The bridge to possible

Cisco Secure Email

Ordering Guide for GPL

December 2022

Contents

Introduction

Purpose

This ordering guide is designed to help Cisco sales teams, partners, and qualified distributors order Cisco® Secure Email (previously known as Cisco Email Security) solutions available on the Global Price List (GPL). This guide will help you:

- Understand
  - Cisco Secure Email Cloud Gateway (previously known as Cisco Cloud Email Security)
  - Cisco Secure Email Gateway (previously known as Cisco Email Security)
  - Cisco Secure Cloud Mailbox (previously known as Cisco Cloud Mailbox Defense)
  - Cisco Secure Awareness Training (previously known as Cisco Security Awareness)
  - Cisco Secure Email Domain Protection (previously known as Cisco Domain Protection)
  - Cisco Secure Email Phishing Defense (previously known as Cisco Advanced Phishing Protection)
- Understand specific Cisco Secure Email Global Price List offers and identify the right ones for your customers.
- Ensure that the correct SKUs and quantities are configured and ordered to reduce the risk of order rejection.
- Provide information about the end-to-end, quote-to-fulfillment process in Cisco Commerce Workspace and the Cisco Service Contract Center for these offers. Note that Cisco Secure Email Cloud Gateway is available for order only through Cisco Commerce.

Products overview

SecureX Integration: Announced on June 30th, 2020, Cisco Secure Email is part of a simplified platform experience. Connect Cisco's integrated security portfolio to your existing infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. Details here: Announcing SecureX

Cisco Secure Email Cloud Gateway (previously known as Cisco Cloud Email Security/IronPort Hosted Email Security) provides strong email security and exceptional threat protection for organizations of all sizes. Email Cloud Gateway builds on the value of the Cisco network infrastructure that customers have already deployed and encourages the incremental adoption of Cisco security solutions.

Cisco Secure Email Gateway (previously known as Cisco Email Security/IronPort Email Security) is an all-in-one Cisco Secure Email Gateway that offers simple, fast deployment, with few maintenance requirements, low latency, and low operating costs.

Cisco Secure Email Gateway (Hybrid Deployment) is a unique service offering that facilitates the deployment of your email security both on-premises and in the cloud.

Cisco Secure Cloud Mailbox is an integrated, cloud-native security solution for Microsoft 365 that focuses on simple deployment, easy attack remediation, superior visibility, and best-in-class efficacy from Cisco Talos®. It augments native Microsoft 365 security and provides complete visibility into inbound, outbound, and internal user-to-user messages. **Cisco Secure Email Phishing Defense** is a cloud service with the choice of an on-premises/cloud sensor that identities and stops deception-based attacks such as social engineering, impostors, and Business Email Compromise (BEC).

Cisco Secure Email Domain Protection is a cloud service that helps prevent phishing emails from being sent using a customer domain(s). It automates the process of implementing the DMARC email authentication standard.

Cisco Secure Awareness Training (CSA) is a cloud service that helps customers conduct automated security simulations and trainings to their end users, thereby achieving security compliance.

Order requirements

All Cisco Secure Email orders require the following during order entry:

- End-user email address (do not submit an email alias)—email addresses will be used to communicate with direct contacts during the provisioning and network configuration
- Cisco account manager (security sales specialist) email address
- Cisco or partner sales engineer email address

When completing the Cisco Secure Email Cloud Gateway order, some additional information is required for provisioning:

- Customer's primary technical contact name, phone, and email
- Cisco Account Managers (AM) and Solution Architect (SA) name and email, partner name, and email
- Desired data center, if the customer is using Google Apps or Office 365, and the desired custom name

Note: The desired custom name will be used as part of the MX record for the customer (for example, mx1.CUSTOMNAME.iphmx.com).

Failure to provide email addresses will delay the order provisioning process beyond the 3-day Service-Level Agreement (SLA).

Scope

This ordering guide provides information about Cisco Secure Email products on the Cisco Global Price List.

Notes:

Additional documentation and product literature for the Cisco Secure Email Gateway Appliance are available at: https://www.cisco.com/c/en/us/products/security/email-security-appliance/index.html.

A full description of Cisco Secure Email Gateway Appliance along with the detailed terms and conditions for the solution is available at: https://www.cisco.com/c/en/us/about/legal/service-descriptions.html.

Additional documentation and product literature for Cisco Secure Email Cloud Gateway are available at: https://www.cisco.com/web/products/security/cloud_email/index.html.

A full description of Cisco Secure Email Cloud Gateway along with the detailed terms and conditions for the service is available at: https://www.cisco.com/c/en/us/about/legal/service-descriptions.html.

Additional documentation and product literature for the Cisco Secure Email Gateway (Hybrid Deployment) offering is available at: https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet_c78-734189.html.

Any order will be subject to the detailed terms and conditions set out therein.

Cisco Secure Email Cloud Gateway ordering guidelines

Cisco Secure Email Cloud Gateway is a Software-as-a-Service (SaaS) offering to protect customers from email-based threats before they reach a user's mailbox. To purchase Cisco Secure Email Cloud Gateway, customers need software subscription licenses (for cloud), including software support (refer to the “Software subscription licenses” section).

Before you start ordering Cisco Secure Email Cloud Gateway, please note:

Cisco Secure Email Cloud Gateway is not the correct product to order if:

1) Customer wants to send outbound bulk/marketing mails
    a. **Better solution:** Please order an on-premises Cisco Secure Email Gateway Appliance license (there are virtual offerings like KVM, AWS, and VMware available)

Also, if you have a customer with 50,000, users or more, we recommend purchasing SWSS premium license to ensure solution is architected properly. For any clarifications, please engage ces-activations@cisco.com.

Worldwide availability for the GPL

Cisco Secure Email Cloud Gateway on the Cisco Global Price List is a product offering available worldwide except in U.S. export-controlled countries (Cuba, Iran, North Korea, Sudan, and Syria). Customers are typically served out of a cloud presence closest to their deployment location out of the four data centers around the world.

Note: Although there are eight data centers, Cisco Secure Email Cloud Gateway is deployed in a pair of data centers—one pair in the United States, one pair in Europe, one pair in Canada, and one pair in APJ. Multinational companies should choose their preferred pair in the United States, Europe, Canada, or Europe.

Note: The provisioning of the cloud service may take up to 72 hours, assuming the order information is complete and correct.

Sub-enterprise licenses

The Data Loss Prevention and PXE Encryption add-on licenses may be purchased for less than what they would cost for a full enterprise deployment, because they may be applied to a subset of the user population. For example, licenses may be bought for the accounting, legal, finance, and research and development departments, or any other department that requires data protection and confidentiality for its email communications.

Trial Cisco Secure Email Cloud Gateway

Cisco Secure Email Cloud Gateway evaluation products can be requested on behalf of the customer either by the Cisco sales team or a partner:

- Cisco sales team can place trial request on CloudSec SFDC
- Partners can reach out to partnerhelp-ces-pov@cisco.com to raise trial request

Cisco offers a free 45-day evaluation of Cisco Secure Email Cloud Gateway with an option to extend the evaluation. Please consult your Cisco Account Representative to extend the evaluation.

Please note

- Evaluation requests need to be generated by either the Cisco sales team or a partner. End customers cannot directly request a free trial of Cisco Secure Email Cloud Gateway at the present time
- The evaluation form that was earlier available at: https://order.ces.cisco.com/eval/ is going to be discontinued soon. Thus, we encourage the Cisco sales team and partners to request trials via the options mentioned above

Cisco Secure Email Gateway (Hybrid Deployment) ordering guidelines

Cisco Secure Email Gateway (Hybrid Deployment) is for customers wanting to have a mix of on-premises and cloud environment and also give them flexibility to migrate from on-premises to cloud security at any point within the contract term. To purchase Hybrid Email Security, customers need to buy:

1) "Hybrid" software subscription (that combines on-premises and cloud licenses), including software support (refer to the "Software subscription licenses" section)
2) Physical hardware appliances OR virtual appliances (for on-premises)
3) Redistribution form—to be filled anytime (within the contract term) that the customer wants to migrate users from on-premises to cloud (refer to the "License redistribution request" section below)
4) Before you start ordering Cisco Secure Email Gateway (Hybrid Deployment), please note the following.

These offerings are applicable only to:

- Customers wanting to purchase the same license to manage a subset of users on-premises (using Cisco Secure Email Gateway Appliance) and others in cloud (using Cisco Secure Email Cloud Gateway)
- Customers purchasing a license for on-premises but wanting to migrate the users to cloud over the contract period, not vice versa

Note: Do not use Hybrid SKUs if the customer will have certain features permanently on-premises (for example, outbound always on-premises) and certain features always on-cloud. In that case, please order on-premises features/bundle and cloud features/bundle separately in order to ensure the correct quantity is ordered at both places.

Once a license is ordered, customers can move users from on-premises to cloud anytime within the contract term by raising a license redistribution request.

License redistribution request

Customers can request migrating users from on-premises to cloud at any point within the contract term using a license redistribution form.

Only an AM or SA can raise a license redistribution request on behalf of the customer.

Please keep PO # details and a new count of users before making the request.

Cisco Secure Email Gateway Appliance offerings

Understanding the offerings

Cisco Secure Email Gateway Appliance solutions encompass two platforms (email security and security management). There are three offer categories across each of these platforms:

1) Physical hardware appliances or virtual appliances (refer to the "Appliance ordering guidelines" section)
2) Cisco Smart Net Total Care® hardware support, and
3) Software subscriptions, including software support (refer to the "Software subscription licenses" section)

Software subscription licenses

Cisco Secure Email solutions provide a rich set of software features. The platform requires the software subscription licenses in order to activate the features.

Note: Customers may purchase and activate software features only for the associated platform. For example, they can run a Cisco Secure Email software feature on a Cisco Secure Email Gateway Appliance but not on a Cisco Management Security Appliance.

For customers wanting physical appliance-based Email Security, they need to purchase the hardware and software subscription or else the hardware will only work as a Message Transfer Agent (MTA), just passing through the emails without any functionality.

For customers wanting virtual appliance- or cloud-based Email Security, they need to purchase a corresponding software license to enable MTA functionality.

Software subscription support

All Cisco® Secure Email licenses include Software Support Basic for the term of the software subscription licenses. The Basic service level provides:

- Software updates and major upgrades that keep applications performing optimally at the most current feature set
- Access to Cisco Technical Assistance Center (TAC) for fast, specialized support
- Online tools to build in-house expertise and boost business agility
- Collaborative learning for additional knowledge and training opportunities

Upgrading to the high-value service levels, such as Solution Support, Software Support Enhanced, and Software Support Premium, provides everything included in Basic, plus more. These are for-fee services and can be configured for customers. Please refer to the SWSS ordering guide for more details.

The Solution Support service level includes 24x7 technical support with priority case handling, no need to triage an issue before contacting Cisco, and a primary point of contact who has deep solution expertise and who will coordinate support across Cisco and Solution Support Alliance products.

Software Support Enhanced includes all the features in Solution Support, plus offers prioritized case handling over Solution Support, technical onboarding, and adoption assistance.

Software Support Premium includes all the features of Enhanced, plus offers the fastest case handling and a designated technical expert who will know the customer's IT environment and will share best practices for the full lifecycle of the product.

SWSS Enhanced is defaulted for all Secure Email licenses a la carte and in Secure Choice EA.

The above service levels are available to purchase within the product configuration.

Some government agencies, as well as military and high-security private enterprises use on-premise devices that are unable to directly pull updates from Cisco's cloud server due to network restrictions. To address this limitation, Cisco offers Enhanced Support with Offline Updater, in which Cisco support provides software updates and certificates along with deployment and configuration guidance via secure offline methods.

