure Email Cloud deployments use both Cloud Gateway(s) and at least one (1) Email and Web Manager. Parts of the configuration and best practices direct administrators to use quarantine(s) located on the Email and Web Manager for centralized management purposes.

Basic Configuration

Mail Policies > Recipient Access Table (RAT)

The Recipient Access Table defines which recipients are accepted by a public listener. At a minimum, the table specifies the address and whether to accept or reject it. Please review the RAT to add and manage your domains as needed.

Network > SMTP Routes

If the SMTP route destination is Microsoft 365, please see [Office365 Throttling CES New Instance with "4.7.500 Server busy. Please try again later"](#).

Security Services

The services listed are configured for all Cisco Secure Email Cloud customers with the values provided:

IronPort Anti-Spam (IPAS)

- Enabled and configure Always scan 1M and Never scan 2M
- Timeout for Scanning Single Message: 60 seconds

URL Filtering

- Enable URL Categorization and Reputation Filters
- (Optional) Create and configure URL Allowlist named "bypass_urls."

- Enable Web Interaction Tracking
- Advanced Settings:
 - URL Lookup Timeout: 15 seconds
 - Maximum number of URLs scanned in body and attachment: 400
 - Rewrite URL text and HREF in Message: No
 - URL Logging: Enabled
- (Optional) As of [AsyncOS 14.2 for Cloud Gateway](#), URL Retrospective Verdict and URL Remediation are available; see release notes provided and [Configure URL Filtering for Secure Email Gateway and Cloud Gateway](#)

Graymail Detection

- Enable and configure Always scan 1M and Never scan 2M
- Timeout for Scanning Single Message: 60 seconds

Outbreak Filters

- Enable Adaptive Rules
- Maximum Message Size to Scan: 2M
- Enable Web Interaction Tracking

Advanced Malware Protection > File Reputation and Analysis

- Enable File Reputation
- Enable File Analysis
 - Please see Global Settings to review file types for File Analysis

Message Tracking

- Enable Rejected Connection Logging (if required)

System Administration

Users (System Administration > Users)

- Remember to review and set passphrase policies associated with **Local User Account & Passphrase Settings**
- If possible, configure and enable Lightweight Directory Access Protocol (LDAP) for authentication (**System Administration > LDAP**)

Log Subscriptions (System Administration > Log Subscriptions)

- If not configured, create and enable:
 - Configuration History Logs
 - URL Reputation Client Logs
- In the Log Subscriptions Global Settings, edit settings and add the headers **To, From, Reply-To, Sender**.

Additional Configuration (Optional)

Additional services to review and consider:

System Administration > LDAP

- If you configure LDAP, Cisco recommends LDAP with SSL enabled


URL Defense

- Please see [Configure URL Filtering for Secure Email Gateway and Cloud Gateway](#) for the most up-to-date configuration best practices for URL Defense.
- Cisco also deeply delves into URL Defense; please see [URL Defense Guide](#).
- Some examples included in the URL Defense Guide are also incorporated into this document.

SPF

- Sender Policy Framework (SPF) DNS records are created externally to Cloud Gateway. Therefore, Cisco strongly recommends all customers build SPF, DKIM, and DMARC best practices into their security posture. Please see [SPF Configuration and Best Practices](#) for more information on SPF validation.
- For Cisco Secure Email Cloud customers, a macro is published for all Cloud Gateway(s) per the allocation hostname to make it easier to add all hosts.
- Place this before ~all or -all within the current DNS TXT (SPF) record, if it exists:

```
exists:%{i}.spf.<allocation>.iphmx.com
```

 **Note:** Ensure the SPF record ends with either **~all** or **-all**. Validate the SPF records for your domains before and after any changes!

- Recommended information and tools for more about SPF:
 - [SPF Record Checker - Free SPF Lookup \(dmarcian.com\)](#)
 - [SPF Record Syntax Table - Everything SPF - dmarcian.com](#)

Additional SPF Examples

- An excellent example of SPF is if you receive emails from your Cloud Gateway and send outbound emails from other mail servers. You can use the "a:" mechanism to specify mail hosts:

```
<#root>
```

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~
```

```
all
```

- If you only send outbound emails through your Cloud Gateway, you could use:

```
<#root>
```

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~
```

```
all
```

- In this example, the "ip4:" or "ip6:" mechanism specifies an IP address or IP address range:

```
<#root>
```

```
v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16
```

```
~all
```

CLI Level Changes

- As noted in Prerequisites, Cisco Secure Email Cloud customers can request CLI access; please see [Command Line Interface \(CLI\) Access](#).