To order, book your CSEMAIL-SEC-SUB product with $0 Basic support only, and then order Enhanced Support with Offline Updater as an add-on via a separate support ATO PID: SUP-OFFLINEUPDTR. Please see the Email Support Ordering Guide for additional details.

Cisco Talos Incident Response

The Cisco Talos Incident Response (CTIR) retainer provides a full suite of proactive and emergency services to help you prepare, respond, and recover from a cybersecurity breach. CTIR enables 24-hour emergency response capabilities and direct access to Cisco Talos, the world's largest threat intelligence and research group.

You can order and transact CTIR with Cisco Secure Email subscription ordering. This will provide you with yet another option to create a stronger security posture and stay protected in case of a security breach. CTIR will be auto-attached with correct sizing based on the product order size. The auto-attached CTIR SKU can be removed and is not mandatory. Also, you can manually select from the available CTIR options in case there is no auto-attach from the "Services" tab.

CTIR options available in the Cisco Secure Email configuration:

CTIR SKU	Description
SVS-CTIR-EMAIL-S	Cisco Talos Incident Response Retainer-Small, Attach with EMAIL
SVS-CTIR-EMAIL-M	Cisco Talos Incident Response Retainer-Medium, Attach with EMAIL
SVS-CTIR-EMAIL-L	Cisco Talos Incident Response Retainer-Large, Attach with EMAIL

To learn more about CTIR, click here.

Ordering Email Security subscription licenses

The Cisco Secure Email software can be easily ordered using a unified Email Security SKU and configuring it with the following details:

1) Term (1, 3, or 5 year)
2) Payment mode (prepaid and annual)
3) Subscription start and end date
4) Form factor (choose on-premises, cloud, or hybrid license)
5) Choosing needed bundle and add-on features

Table 1. Cisco Secure Email license

Product	Description	Unified license SKU
Cisco Secure Email	A Cisco Secure Email software subscription license that can be deployed on-premises or via cloud or hybrid. This SKU only allows prepaid and annual billing options.	**CSEMAIL-SEC-SUB**

The license should then be configured through the following steps:

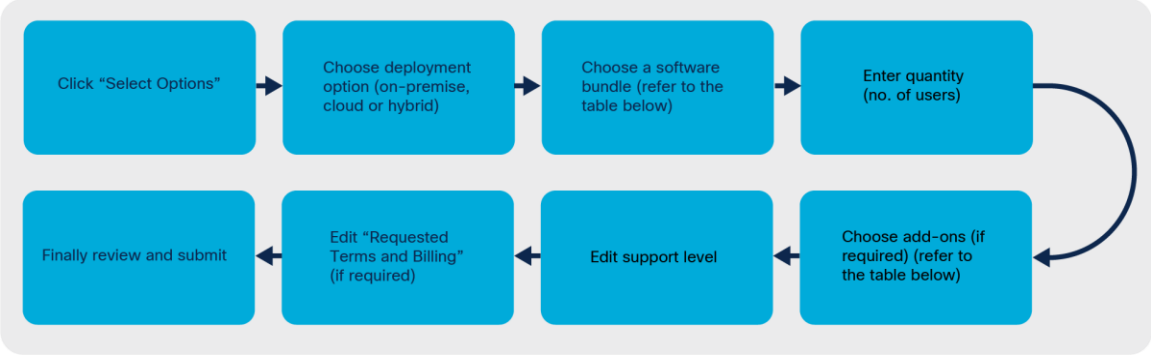


Figure 1.
Ordering process flow in CCW

Table 2. Software bundles and add-ons

Bundle	Description
Essentials bundle	The Cisco Secure Email Cloud Gateway Essentials Bundle purchased through the Global Price List consists of the following bundled services: • Entitlement to the service • **IPAS:** Antispam filtering • **VOF:** Outbreak filters for zero-hour antivirus protection and URL filtering • **AV:** Sophos antivirus filtering • **Cisco Secure Email Malware Defense:** includes file reputation and Cisco Threat Grid sandboxing capabilities This comes with default Threat Grid sandboxing limit of: • 200 file uploads per day for customers with 100–9999 order quantity • 2000 file uploads per day for customers with 10,000–24,999 order quantity • 6000 file uploads per day for customers with 25,000+ order quantity If customers need additional sandboxing capacity, they need to purchase the appropriate add-on Threat Grid sample packs. For details on Threat Grid offerings, visit: https://www.cisco.com/c/en/us/products/collateral/security/amp-threat-grid-cloud/guide-c07-733608.html.

Bundle	Description
Advantage Bundle	The Cisco Secure Email Cloud Gateway Advantage Bundle combines the Essential Bundle features and below listed additional features in one bundle of services: • Entitlement to the service • **IPAS:** Antispam filtering • **VOF:** Outbreak filters for zero-hour antivirus protection and URL filtering • **AV:** Sophos antivirus filtering • **DLP: D**ata loss prevention scanning • **Cisco Secure Email Encryption Service:** Cisco Secure Email Encryption Service • **Graymail Safe Unsubscribe: A**llows users who receive legitimate marketing emails to safely unsubscribe through a third party • **Cisco Secure Email Malware Defense:** includes file reputation and Cisco Threat Grid sandboxing capabilities, comes with unlimited Threat Grid uploads (Unlimited uploads*)For details on Threat Grid offerings, visit: https://www.cisco.com/c/en/us/products/collateral/security/amp-threat-grid-cloud/guide-c07-733608.html. * https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/amp-threatgrid-clarity-offer-description.pdf
Premier Bundle	The Cisco Secure Email Cloud Gateway Premier Bundle combines the Advantage bundle Security features and additional feature listed below in one bundle of Service in one bundle of services: • Entitlement to the service • **IPAS:** Antispam filtering • **VOF:** Outbreak filters for zero-hour antivirus protection and URL filtering • **AV:** Sophos antivirus filtering • **DLP: D**ata loss prevention scanning • **Cisco Secure Email Encryption Service:** Cisco Secure Email Encryption Service • **Graymail Safe Unsubscribe: A**llows users who receive legitimate marketing emails to safely unsubscribe through a third party • **Cisco Secure Email Malware Defense:** includes file reputation and Cisco Threat Grid sandboxing capabilities, comes with unlimited Threat Grid uploads • **Cisco Secure Cloud Mailbox (Available for MS365 Customer only)** • **Cisco Secure Awareness Training:** Software-as-a-Service (SaaS) product used by administrators to automate end-user security training and simulation across 40 different languages For details on Threat Grid offerings, visit: https://www.cisco.com/c/en/us/products/collateral/security/amp-threat-grid-cloud/guide-c07-733608.html. * https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/amp-threatgrid-clarity-offer-description.pdf
Cisco Secure Cloud Mailbox for Microsoft 365	Cisco Secure Cloud Mailbox is an integrated, cloud-native security solution for Microsoft 365 that focuses on simple deployment, easy attack remediation, superior visibility, and best-in-class efficacy from Cisco Talos. It augments native Microsoft 365 security and provides complete visibility into inbound, outbound, and internal user-to-user messages.

Bundle	Description
Add-on	**Description**
Data Loss Prevention	The Email Security Data Loss Prevention (DLP) Add-On provides the data loss prevention scanning feature as an add-on to the Essentials Bundle.
Image Analyzer	The Email Security Image Analyzer Add-On provides scanning for adult content in images contained in emails, often deployed along with DLP to implement acceptable use policies.
Intelligent Multiscan	The Email Security Intelligent Multiscan Add-On provides additional antispam classification capabilities by combining the results of the multiple antispam classifier with the Cisco IPAS classifier in the all Secure Email Bundles. It increases the spam catch rate at the possible expense of a greater number of false positives.
McAfee Antimalware	The Email Security McAfee Antimalware Add-On provides additional antivirus protection as an add-on to the Sophos antivirus engine that comes with the Essentials, Advantage and Premier Bundles.
Encryption	The Email Security Encryption Add-On provides the Cisco Secure Email Encryption Service technology as an add-on to the Essentials Bundle.
Graymail Safe Unsubscribe	The Email Security Safe Unsubscribe Add-On allows users who receive legitimate marketing emails to safely unsubscribe through a third party.
Cisco Secure Cloud Mailbox	The Cisco Secure Cloud Mailbox add-On provides an internal (east-west) email scanning solution for Cisco Secure Email Cloud Gateway customers with mailboxes hosted in Microsoft 365. Internal Mailbox Defense is powered by Cisco Secure Cloud Mailbox (SKU = CES-IMD-LIC).
Cisco Secure Email and Web Manager (previously known as Security Management Appliance) **(On-premises and Hybrid)**	Provides centralized reporting, message tracking, and quarantines across multiple Cisco Secure Email Gateway Appliances (Email Reporting + Tracking + Centralized Quarantines) on-premises **Note:** The management appliance need not be ordered separately for cloud users.

The Cisco Secure Email portfolio uses tiered quantity-based pricing, with the user count entered as the applicable quantity. Sales and partner representatives should work with customers to determine the correct sizing for each customer deployment so that the appropriate user count is selected for each license. Cisco Commerce and the Cisco Service Contract Center automatically select the appropriate SKU associated with the user count that is entered. They then apply the associated price point to the entered quantity to generate a total price for that particular SKU. For the Cisco Secure Email Gateway Appliance, a user quantity is equal to the number of unique mailboxes desired.

Cisco Secure Email Unified SKU overview

Orders for Cisco Secure Email Unified SKU involve four SKU types:

- The subscription SKU, which is used to define the subscription term and start date
- The product SKUs, which are used to define the products and quantities that make up the subscription
- The product add-on SKUs, which can only be added on to other product SKUs
- The support SKUs, which define the level of support for the subscription

Orders start with the selection of the Email Security subscription SKU. This is followed by the configuration of the subscription by selecting the product, add-on, and support SKUs that will constitute the subscription.

Subscription SKU

There is only one subscription SKU for Email Security. The term and payment option of the subscription applies to all products included in the subscription.

SKU type	SKU	Description
Subscription	CSEMAIL-SEC-SUB	Cisco Secure Email XaaS Subscription

Step 1: Selecting the subscription SKU

There is only one Email Security subscription SKU (CSEMAIL-SEC-SUB). There is no price for the subscription SKU. Pricing is determined when product SKUs are added and configured. Select a quantity of one because each end customer can have only one configuration (On-premises, Hybrid or Cloud) through one CSEMAIL-SEC-SUB subscription. Product quantities will be entered when the product SKUs are added to the subscription.

Note: Each line item of CSEMAIL-SEC-SUB can have only one deployment scenario (such as on-premises, cloud, or hybrid).