Anti-Spoof Filter

- Please be sure to review the [Best Practices Guide for Anti-Spoofing](#)
- This guide provides you with profound examples and configuration best practices for email spoof prevention

Add Header Filter

- CLI only, please write and enable the addHeaders [message filter](#):

```
addHeaders: if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Host Access Table (Mail Policies > Host Access Table (HAT))

HAT Overview > Additional Sender Groups


- ESA User Guide: [Creating a Sender Group for Message Handling](#)
 - BYPASS_SBRs – Place higher for sources that skip reputation
 - MY_TRUSTED_SPOOF_HOSTS – Part of Spoofing Filter
 - TLS_REQUIRED – For TLS Forced connections

In the predefined SUSPECTLIST sender group

- ESA User Guide: [Sender Verification: Host](#)
 - enable "SBRS Scores on None."
 - (Optional) enable "Connecting host PTR record lookup fails due to temporary DNS failure."

Aggressive HAT Sample

- BLOCKLIST_REFUSE [-10.0 to -9.0] POLICY: BLOCKED_REFUSE
- BLOCKLIST_REJECT [-9.0 to -2.0] POLICY: BLOCKED_REJECT
- SUSPECTLIST [-2.0 to 0.0 and SBRS scores of "None"] POLICY: THROTTLED
- ACCEPTLIST [0.0 to 10.0] POLICY: ACCEPTED

 **Note:** The HAT examples show additionally configured Mail Flow Policies (MFP). For complete information for MFP, please refer to "Understanding the Email Pipeline > Incoming/Receiving" in the [User Guide](#) for the appropriate version of AsyncOS for the Cisco Secure Email Gateway you have deployed.

HAT example:


Sender Groups (Listener: IncomingMail)															
Add Sender Group...		SenderBase™ Reputation Score (?)					External Threat Feed Sources Applied	Mail Flow Policy	Delete						
Order	Sender Group	-10	-8	-6	-4	-2	0	2	4	6	8	+10			
1	SMA												None applied	RELAYED	
2	CISCO_MONITORING												None applied	ACCEPTED	
3	RELAYLIST												None applied	RELAYED	
4	TLS_REQUIRED												None applied	TLS_REQUIRED	
5	MY_TRUSTED_SPOOF_HOSTS												None applied	ACCEPTED	
6	BYPASS_SBRs_SPAM												None applied	ACCEPTED_NOSPAM	
7	BYPASS_SBRs												None applied	ACCEPTED	
8	BLOCKLIST_REFUSE	=====											None applied	BLOCKED_REFUSE	
9	BLOCKLIST_REJECT	=====	=====										None applied	BLOCKED_REJECT	
10	SUSPECTLIST					=====							None applied	THROTTLED	
11	FREEMAIL												None applied	THROTTLED	
12	ACCEPTLIST						=====	=====					None applied	ACCEPTED	
	ALL												None applied	ACCEPTED	

Mail Flow Policy ([Default Policy Parameters](#))

Default Policy Parameters

Security Settings

- Set Transport Layer Security ([TLS](#)) to preferred
- Enable Sender Policy Framework ([SPF](#))
- Enable DomainKeys Identified Mail ([DKIM](#))
- Enable Domain-based Message Authentication, Reporting, and Conformance ([DMARC](#)) Verification and Send Aggregate Feedback Reports

 **Note:** DMARC requires additional tuning to configure. For further information on DMARC, please refer to "Email Authentication > DMARC Verification" in the [User Guide](#) for the appropriate version of AsyncOS for the Cisco Secure Email Gateway you have deployed.

Incoming Mail Policies

Default Policy is configured similar to:

Anti-Spam

- Enabled, with thresholds left at default thresholds. (Modification of the scoring could increase false positives.)

Anti-Virus

- Message Scanning: **Scan for Viruses only**
 - assure check box for "Include an X-header" is enabled
- For **Unscannable Messages** and **Virus Infected Messages**, set **Archive Original Message** to **No**

AMP

- For **Unscannable Actions on Message Errors**, use **Advanced** and **Add Custom Header to Message**, X-TG-MSGERROR, value: True.
- For **Unscannable Actions on Rate Limit**, use **Advanced** and **Add Custom Header to Message**, X-TG-RATELIMIT, value: True.
- For **Messages with File Analysis Pending**, use **Action Applied to Message**: "Quarantine."

Graymail

- Scanning is enabled for each verdict (Marketing, Social, Bulk), with **Prepend** for **Add Text to Subject** and action is **Deliver**.
- For **Action on Bulk Mail**, use **Advanced** and **Add Custom Header (optional)**: X-Bulk, value: True.

Content Filters

- Enabled and URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT are selected
- These content filters are provided later in this guide

Outbreak Filters

- The default threat level is 3; please adjust to your security requirements.