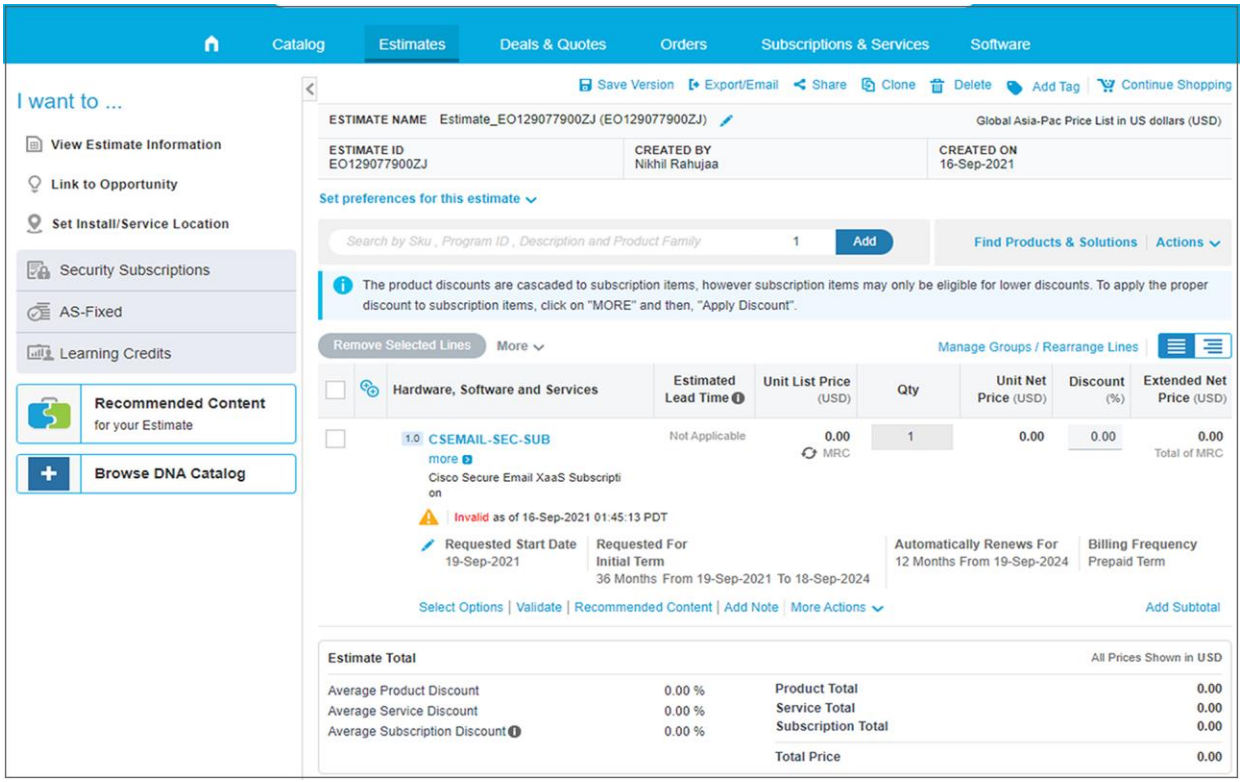


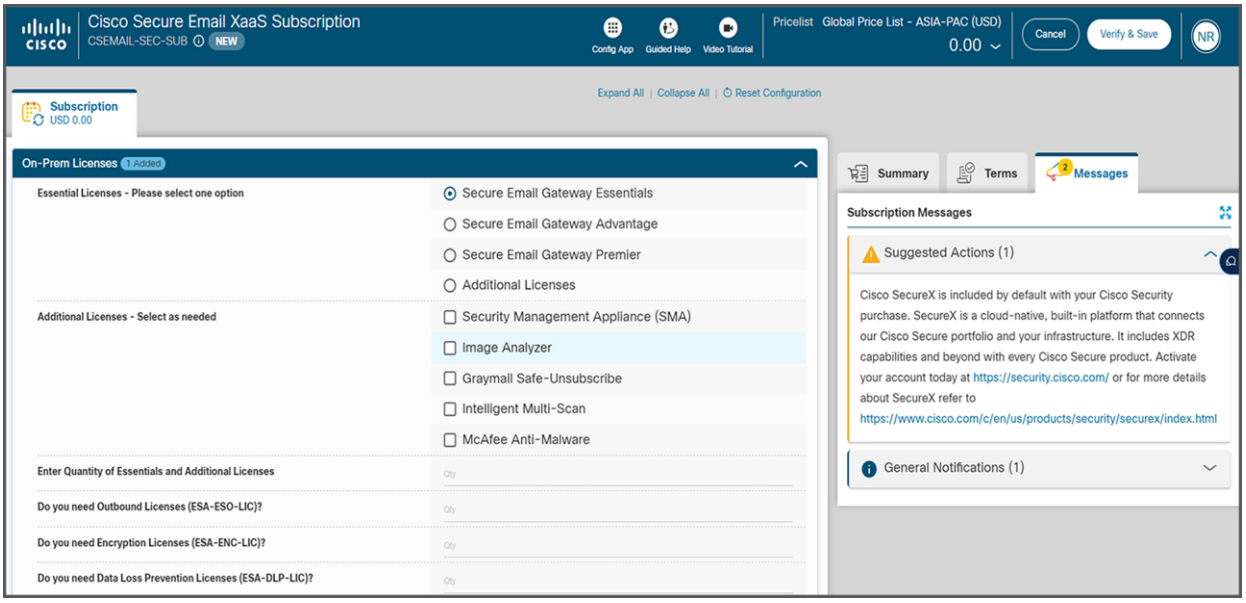
Figure 2.
How to select subscription SKU IN CCW

Step 2: Selecting the subscription license (software subscriptions)

After selecting the subscription SKU, choose “Select Options” to select the licenses and to edit the subscription term and the requested start date.

When the subscription terms have been set, the next step is to add products to the subscription. The term for the product is defined by the subscription term.

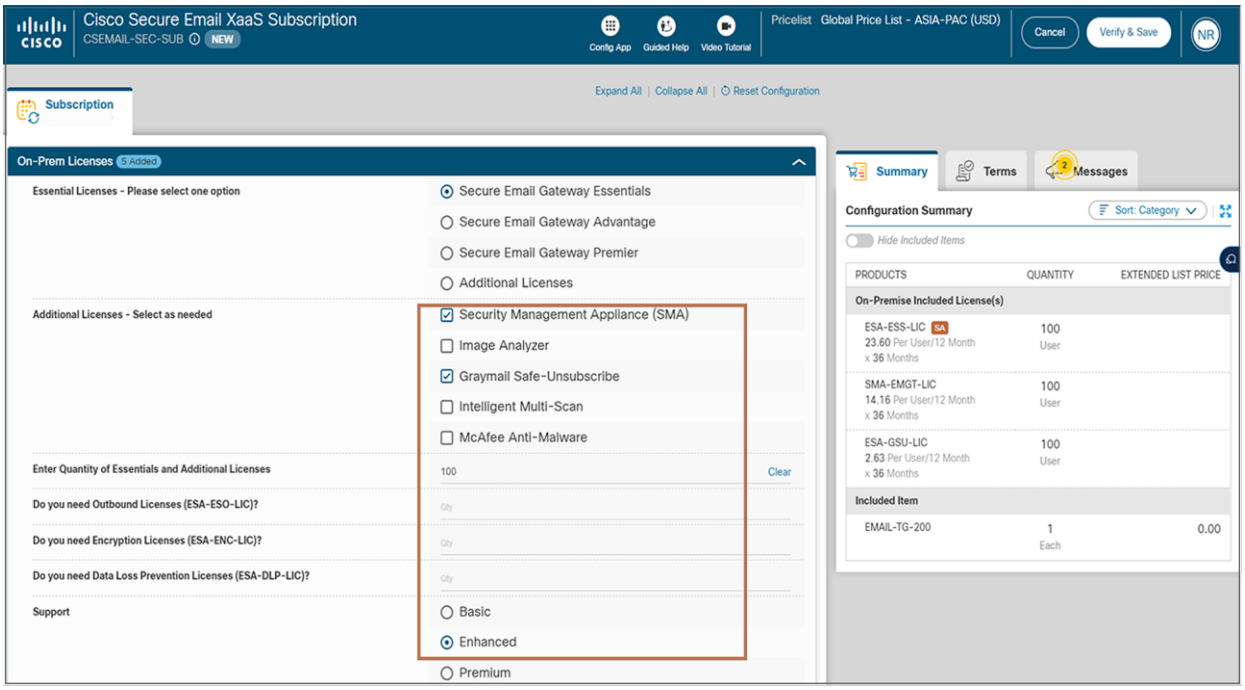
Start by selecting the appropriate product in the subscription configuration summary. The guidance below uses On-Prem License and Essential bundle as the product selection as an example.



Note: For information on various software license options, refer Table 2 on page 9.

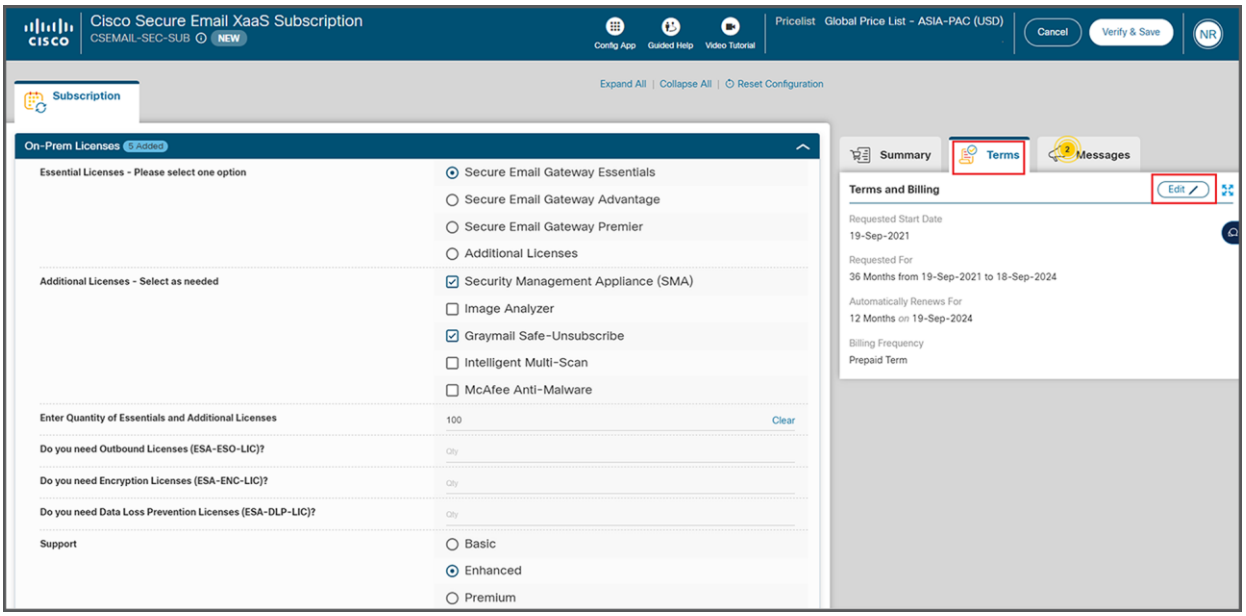
Step 3: Quantity and additional selections

Once the selection of the license and “add-on” licenses are made, the next step is to enter the quantity. The user is also asked to choose the support plan, and once all of the selections and quantities are entered, the “Configuration Summary” on the right shows the updated subtotal. Monthly rates for each license SKU are shown in the breakup; however, the billing currently is either annual or prepaid as per the Subscription Term configuration page of CSEMAIL-SEC-SUB.

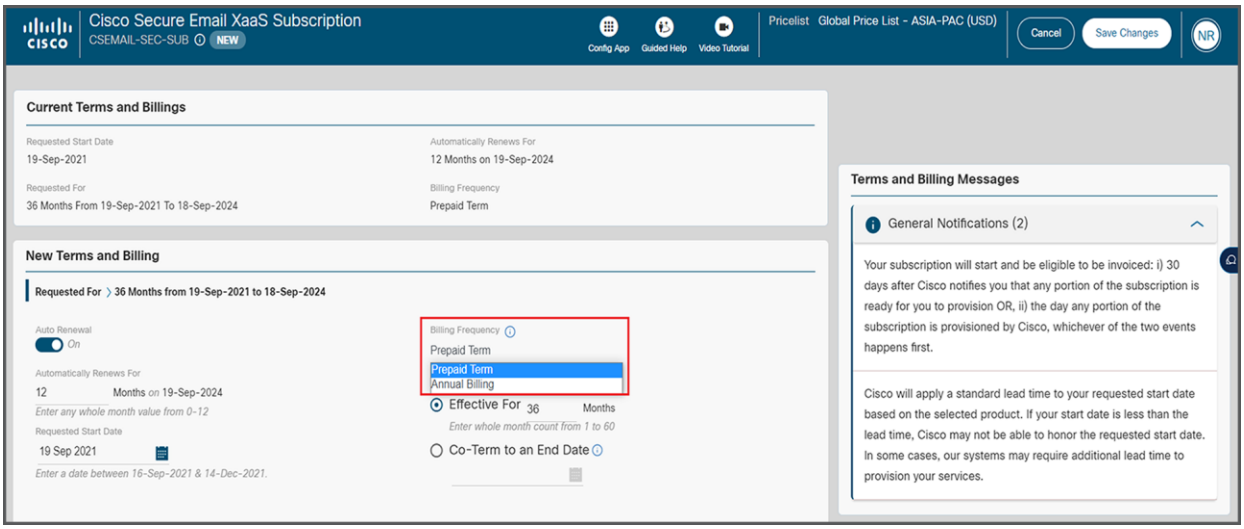


Step 4: Review and confirm the subscription term

Select the “Terms” tab to view the subscription term details. To make any changes to the subscription term, click on the “Edit” option.



The subscription term will default to a 36-month term and prepaid term billing. The requested start date may also be changed at this time.



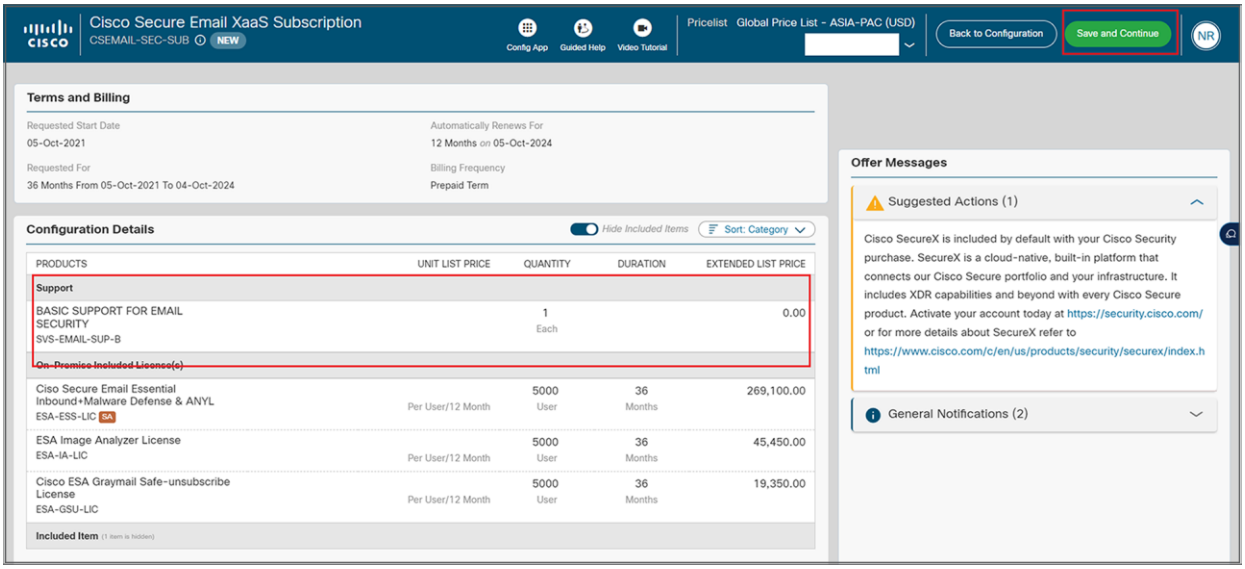
Currently only annual and prepaid billing is supported.

- Only terms that are multiples of 12 months (for example, 12, 24, 36) are allowed (for example, no 42-month “co-term” subscriptions with annual billing).
- The PO needs to be issued for the full amount of the entire term, but billing will occur annually at the start of each service year.

The service is provisioned, and the subscription starts on the service start date. The provisioning of the service may take up to 72 hours, assuming the order information is complete and correct.

Step 5: Review changes and confirm

Click on “Verify and Save” on the top-right corner of the main screen to go to the My Offer Summary screen shown below. Click on “Save and Continue” to confirm and return to the CCW Estimate screen.



Note: Hybrid bundles contain underlying on-premises Cisco Secure Email Gateway Appliance and Cisco Secure Email Cloud Gateway software subscription SKUs that need to be configured with the appropriate quantity. Subscription terms follow that of the parent CSEMAIL-SEC-SUB.

Note: The Cisco Secure Email Management feature allows administrators to centrally report and search quarantines across multiple email gateways at the same time. This feature is part of the Cisco Security Management Appliance (SMA) and needs to be ordered separately. This feature need not be purchased separately for Cisco Secure Email Cloud Gateway.

If customers currently have a valid contract and a valid term license that do not contain the Centralized Management feature, they can request the feature through https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart. They will receive a Centralized Management license co-termed with their existing license.

Table 3. Content Security Management software offerings

Bundles	Description
Cisco Secure Email Management	Provides centralized reporting, message tracking, and quarantines across multiple Cisco Secure Email Gateway Appliances (Email Reporting + Tracking + Centralized Quarantines)
Bundle features	
Email Reporting	Provides concise scenario-based reports to help administrators troubleshoot and keep tabs on their message flows
Email Message Tracking	Helps administrators track the flow of individual email messages
Email Centralized Quarantines	Helps end users and administrators manage their quarantines

Software license agreements

The Cisco End User License Agreement (EULA) and the Cisco Secure Email Supplemental End User License Agreement (SEULA) are provided with each software license purchase. The documents are available at the following links:

- Cisco EULA: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html
- Cisco SEULA: https://www.cisco.com/web/about/doing_business/legal/service_descriptions/related.html

Cisco Secure Email Threat Defense ordering guidelines

Cisco Secure Email Threat Defense (formerly known as Cloud Mailbox) is an integrated, cloud-native security solution for Microsoft 365 that focuses on simple deployment, easy attack remediation, superior visibility, and best-in-class efficacy from Cisco Talos. It augments native Microsoft 365 security and provides complete visibility into inbound, outbound, and internal user-to-user messages.

With Cisco Secure Email Threat Defense, customers can:

- Detect and block threats with superior threat intelligence from Cisco Talos, one of the largest threat research and efficacy teams
- Combat advanced threats using Cisco Secure Email Malware Defense and Cisco Threat Grid
- Get complete visibility into inbound, outbound, and internal messages
- Leverage fast, API-driven remediation of messages with malicious content
- Use an integrated dashboard for search, reporting, and tracking, including conversation view and message trajectory
- Enhance Microsoft 365 email security in less than 5 minutes without changing the mail flow

Businesses of all sizes in all verticals who use Microsoft 365 can use Email Threat Defense to protect the number one threat vector—email.

Cisco Secure Email Threat Defense is available as part of CSEMAIL-SEC-SUB as well as a standalone CMD-SEC-SUB subscription SKU. The product SKU specifies the seat count and subscription term. Pricing follows a tiered model and is calculated dynamically based on the seat count banding and term of the subscription. Here are all the available support options to choose from:

- **Basic:** SVS-CMD-SUP-B
- **Solution Support:** SVS-CMD-SUP-S
- **Enhanced Support:** SVS-CMD-SUP-E
- **Premium Support:** SVS-CMD-SUP-P

All Cisco Secure Email Threat Defense purchases include Enhanced Support by default for the first year of the subscription and would be defaulted to Basic for the consequent renewals. Cisco Secure Email Threat Defense pricing will be upgraded to Core Discount Category as on 12th November 2022.

Cisco Secure Awareness Training ordering guidelines

The Cisco Secure Awareness Training product is a Software-as-a-Service (SaaS) product used by administrators to automate end-user security training and simulation across 40 different languages.

The product comes with multiple training catalogs and simulation templates that can be customized and modified as per the customer's needs.

The product is sold as term and content SKUs as well as a Subscription Billing Platform (SBP) unified SKU, with terms being 1, 3, or 5 years.

Table 4. Cisco Secure Awareness Training offerings—SBP unified SKU

Offerings	Description	Top-level SKU
Cisco Secure Awareness Training	Top-level Cisco Secure Awareness Training unified SKU that contains all offers for 1, 3, or 5 years	SA-SEC-SUB

Table 5. Cisco Secure Awareness Training offerings—offerings underlying the SBP SKU (mentioned in Table 4)

Offerings	Description	Top-level SKU
Cisco Secure Awareness Training - Simulation + Training Select(Ultimate License)	Ultimate bundle of Cisco Security Awareness Training offers unlimited access to available CSA assets including complete library of simulations, topics and languages	SA-ULT-LIC
Cisco Secure Awareness Training - Simulation Only	This is for customers particularly wanting to generate only quizzes and simulations to end users to test if they open, click through, and generate reports for compliance purposes.	SA-SS-LIC
Cisco Secure Awareness Training - Simulation + Training Select	This is for customers having to automate entire end-user quizzing and simulation followed up by focused video-based trainings. Customers get the ability to choose any 12 topics from each category (listed below) and deliver them to their end users. Refer to Table 6 for details. **Note:** Once 12 topics are chosen and delivered to any of their users, they cannot be reversed. However, admins can preview the entire package themselves before deploying and have flexibility to change the topics before it is deployed.	SA-SLT-LIC

Table 6. Cisco Secure Awareness Training categories and topics

Awareness category	Topics	
Essentials	• Protecting Sensitive Information • Overview of Information Classification • Common Threats to Information • Creating Strong Passwords • Web and Cyber Threats	• Safe Internet Practices • Security at the Office • Working Remotely and Traveling Safely • Email Security • Identifying a Scam Attempt • Browsing the Web Securely
End-User Trainings	• Introduction to Information Security • Access Control • Bring Your Own Device (BYOD) • Business Email Compromise • Confidentiality on the Web • Cloud Computing • Data Leakage • Email • Identity Theft • Incident Reporting • Information Classification • Information Lifecycle • Intellectual Property • Malware • Mobile Devices	• Passwords • Phishing • Physical Security • Privacy • Protecting Payment Card Data • Protecting Your Home Computer • Ransomware • Responsible Use of the Internet • Smartphones • Social Engineering • Social Networks • The Clean Desk Principle • Traveling Securely • Unintentional Insider Threat • Working Remotely
Phishing	• Introduction to Information Security • Business Email Compromised • Email • Identity Theft • Malware • Phishing • Ransomware • Social Engineering	
Microlearnings	• Business Email Compromised – “BEC” • C-Level Email Impersonation • Incident Reporting – Missing Laptop • Mass Market Phishing • Phishing via SMS – “Smishing” • Ransomware – Files Locked • Spear Phishing • Top Executive Phishing – “Whaling” • Vishing – You Win a Prize • Web Phishing Through Search Engines	

Awareness category	Topics	
Nanolearnings	• Being Security Aware • Cyber Attack Detection • Identity Theft – Example of an Attack • Insider Threat • Phishing – 6 Clues • Phishing – Ransomware • Phishing – Vishing • Phishing – Spear Phishing (CEO Fraud) • Phishing – Phishing Website • Phishing Smishing	• Phishing – Anatomy of Spear Phishing • Preventing Security Breaches • Protecting Sensitive Information • Social Engineering • Social Networks • Wi-Fi Security
Manager Training	• Introduction to Information Security • Components of an Information Security Governance Framework • Information Security and Technology • Information Security Roles and Responsibilities • Security Risks Posed by New Technology and Mobility	
IT Administrators	• Common Network Attacks • Network Security Overview • Securing Data Repositories • Securing Networks	
IT Developers	• Application Security Overview • Common Application Attacks • Cryptography Overview • Secure Development	

Note: The catalog gets updated every month with new content.