 - If the threat level for a message equals or exceeds this threshold, the message moves to the Outbreak Quarantine. (1=lowest threat, 5=highest threat)
- Enable message modification
- URL Rewriting set for "Enable for all messages."
- Change Subject prepend to: [Possible \$threat_category Fraud]

Policies									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

Policy Names (shown)

• BLOCKLIST Mail Policy

BLOCKLIST mail policy is configured with all services disabled, except Advanced Malware Protection, and links to a content filter with the action of QUARANTINE.

• ALLOWLIST Mail Policy

The ALLOWLIST mail policy has Antispam, Graymail disabled and Content Filters enabled for URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT, or content filters of your choice and configuration.

• ALLOW_SPOOF Mail Policy

The ALLOW_SPOOF mail policy has all default services enabled, with Content Filters enabled for URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR, or content filters of your choice and configuration.

Outgoing Mail Policies

Default Policy is configured similar to:

Anti-Spam

- Disabled

Anti-Virus

- Message Scanning: **Scan for Viruses only**

- un-check the check box for "Include an X-header."
- (Optional) For all messages: **Advanced** > **Other Notification**, enable "Others" and include your admin/SOC contact email address

Advanced Malware Protection

- Enable File Reputation only
- **Unscannable Actions on Rate Limit**: use **Advanced** and **Add Custom Header to Message: X-TG-RATELIMIT**, value: "True."
- **Messages with Malware Attachments**: use **Advanced** and **Add Custom Header to Message: X-TG-OUTBOUND**, value: "MALWARE DETECTED."

Graymail

- Disabled

Content Filters

- Enabled and TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER, or content filters of your choice are selected.

Outbreak Filters

- Disabled

DLP

- Enable, based on your DLP licensing and DLP configuration.

Other Settings

Dictionaries (Mail Policies > Dictionaries)

- Enable and review **Profanity** and **Sexual_Content** Dictionary
- Create **Executive_FED** dictionary for Forged Email Detection with all executive names
- Create additional dictionaries for restricted or other keywords as you see needed for your policies, environment, security control


Destination Controls (Mail Policies > Destination Controls)

- For the Default domain, configure **TLS Support** as **Preferred**
- You can add destinations for webmail domains and set lower thresholds
- Please see our [Rate Limit Your Outbound Mail with Destination Control Settings](#) guide for more information.

Destination Control Table							Items per page 20
Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	<input type="checkbox"/>
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	Off	Default	

* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
^ DANE will not be enforced for domains that have SMTP Routes configured.

Content Filters

 **Note:** For additional information on Content Filters, please refer to "Content Filters" in the [User Guide](#) for the appropriate version of AsyncOS for the Cisco Secure Email Gateway you have deployed.

Incoming Content Filters

URL_QUARANTINE_MALICIOUS

Condition: URL Reputation; url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)

Action: Quarantine: quarantine("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

Condition: URL Reputation; url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)

Action: URL Reputation; url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_INAPPROPRIATE

Condition: URL Category; url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal

Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)

Action: Quarantine; duplicate-quarantine("INAPPROPRIATE_CONTENT")

DKIM_FAILURE

Condition: DKIM Authentication; dkim-authentication == hardfail

Action: Quarantine; duplicate-quarantine("DKIM_FAIL")

SPF_HARDFAIL

Condition: SPF Verification; spf-status == fail

Action: Quarantine; duplicate-quarantine("SPF_HARDFAIL")

EXECUTIVE_SPOOF

Condition: Forged Email Detection; forged-email-detection("Executive_FED", 90, "")

Condition: Other Header; header("X-IronPort-SenderGroup") != "(?i)allows spoof"

* set **Apply rule: Only if all conditions match**

Action: Add/Edit Header; edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