Table 7. Cisco Secure Awareness Training languages supported

EN	English	**HR**	Croatian	**SR**	Serbian
EN-UK	English (United Kingdom)	**HU**	Croatian	**SV**	Swedish
FR	French (Canada)	**ID**	Indonesian	**TH**	Thai
FR-FR	French (France)	**IT**	Italian	**TR**	Turkish
ES	Spanish (Latin America)	**JA**	Japanese	**UK**	Ukrainian
ES-ES	Spanish (Spain)	**KO**	Korean	**VI**	Vietnamese
AR	Arabic	**MS-MY**	Malay (Malaysia)	**ZH-HK**	Chinese (Hong Kong)
CS	Czech	**NB**	Norwegian		(Script traditional; narration Cantonese)
DA	Danish	**NL**	Dutch	**ZH-CN**	Chinese (PRC)
DE	German	**PL**	Polish		(Script simplified; narration Mandarin)
EL	Greek	**PT**	Portuguese (Brazil)	**ZH-YU**	Chinese (PRC)
FA	Persian	**PT-PT**	Portuguese (Portugal)		(Script simplified; narration Cantonese)
FI	Finnish	**RO**	Romanian	**ZH-TW**	Chinese (Taiwan)
HE	Hebrew	**RU**	Russian		(Script traditional; narration Mandarin)
HI	Hindi	**SK**	Slovak		

Note: Customers have the ability to configure their view to only the specific languages required for them.

Note: The product can be ordered beginning February 24, 2020.

Trial Cisco Secure Awareness Training

A trial can be requested for the customer using the Cisco Secure Awareness Training (CSA) trial request form and filling out the requisite details at the form here.

A 45-day trial with a 100-user license is issued to customers.

If there are additional queries, you can reach out to sat-inquiries@cisco.com or esa-pm@cisco.com.

Cisco Secure Email Phishing Defense ordering guidelines

Cisco Secure Email Phishing Defense is a cloud service that identifies and stops deception-based attacks such as social engineering, impostors, and Business Email Compromise (BEC).

Cisco Secure Email Phishing Defense

- Combines local email intelligence and advanced machine learning techniques to model trusted email behavior on the Internet, within organizations, and between individuals.
- Integrates machine learning techniques to drive daily model updates, maintaining a real-time understanding of email behavior to stop identity deception.
- Combines Rapid DMARC, Advanced Display Name Protection, and Look-Alike Domain Imposter-driven detection to stop BEC attacks.

This service comes in multiple flavors (software subscription licenses) depending upon the customer's choice to deploy an inbuilt feature called "Data Collection Sensor" on-premises or cloud.

Data Collection Sensor - Virtual Appliance or Hosted Sensor

- Enables receipt of inbound email traffic, analysis and extraction of metadata, and transmission of metadata to the cloud for further analysis.
- Contains tools for monitoring and configuring one or more sensors post-installation.
- Contains tools for updating the software version run by a sensor post-installation.

The service is fully certified and compliant with all regulatory requirements.

Important:

- The product comes with either a 1- or 3-year subscription and has similar seat bands as other Email Security offerings.
- It is recommended to deploy the service behind Cisco Secure Email Gateway.

Note: Cisco announces the end-of-sale and end-of-life dates for the Cisco Secure Email Phishing Defense (TnC & SaaS Subscription). The last day to order the affected product(s) is December 14, 2022. The last day to renew or add to an existing subscription is December 14, 2022. It is advised to consider Cisco Secure Email Threat Defense (formerly known as Cloud Mailbox and Cloud Mailbox Defense) as a replacement for Cisco Secure Email Phishing Defense and contact the product team (ces-pm@cisco.com) to learn about the migration strategy.

Table 8. Cisco Secure Email Phishing Defense offerings

Offerings	Description	Top-level SKU
Cisco Secure Email Phishing Defense On-Prem (with on-premises sensor)	This is for customers particular about the content of their email not leaving customer premise while only metadata is sent to the cloud.	L-ESA-APP-LIC=
Cisco Secure Email Phishing Defense On-Prem (with cloud sensor)	This is for customers with an on-premises email gateway/mailbox but not concerned with email going to the cloud for Cisco Secure Email Phishing Defense.	L-ESA-APPC-LIC=
Cisco Secure Email Phishing Defense Cloud (with cloud sensor)	This is for customers preferring email analysis on the cloud.	L-CES-APPC-LIC=
Cisco Secure Email Phishing Defense Migration	This SKU MUST be added for any existing Agari Advanced Phishing Protection accounts that are now being booked under Cisco and is NOT applicable to renewals. To ensure no loss in data, customer data MUST be migrated from the Agari instance to Cisco. Failure to add this SKU will result in delayed booking.	L-CES-APPMR-LIC=

Cisco Secure Email Domain Protection ordering guidelines

Cisco Secure Email Domain Protection is a cloud service that helps protect customers' brand phishing emails from being sent using a customer domain(s). It automates the process of implementing the DMARC email authentication standard to better protect employees, customers, and suppliers from phishing attacks using a customer domain(s).

Cisco Secure Email Domain Protection protects the customers' brand identity and also increases email marketing effectiveness by reducing phishing messages from reaching inboxes.

The product comes in two flavors depending upon whether the customer is on-premises or a Cisco Secure Email Cloud Gateway customer.

Table 9. Cisco Secure Email Domain Protection offerings

Offerings	Description	Top-level SKU
Cisco Secure Email Domain Protection (for on-premises customers)	This is for customers with on-premises mailboxes/email gateways.	L-ESA-DMP-LIC=
Cisco Secure Email Domain Protection (for cloud customers)	This is for customers with cloud-based mailboxes/email gateways.	L-CES-DMP-LIC=
Cisco Secure Email Domain Protection Migration	This SKU MUST be added for any existing Agari Domain Protection accounts that are now being booked under Cisco and is NOT applicable to renewals. To ensure no loss in data, customer data MUST be migrated from the Agari instance to Cisco. Failure to add this SKU will result in delayed booking.	L-CES-DMPMR-LIC=

Either of these products come with a dedicated 1-year service SKU that provides customers with dedicated Customer Support staff to help with the products as and when required.

Table 10. Email Software Advanced Phishing Protection offerings

Offerings	Description	Top-level SKU
Cisco Email Domain and Cloud Advanced Phishing Protection Service	A 1-year service SKU that provides customers with a hands-on expert to guide them when required.	L-EML-DPAP-SVC=

This is a subscription service offering designed to accelerate solution adoption and time to value for Cisco customers. It is a full-service approach for customers who do not have in-house expertise or resources to implement the cloud service or who want to buy services instead of doing it themselves.

Each Cisco customer who purchases the DPAP service will be assigned a technical hands-on resource to deliver value and act as a single point of contact for the cloud service. The service includes:

- **Days per year:** Up to 24 days (192 person-hours) of Supplier Personnel time
- **Onsite:** Up to 25% services are done on-site
- **Travel:** Included in price
- **Duration:** 12 months to use the services from date of purchase

Order as many quantities that would satisfy the customer's required days of support.

Trial Cisco Secure Email Domain Protection/Cisco Secure Email Phishing Defense

Any account manager/content security expert/partner with a CCO ID should be able to request trial/evaluation for Cisco Secure Email Domain Protection/Cisco Secure Email Phishing Defense by going to https://order.ces.cisco.com/eval/ and clicking on "Request DP or APP evaluation."

Cisco Secure Email Gateway Appliance ordering guidelines

Table 11 lists the Cisco Secure Email product lines that are available through Cisco Price Lists.

Table 11. Cisco Secure Email platforms

Product Name	Description
Cisco Secure Email	Cisco Secure Email offerings provide protection against email threats, reduce downtime associated with email-borne malware, simplify the administration of corporate mail systems, and reduce the burden on technical staff while offering insight into mail system operation. Cisco Secure Email Gateway Appliances include the following components: • Cisco Secure Email Gateway Appliance hardware, including the Cisco Secure Email Appliances C195, C395, and C695 • Email Security software subscription bundles and standalone offerings, including Cisco Software Support • Smart Net Total Care Services for Cisco Secure Email Gateway Appliances

Product Name	Description
Cisco Content Security Management	Content Security Management offerings provide a single management interface for Cisco Email and Web Security Appliances. By providing a single location to centralize email reports and spam quarantines as well as manage web security and Cisco Data Loss Prevention (DLP) policies, the Content Security Management Appliance provides valuable functions for email and web administrators. Content Security Management Appliances include the following components: • Security Management Appliance hardware, including the Cisco Security Management Appliances M195, M395, and M695 • Security Management software subscription bundles and standalone offerings, including Software Support Security Management Appliance hardware, including the Cisco Security Management Appliances M195, M395, and M695 • Smart Net Total Care Services for Security Management Appliances

Physical appliances

Cisco offers the Email Security hardware appliances listed in Table 12 below.

Table 12. Cisco Secure Email Gateway Appliances

Appliance type	Deployment*	SKU	Description*
Cisco Secure Email	Small businesses and branch offices	ESA-C195-K9	ESA C195 Cisco Secure Email Gateway Appliance with Software
	Midsize offices	ESA-C395-K9	ESA C395 Cisco Secure Email Gateway Appliance with Software
	Large enterprises and service providers	ESA-C695-K9 ESA-C695F-K9	ESA C695 Cisco Secure Email Gateway Appliance with Software ESA C695 Email Security with 1 GE or 10 GE Fiber Interfaces
Cisco Security Management	Small businesses and branch offices	SMA-M195-K9	SMA-M195 Security Management Appliance with Software
	Midsize offices	SMA-M395-K9	SMA M395 Security Management Appliance with Software
	Large enterprises and service providers	SMA-M695-K9 SMA-M695F-K9	SMA M695 Security Management Appliance with Software SMA M695 Security Management with 1 GE or 10GE Fiber Interfaces

* Sizing will vary depending on a number of factors, not limited to deployment configurations, software feature sets, and policies. Work closely with your customers to understand the specific hardware and performance needs of their Cisco Secure Email deployments.

Virtual appliances

Customers can also choose to have virtual appliances in place or alongside of physical appliances.

The virtual appliances come in multiple flavors and are supported on platforms like VMWare and KVM.

Table 13. Email Security Virtual Appliances

Appliance type	Deployment	Model
Cisco Secure Email	Small businesses and branch offices (up to 1000 employees)	C100v
	Midsize offices (up to 5000 employees)	C300v
	Large enterprises and service providers	C600v
Cisco Security Management	Small businesses and branch offices	M100v
	Midsize offices	M300v
	Large enterprises and service providers	M600v

Cisco Smart Net Total Care service

Customers can buy the Smart Net Total Care service for Cisco Secure Email Gateway Appliances.

This service gives customers access to a wealth of Cisco support tools and expertise, providing them with greater network availability and performance while reducing operating costs. The service provides:

- **Fast support from experts:** Connect directly to the Cisco Technical Assistance Center (TAC), staffed by thousands of certified Cisco professionals who have experience diagnosing the toughest problems.
- **Online self-help support:** Access extensive 24-hour support resources through Cisco's online knowledge base, communities, resources, and tools.
- **Smart, proactive diagnostics:** Gain critical insight with the embedded Cisco Smart Call Home feature, which offers detailed diagnostics and immediate alerts on enabled network devices.
- **Ongoing operating system updates:** Access new OS features, including both minor and major OS releases, with the latest operating system software updates within your licensed feature set.
- **Rapid hardware replacement:** Get the coverage you need for each device with flexible hardware replacement options, including Next-Business-Day (NBD) advance replacement.

Please refer to Table 14 and the following link for more detailed information regarding the Smart Net Total Care service: https://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2978/serv_group_home.html.

Table 14. Smart Net Total Care service SKUs for Cisco Secure Email Gateway Appliances

Appliance type	Appliance SKU	8x5xNBD Smart Net Total Care SKU	8x5x4 Smart Net Total Care SKU
Cisco Secure Email	ESA-C195-K9	CON-SNT-ESAC195K	CON-SNTE-ESAC195K
	ESA-C395-K9	CON-SNT-ESAC395K	CON-SNTE-ESAC395K
	ESA-C695-K9	CON-SNT-ESAC695K	CON-SNTE-ESAC695K
	ESA-C695F-K9	CON-SNT-ESAC695F	CON-SNTE-ESAC695F
Cisco Security Management	SMA-M195-K9	CON-SNT-SMAM195K	CON-SNTE-SMAM195K
	SMA-M395-K9	CON-SNT-SMAM395K	CON-SNTE-SMAM395K
	SMA-M695-K9	CON-SNT-SMAM695K	CON-SNTE-SMAM695K
	SMA-M695F-K9	CON-SNT-SMAM695F	CON-SNTE-SMAM695F

Note: "8x5xNBD" denotes that service is available during an 8-hour day, 5 days a week, beginning the next business day after the request. "8x5x4" indicates that service is available during an 8-hour day, 5 days a week, providing a 4-hour response time.

Accessories

The Cisco Secure Email platforms include numerous accessories that are either required for basic functions (for example, power cords) or optional based on specific needs of the customer (for example, a locking faceplate). Some accessories are offered as spares (products that can be ordered separately). These spares might be ordered as replacements, supplements to the current product, or backup spare parts. Configurable accessories are ordered as part of a hardware appliance configuration in Cisco Commerce. For example, an order can be placed for a Cisco Secure Email Appliance C395, and a country-specific power cord can be selected as part of the overall configuration. When an order is complete, the appliance and the cord will be shipped.

Tables 15 and 16 list spare and configurable accessories, respectively.

Table 15. Spare accessories

Cisco Secure Email accessories (spare)	
Product	**SKU**
Cable Management Arm for C240, C260 Rack Servers	UCSC-CMA2=
Content Sec x95 600GB 12G SAS 10K RPM SFF HDD	CCS-HDD-600GB10K=
C220 M5 Security Bezel	UCSC-BZL-C220M5=
Cisco Content Sec AC Power Supply 770W for x95 Appliance	CCS-PSU1-770AC=
10GBASE-SR SFP Module Product Family SFP10G	SFP-10G-SR=
1000BASE-SX SFP Transceiver Module, MMF, 850nm, DOM	GLC-SX-MMD=

Cisco Secure Email accessories (spare)	
Ball Bearing Rail Kit for C220 and C240 M4 and M5 Rack Servers	UCSC-RAILB-M4=

Table 16. Configurable accessories

Cisco Secure Email accessories	
Product	**SKU**
Content Sec 2.1 GHz 4110/85W 8C/11MB Cache/DDR4 2400MHz	CCS-CPU-4110D
Content Sec 2.1 GHz 4116/85W 12C/16.50MB Cache/DDR4 2400MHz	CCS-CPU-4116D
Content Sec 2.6 GHz 6126/125W 12C/19.25MB Cache/DDR4 2666MHz	CCS-CPU-6126D
Content Sec x95 600GB 12G SAS 10K RPM SFF HDD	CCS-HDD-600GB10K
Cisco Content Security Trusted Platform Module TPM 2.0	CCS-TPM2-002
C220 M5 Security Bezel	UCSC-BZL-C220M5
Content Sec x95 16GB DDR4-2666-MHz RDIMM/PC4-19200/Single Rank/x4/1.2v	CCS-MEM-16GB
Cisco Content Sec Quad Port 1G Copper PCI	CCS-PCIE-IRJ45
Cisco Content Sec SAS Modular Raid Controller 2GB Cache	CCS-MRAID-M5
Riser 1B incl 3 PCIe Slots (x8, x8, x8); All Slots from CPU1	CCS-PCI-1B-240M5
Cisco Content Sec AC Power Supply 770W for x95 Appliance	CCS-PSU1-770AC
Cisco Content Sec Power Supply Blanking Panel for x95	CCS-PSU-M5BLNK
Cisco Content Dual-Port 10G SFP+ NIC	CCS-PCIE-ID10GF
1000BASE-SX SFP Transceiver Module, MMF, 850nm, DOM	GLC-SX-MMD
10GBASE-SR SFP Module Product Family SFP10G	SFP-10G-SR
Power Cord, China AC Power Cord - 250V, 10A	CAB-250V-10A-CN
Power Cord, China SFS Power Cord - 250V, 10A	SFS-250V-10A-CN
Power Cord, C13 to C14 (Recessed Receptacle), 10A	CAB-C13-C14-AC
Power Cord, India SFS Power Cord - 250V, 10A	SFS-250V-10A-ID
Power Cord, Israel SFS Power Cord - 250V, 10A	SFS-250V-10A-IS
Power Cord, Australia 250VAC 10A 3112 Plug	CAB-9K10A-AU
Power Cord, EU 250VAC 10A CEE 7/7 Plug	CAB-9K10A-EU
Power Cord, Italy 250VAC 10A CEI 23-16/VII Plug	CAB-9K10A-IT

Cisco Secure Email accessories	
Power Cord, Switzerland 250VAC 10A MP232 Plug	CAB-9K10A-SW
Power Cord, UK 250VAC 10A BS1363 Plug (13 A Fuse)	CAB-9K10A-UK
Power Cord, North America 125VAC 13A NEMA 5-15 Plug	CAB-9K12A-NA
Power Cord, Japan 3PIN	CAB-JPN-3PIN
Power Cord, North America 200/240V 6A	CAB-N5K6A-NA
Power Cord, Argentina SFS Power Cord - 250V, 10A	SFS-250V-10A-AR
AC Power Cord, NEMA L6-20 - C13, 2M/6.5ft	CAB-AC-L620-C13
Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	CAB-C13-C14-2M
Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	CAB-C13-CBN
Power Cord, Brazil 250V, 10A	CAB-250V-10A-BR
Power Cord, Korea AC Power Cord, C13, 1.8M	CAB-AC-C13-KOR

FIPS-compliant products

Cisco Secure Email appliance offerings provide Federal Information Processing Standards (FIPS) Level I compliance through the software-based Cisco Common Crypto Module. A FIPS-compliant mode is selectable within the GUI of specific versions of the AsyncOS® operating system. Cisco Secure Email customers requiring FIPS Level I compliance should select from the following SKUs:

- ESA-C195-K9
- ESA-C395-K9
- ESA-C695-K9
- ESA-C695F-K9

Try and Buy (TAB) Cisco Secure Email Gateway Appliance

The Try and Buy (TAB) process for Cisco Secure Email products generally matches the standard Cisco Try and Buy process. Direct partners can select either Cisco or a distributor to fulfill the order. Indirect partners must select a distributor to fulfill the order. A distributor ordering on behalf of a partner selects itself to fulfill the order. Whoever places the order on Cisco (direct partner or distributor) must be enrolled in the TAB program using the Partner Program Enrollment (PPE) tool. Direct customers can order through the TAB process by going through their partner or Cisco sales team, but they must first be enrolled in the TAB program (C2A). After a customer is enrolled, the partner or Cisco sales team can create a nonstandard sale for the TAB order using the existing TAB process for direct customers (Figure 1).

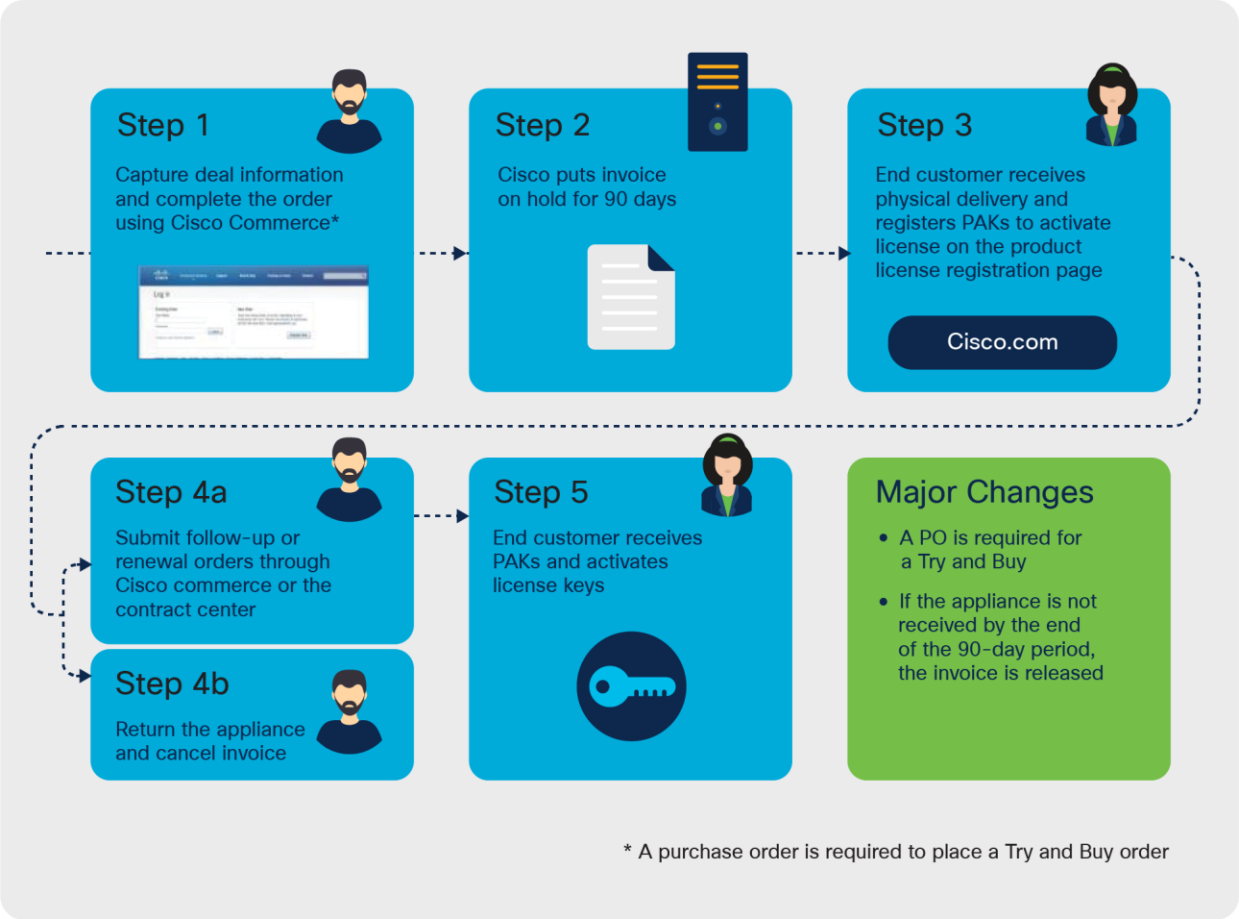


Figure 3.
Try and Buy: Initial order process (high-level workflow)

Figure 2 shows a sample order.