Action: Quarantine; duplicate-quarantine("FORGED_EMAIL")

DOMAIN_SPOOF

Condition: Other Header; header("X-Spoof")

Action: Quarantine; duplicate-quarantine("ANTI_SPOOF")

SDR

Condition: Domain Reputation; sdr-reputation (['awful'], "")

Condition: Domain Reputation; sdr-age ("days", <, 5, "")

* set **Apply rule: If one or more conditions match**

Action: Quarantine; duplicate-quarantine("SDR_DATA")

TG_RATE_LIMIT

Condition: (None)

Action: Add/Edit Header; edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", "")

ACCOUNT_TAKEOVER

Condition: Other Header; header("X-AMP-Result") == (?i)malicious

Condition: URL Reputation; url-reputation(-10.00, -6.00 , "", 1, 1)

***Set Apply Rule: If one or more conditions match**

Action: Notify;notify ("<Insert admin or distro email address>", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")

Action: duplicate-quarantine("ACCOUNT_TAKEOVER")

Order	Filter Name	Description Rules Policies	Duplicate	Delete
1	Stop_O365_OpenRelay	Stop_O365_OpenRelay: if (header("X-IronPort-Tenant") != "placeholder") { duplicate-quarantine("OPEN_RELAY"); }		
2	TG_OUTBOUND_MALICIOUS	TG_OUTBOUND_MALICIOUS: if (header("X-TG-OUTBOUND") == "MALWARE") { quarantine("TG_OUTBOUND_MALWARE"); }		
3	Strip_Secret_Header	Strip_Secret_Header: if (header("PLACEHOLDER") == "PLACEHOLDER") { strip-header("X-IronPort-Tenant"); }		
4	EXTERNAL_SENDER_REMOVE	EXTERNAL_SENDER_REMOVE: if (true) { edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", ""); }		
5	ACCOUNT_TAKEOVER	ACCOUNT_TAKEOVER: if (header("X-AMP-Result") == "(?i)malicious" OR (url-reputation(-10.00, -6.00, "", 1, 1)) { notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING"); duplicate-quarantine("ACCOUNT_TAKEOVER"); }		
6	ENCRYPT_OUT	ENCRYPT_OUT: if (subject == "(?i)*encrypt*") { edit-header-text("Subject", "(?i)*encrypt*\\s?", ""); encrypt-deferred ("CRES_HIGH", "\$Subject", 0); }		
7	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-OUTBOUND-RATELIMIT")) { tag-message ("NOOP"); }		

For Cisco Secure Email Cloud customers, we do have example content filters included within the gold configuration and best practice recommendations. In addition, please review the "SAMPLE_" filters for more information on conditions and actions associated that can be beneficial in your configuration.

Cisco Live

Cisco Live hosts many sessions globally and does offer in-person sessions and technical breakouts that cover Cisco Secure Email best practices. For past sessions and access, please visit [Cisco Live \(requires CCO login\)](#):

- Cisco Email Security: Best Practices and Fine Tuning - BRKSEC-2131
- DMARCCate Your Email Perimeter - BRKSEC-2131
- Fixing Email! - Cisco Email Security Advanced Troubleshooting - BRKSEC-3265
- API Integrations for Cisco Email Security - DEVNET-2326
- Securing SaaS Mailbox Services with Cloud Email Security from Cisco - BRKSEC-1025
- Email Security: Best Practices and Fine Tuning - TECSEC-2345
- 250 not OK – Going on the Defensive with Cisco Email Security - TECSEC-2345
- Cisco Domain Protection and Cisco Advanced Phishing Protection: Making the Most of the Next Layer in Email Security! - BRKSEC-1243

- [SPF is Not an Acronym for "Spoof"! Let's Utilize the Most out of the Next Layer in Email Security! - DGTL-BRKSEC-2327](#)

If a session is unavailable, Cisco Live reserves the right to remove it due to the age of the presentation.

Additional Information

Cisco Secure Email Gateway Documentation

- [Release Notes](#)
- [User Guide](#)
- [CLI Reference Guide](#)
- [API Programming Guides for Cisco Secure Email Gateway](#)
- [Open Source Used in Cisco Secure Email Gateway](#)
- [Cisco Content Security Virtual Appliance Installation Guide](#)(includes vESA)

Secure Email Cloud Gateway Documentation

- [Release Notes](#)
- [User Guide](#)

Cisco Secure Email and Web Manager Documentation

- [Release Notes and Compatibility Matrix](#)
- [User Guide](#)
- [API Programming Guides for Cisco Secure Email and Web Manager](#)
- [Cisco Content Security Virtual Appliance Installation Guide](#)(includes vSMA)

Cisco Secure Product Documentation

- [Cisco Secure portfolio naming architecture](#)

Related Information

- [Cisco Secure Email Security Compliance](#)
- [Offer Description: Secure Email](#)
- [Cisco Universal Cloud Terms](#)
- [Cisco Support & Downloads](#)
- [\[EXTERNAL\] OpenSPF: SPF Basics and Advanced Information](#)