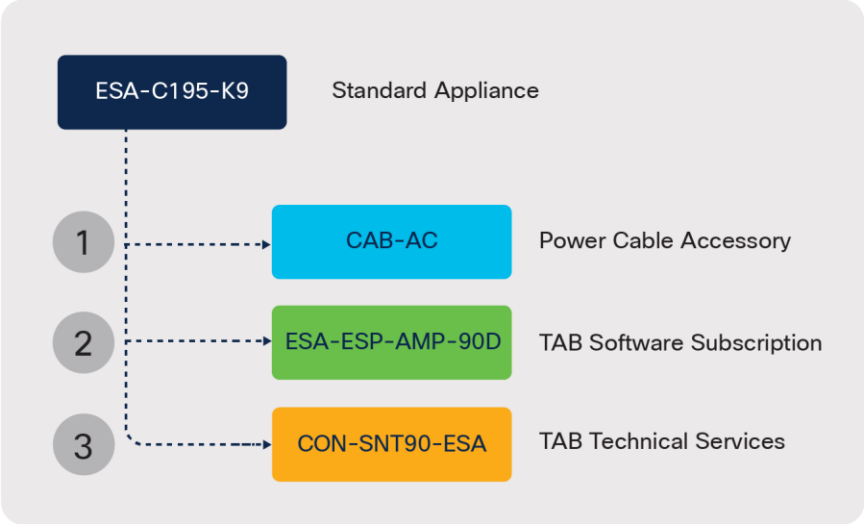


Figure 4.
Try and Buy offering for Cisco Secure Email

Three Items are ordered:

1. Standard hardware product and power cable accessories: The Try and Buy hardware selected should be the same model as the hardware that the customer expects to run in their production deployment.
2. One Try and Buy software subscription SKU. (The SKU options are listed in Table 17).
3. The associated Try and Buy technical services SKU.

Table 17. Try and Buy software subscription SKUs

Try and Buy SKU	Description
ESA-ESP-AMP-90D	Cisco Secure Email Advantage Bundle (AS+AV+OF_ENC+DLP+Malware Defense+GSU) 90 days license
SMA-EMG-90D	Email Management Software Bundle 90-day license

Note: The TAB software subscription and technical services SKUs can be ordered only as part of a bundle with standard hardware.

Post order process

If an evaluation license is ordered through a distributor, the distributor drop-ships the order. The order is shipped to the customer and includes both the hardware and a physical license PAK.

Note: Under the full-term or follow-up license ordering process, the customer receives the PAK by e-delivery.

This PAK is entered by the customer in the SWIFT tool as part of the standard license activation process. At the time of the order, the invoice for the hardware and licenses is put on hold for 90 days. When activated, the license remains activated for 90 days.

End of evaluation

After this 90-day period, the customer must either keep the hardware unit and purchase a 1-, 3-, or 5-year license using the standard ordering process or return the hardware using the standard Cisco return process. If the hardware is not returned at the end of the evaluation period, the invoice is released to the customer for payment.

For more details regarding the Try and Buy process, including enrollment, ordering, and fulfillment, please visit: https://www.cisco.com/c/en/us/partners/promotions/try-buy-program.html.

For support with Try and Buy, contact dlp-support@cisco.com or the respective account manager or Cisco sales team.

Understanding the ordering process

There are four main ordering processes for Cisco Secure Email offerings on the Cisco Price List:

- First-time orders of hardware appliances and software feature licenses
- Renewal orders that include both hardware appliances and software feature licenses
- Renewal orders of software feature licenses only
- Follow-up orders of software feature licenses to add features or user counts to an appliance or deployment of appliances

The following sections provide general information about the Cisco ordering process and explain the step-by-step processes for ordering under each of these four ordering scenarios. (See Figures 3 and 4).

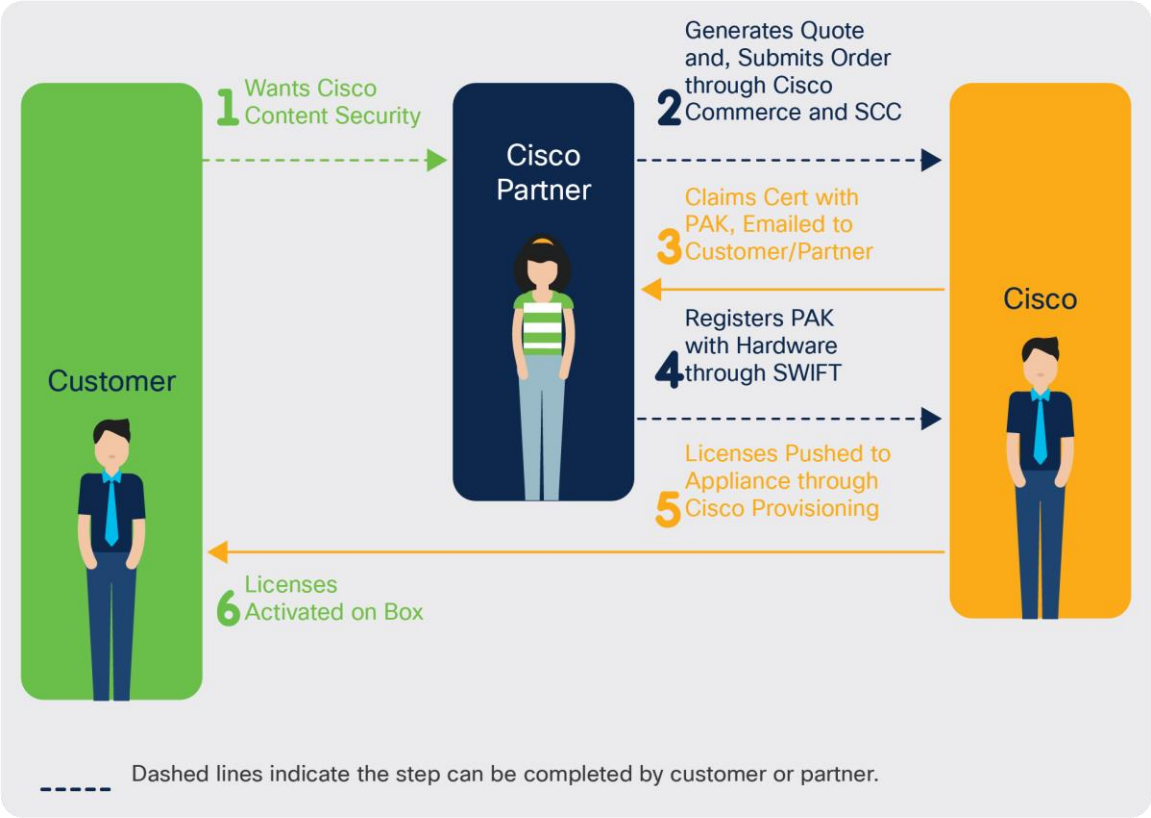


Figure 5.
High-level summary of a transaction

High-level summary of a Cisco Secure Email Appliance price list transaction

Table 18. Cisco Commerce versus Cisco Service Contract Center

Cisco Commerce Appliances with Software and Technical Services	Cisco Contract Center Software Renewals and Contract Management	
• Quote • Order • Configure • Deal registration	• Quoting and ordering: Follow-up and renewal of software subscription licenses and technical services • Contract management	
	Cisco Commerce	**Cisco Service Contract Center**
Initial purchase of Cisco Secure Email appliances, software, and technical services	Yes	No
Add-on additional licenses	Yes	Yes
Add-on additional appliances	Yes	No
Renewal of current licenses	No	Yes
Renewal of additional licenses	No	Yes
Renewal with additional licenses and purchase of additional appliances	Yes (application)	Yes (renewal and licenses)
Search and manage contracts contract management actions	No	Yes

Cisco Commerce

Cisco Commerce is the primary tool used for ordering Cisco Secure Email products offered on the Cisco Price List. Three main steps are involved in creating an order in Cisco Commerce:

Creating a quick quote

Converting a quote to an order

Submitting an order

Figure 4 shows the steps that a partner takes in the purchase and delivery of an order.

Figure 6.
Initial purchase of appliances, software, and technical services

1) Partner adds appliances, software, and technical services to configuration.
2) Partner creates a deal or quick quote, depending on whether the customer is requesting promotion pricing, special pricing, or standard pricing.
3) Partner can configure items in the Deal or Quick Quote space or import a previously created configuration.
4) Partner shares the quote or deal with the account manager for approval, unless the standard contractual pricing is used.
5) Partner converts the quote to an order or creates an order from a deal ID. Within the order space, the partner selects the contract-generation option and other preferences such as shipping and delivery.
6) Partner submits the order to complete the process.

Cisco Service Contract Center

The Cisco Service Contract Center is the primary tool used for ordering services, ordering follow-up software subscription licenses, and processing renewals of Cisco Secure Email offerings available on the Cisco Price List. Three main steps are involved in creating an order in the Service Contract Center: creating a quick quote, validating the quote, and submitting an order.

Partners use the standard quoting process, while distributors have the option of using the standard or quick quote functionality to create a quote. Partners and distributors validate and save a quote after all software subscription licenses and services have been added.

Ordering renewals is possible only in the Cisco Service Contract Center (see Figure 5). The new Cisco Secure Email offerings have undergone a change in pricing: Hardware is less expensive, and software is more expensive than the IronPort hardware and software. The combined price for new orders is the same, but renewals will require a nonstandard discount to keep the former software price parity. To support the first renewal during the integration, Cisco is providing a high-touch support model: Cisco places the quote in the Service Contract Center and passes it to the partner or distributor to place the order. Partners or distributors may also choose to process their own quote after an order service agreement is created and the deal ID is approved. They can then raise a support case to apply the discount before ordering.

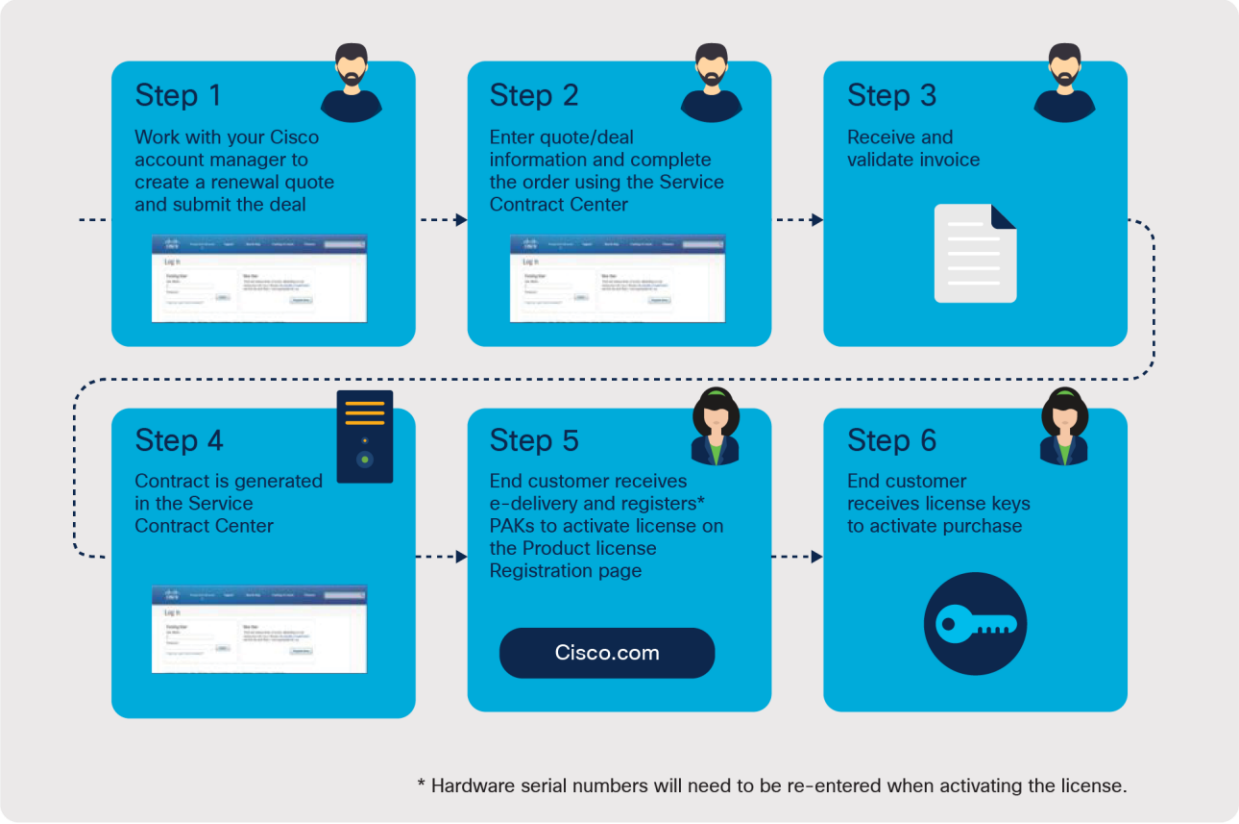


Figure 7.
Renew software and service subscriptions (high-level workflow)

Cisco Software Fulfillment and Infrastructure Technology (SWIFT) tool

The Cisco Software Fulfillment and Infrastructure Technology (SWIFT) tool is a framework used for the entitlement and fulfillment of Cisco software licenses. Customers and partners use the tool for customer data entry and the activation of software subscription licenses. Customers and partners who successfully place an order for a software subscription will receive a claim certificate with a Product Activation Key (PAK), which is entered in the SWIFT tool to provision licenses and associate them with a customer's deployed appliances.

Placing an order

Quote-to-deployment process for Cisco Price List

Before submitting an order, partners and salespeople should understand the quote-to-deployment process for Cisco Secure Email products purchased through the Cisco Price List. Understanding this flow can help ensure the fastest possible processing of orders and deployment for the customer.

Additional resources

Additional resources and documentation regarding the new ordering processes and product and service offerings can be found at: https://www.cisco.com/c/en/us/products/security/index.html.

Understanding the Cisco Secure Email Cloud Gateway ordering process on the GPL

Summary

There are three main steps to order Cisco Secure Email Cloud Gateway offerings on the GPL:

1) Order an initial Cisco Secure Email Cloud Gateway subscription through Cisco Commerce. Be sure to submit the required email addresses for the contacts in the order.
2) A Cisco Secure Email Cloud Gateway operations staff member will activate the order. That person will reach out to the sales engineer to get any necessary information to complete the activation. If the sales engineer has not reached out, email ces-activations@cisco.com to follow up on the order.
3) The customer receives notification that the provisioning is complete.

Cisco Commerce

Cisco Commerce is the primary tool for ordering Cisco Secure Email Cloud Gateway offerings on the GPL (see Figure 8). The three main steps involved in creating an order in Cisco Commerce are: creating a quick quote, converting a quote to an order, and submitting an order.

To access Cisco Commerce, visit: https://www.cisco.com/go/ccw.

For Cisco Commerce training materials, visit: https://www.cisco.com/web/partners/events/commerce_workspace.html.

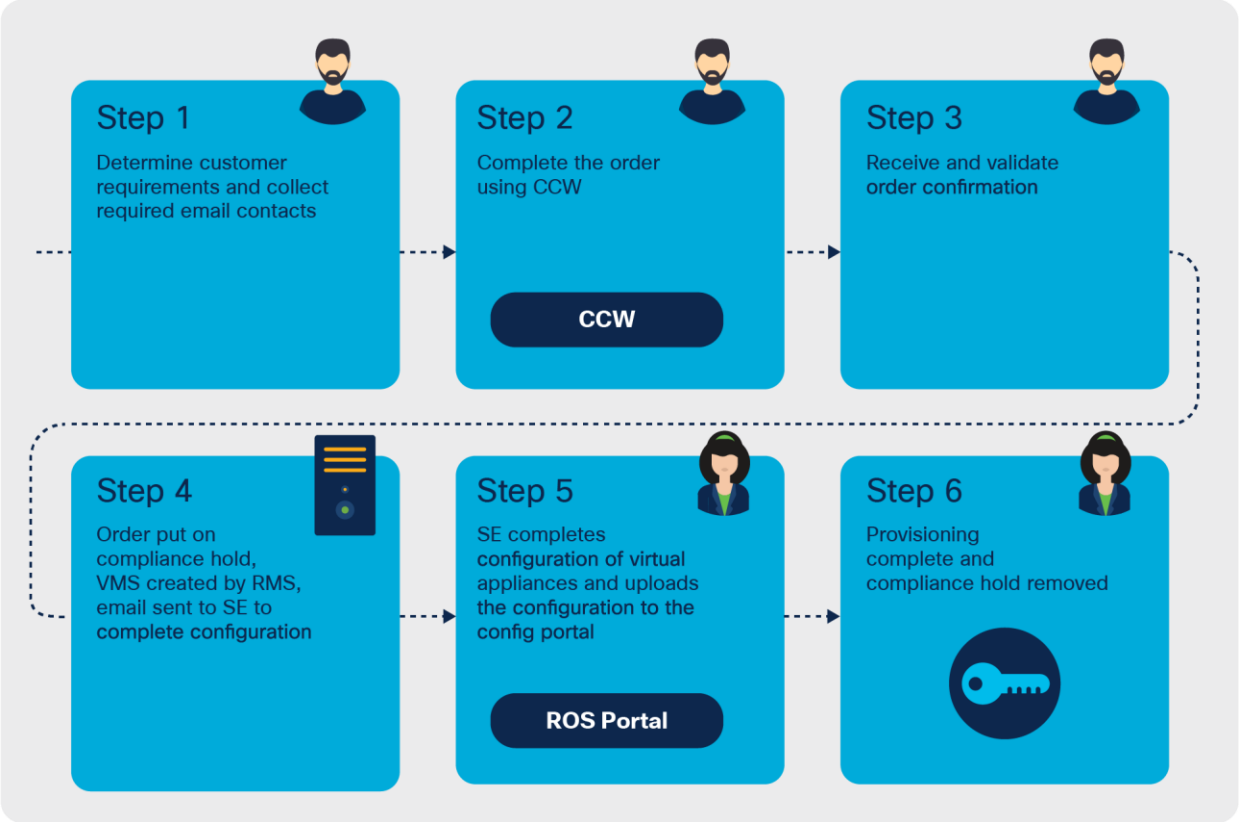


Figure 8.
Initial purchase of a Cisco Secure Email Cloud Gateway subscription

Note: All customers, whether they are new Cisco Secure Email Cloud Gateway customers or existing IronPort (pre-GPL) customers, **must purchase Cisco Secure Email Cloud Gateway on the GPL initially through Cisco Commerce**. For Cisco Secure Email Cloud Gateway renewals, orders booked through Cisco Commerce or GPL are processed in Cisco Commerce. **Cisco Secure Email Cloud Gateway should not be renewed through the Cisco Service Contract Center**.

Placing a Cisco Secure Email Cloud Gateway order on the GPL

Ordering process overview

New orders for Cisco Secure Email Cloud Gateway through the GPL must be submitted through Cisco Commerce.

During the ordering process in Cisco Commerce, the partner or customer must specify the email contact for the sales engineer who will complete the configuration of Cisco Secure Email Cloud Gateway for the customer. The sales engineer (**Required Email**) will receive a technical notification regarding the completion of the configuration.

As soon as the order is submitted, it is placed on a compliance hold. This allows the sales engineer or account manager (**Required Email**) to follow up with the customer (**Required Email**) to begin provisioning the service. A compliance hold is necessary because Cisco's Cisco Secure Email Cloud Gateway sales operations team requires that the configuration of the virtual appliances in the customer's Cisco Secure Email Cloud Gateway instance be complete before the order is processed. For lifting the Cisco Secure Email Cloud Gateway order off the compliance hold, it is critical that:

- A Cisco or partner sales engineer email address is associated with the order
- An end-user email address is associated with the order (do not submit an email alias)
- A Cisco account manager email address is associated with the order
- The sales engineer responds promptly to requests from a Cisco Secure Email Cloud Gateway service delivery manager for information necessary for activation

For more information on software licensing, visit Software Licensing Self Help Portal for Cisco Email and Web Security here.

Subscription changes and cancellations

Subscription changes

Changes to the product or an increase in licensing may be made at any time during the term of the subscription, or at renewal.

Change subscriptions (modify/renew/replace) follow the Cisco standard process, and can be done by:

- Issuing change subscription directly via Cisco Commerce Workplace, or
- Opening a case in Customer Service Hub

A Change-Subscription order can be created to reflect license or product changes, in order to share with the Cisco Secure Email Account Manager to review licensing, product, and term information, and then will be sent to the Cisco Secure Email business unit for approval.

Subscription cancellations

Subscription cancellation requests can be raised by:

- Issuing cancellation request via Cisco Commerce Workplace—click on "Manage Subscriptions" in the subscription information for active subscriptions
- Opening a case in Customer Service Hub

Renewals may be canceled up to 30 days before the start date of the new term. If the subscription is not canceled 30 days prior to the start of the new term, the subscription will automatically renew. Mid-term cancellations of subscriptions for credit are not allowed.

Appendices

Cisco Secure Email Gateway Appliance: Additional information

Encryption orders placed in Russia

Depending on the level of encryption associated with the ESA-ENC-LIC= license, this license and any bundles that incorporate it are treated differently for import classification into Russia, Kazakhstan, and Belarus. ESA-ESP-LIC=, ESA-ESO-LIC=, and ESA-ENC-LIC-K9= orders will initially be classified as category 3 (C3) and placed on order validation hold until a partner verifies that it has obtained the appropriate FSB import permit. Partners and customers who do not require encryption may alternatively purchase the ESA-DLP-LIC= (instead of ESA-ESO- LIC=) and may purchase the ESA-ESI-LIC= or ESA-DLP-LIC= (instead of ESA-ESP-LIC=). These orders will be classified as category 1 (C1) and are subject to immediate importation without an order validation hold.

Delivery mode

On the IronPort price list, the Delivery Mode solution was offered as part of a separate C390D-BUN-R- hardware appliance. Purchase of this SKU entitled the customer to both the hardware appliance and the associated Delivery Mode software license. The Delivery Mode functionality will now be offered as a separate software license that can be applied to the ESA-C380-K9 hardware unit. This license (ESA-DMODE-LIC=) is a fixed-price, perpetual license and will be associated to the standard email appliance through the same process as all other Email Security software licenses. As with the previous offering, no other Email Security software licenses (for example, ESA-ESP-LIC=) may be activated on an appliance that has an activated DMODE license.

China hardware

Due to certain importation requirements, Cisco 390 and 690 Series appliances manufactured specifically for customers in China were offered. These China-specific appliances were ordered using the SKUs with an "-NT" nomenclature. These products are no longer available. All of the 380 and 680 appliances have received the China Compulsory Certificate mark, commonly known as the CCC mark, which satisfies China's compliance requirement for products to be imported, sold, and used in the Chinese market.

Cisco does not recommend that Content Security appliances be sold to service providers in China.

Fiber hardware

For customers deploying Cisco Email and Security Management appliances with their fiber networks, 1 Gigabit Ethernet and 10 Gigabit Ethernet fiber-interface-configured appliances are available when you order the corresponding SKU ESA-C695F-K9 and SMA-M695F-K9. ESA-C695-K9 and SMA M695-K9 are configured with copper interfaces.

Table 19 lists the fiber SKUs that will be automatically configured with the associated fiber products

Table 19. Fiber-configured Email and Security Appliances

Appliance type	Appliance name	Description
Cisco Secure Email	ESA-C695F-K9	ESA C695 Cisco Secure Email Gateway Appliance with 1 GE or 10 GE Fiber Interfaces
Cisco Security Management	SMA-M695F-K9	SMA M695 Security Management Appliance with 1 GE or 10GE Fiber Interfaces

Table 20. Fiber options for Email and Security Appliances

Configurable option	Description
GLC-SX-MMD	1000BASE-SX SFP Transceiver Module, MMF, 850nm, DOM
SFP-10G-SR	10GBASE-SR SFP Module Product Family SFP10G

Email Security support

Support request for Cisco Secure Email should follow regular TAC process.

TAC email: tac@cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-736692-20 12/22