Symantec Encryption Licensing Guide

December 7, 2017

Contents

Chapter 1: Product Overview

Symantec's encryption portfolio provides flexible data protection through a range of offerings including endpoint, file and folder, and email encryption. Integration with Symantec Data Loss Prevention delivers added protection by automatically encrypting sensitive data being moved onto removable media devices or residing in emails and files.
Robust management features include individual and group key management, automated policy controls, and out-of- the-box, compliance-based reporting.

Endpoint Encryption
Protection for laptops, desktops, servers, and removable media from loss or theft.

Email Encryption
Protection for email at various stages in a message's journey.

File and Folder Encryption
Protection for batch transfers, collaboration and file sharing in an organization, and in the cloud.

Currently, our solution is managed by different management servers depending on the needs of the customer. See below to better understand which products fall under which platform.

PLEASE NOTE: Starting October 6, 2014, there was a large shift in license entitlements and all encryption products, with the exception of PGP Command Line, include their respective management platform with their license. Symantec Endpoint Encryption also includes entitlements for Symantec Drive Encryption and Symantec Encryption Management Server. See Chapter 5 for more information on the October 2014 migrations.

Managed by Symantec Endpoint Encryption Management Server (SEE-MS)

Endpoint Encryption	
Endpoint Encryption	•Consolidated endpoint encryption solution to secure data on laptops, desktops, servers and removable media. •Includes entitlements for Drive Encryption and Symantec Encryption Management Server

Managed by Symantec Encryption Management Server (SEMS)

Endpoint Encryption	
Drive Encryption	• Endpoint Encryption for laptops and desktops. • NOTE: Cannot be purchased individually; Drive Encryption and Symantec Encryption Management Server are included in the Endpoint Encryption license.
Email Encryption	
Desktop Email Encryption	•Secure outbound email immediately from the user's laptop/desktop. Email is encrypted on internal mail servers as well.
Gateway Email Encryption	•Email encryption at the gateway without the need for client software.
Mobile Encryption for iOS	•Email encryption for iOS devices to both send and receive messages (encryption and decryption). •NOTE: PGP Viewer for Android is available for free from the Google Play Store but cannot send/reply to email (decryption only).
File and Folder Encryption	
File Share Encryption	•Policy-enforced file encryption for collaborating teams, including Dropbox integration •NOTE: File Viewer for iOS is available for free via Apple iTunes Store.
PGP Command Line	•Automated encryption for file transfer and data-processing applications •NOTE: PGP Command Line SKU does **not include management**. Key Management Server and Client Access are licensed **separately** for this product.

Stand-alone Capability

Customers looking to run disk encryption without the use of a deployment/management server should use Drive Encryption. At this time, Endpoint Encryption v11.x is only meant to be operated using a deployment server with management capability.

Chapter 2: General Encryption Licensing

Step 1: Determine License Type

License Type	Description
Perpetual	• Grant customers the right to use product version indefinitely
Subscription	• Grant a limited-time right to use the software • Renew at end of each term, otherwise the software must be uninstalled

Step 2: Determine Product Sub-Type

Term Type	Description
Initial	• Available in one year, two year, and three year options
Additional User	• Available in one year, two year, and three year options
Renewal	• Available in one year option

Step 3: Determine License Quantity

Products	Meter	Meter Description
Endpoint Encryption		
Endpoint Encryption	Device	• # of laptops/desktops/servers
Email Encryption		
Desktop Email Encryption Gateway Email Encryption Mobile Encryption for iOS	User	• # of users who can encrypt email
File and Folder Encryption		
File Share Encryption	User	• # of users who can encrypt files
PGP Command Line	CPU	• # of CPU Cores on each server • See “Chapter 3: PGP Command Line Licensing”
Command Line Management		
Key Management Server	Server	• # of servers communicating with PGP Command Line
Client Access and CLI API Client Access and C++ API	Device	• Total # of PGP Command Line licenses

Step 4: Determine Pricing for Selected Buying Options

Prices shown below are Corporate USD pricing for single Perpetual License. Note, from Sept 2017 Encryption products need to be purchased with maintenance (the "Support & Maintenance Pricing" tab of the Corporate Price Book notes the maintenance SKU of "SW-TIER-1X":)

Product	MSRP (USD)
Endpoint Encryption	$150 Per Device
Desktop Email Encryption	$139 Per User
Gateway Email Encryption	$40 Per User
Mobile Encryption for IOS	$78 Per User
File, Folder, and Cloud Encryption	
File Share Encryption	$139 Per User
PGP Command Line	$7,119 for 2 CPU cores See Chapter 3 for more specific information about PGP Command Line licensing

Chapter 3: PGP Command Line Licensing

Note: PGP Command Line may be managed via Key Management Server with appropriate Client Access licenses. The most common use case for PGP Command Line is for the unmanaged use case.

Step 1: Determine # of CPU cores

The number of CPU cores on the machine which will run PGP Command Line determines which PGP Command Line SKU to license. The number of CPUs on the machine running PGP Command Line may not exceed the number of CPU cores licensed. A dual-core processor is considered a 2 CPU machine, while a quad-core processor is considered a 4 CPU machine.

- CPUs partitioned via hyper-threading do not require additional licenses beyond the count of the physical CPU cores.
- In virtualized deployments, the quantity of CPUs is determined by the actual CPUs accessed by PGP Command Line. If a core is inaccessible by PGP Command Line due to a virtual machine or logical partitioning (LPAR) configuration, the CPU/core does not need to be licensed.

Step 2: Rules on Stacking or Splitting CPU Licenses

- There is the ability to stack CPU licenses. If a customer already has a “2 CPU license” and upgrades their system to a 4-CPU system, the customer may purchase an additional "2 CPU license“ to reach the required 4 CPU licenses (equivalent of 2 CPU license + 2 CPU license = 4 CPU license)
- However, customers **cannot** break up CPU licenses. For example, a customer could not use a single “8 CPU license” for two 4-CPU systems. To cover two 4-CPU machines would require two 4-CPU licenses.

Again, Symantec PGP Command Line continues to be priced per CPU core of the server which will have Symantec PGP Command Line installed on it.

Example

The customer wants new perpetual license for two servers with 8 CPU cores and 25 servers with 2 CPU cores on which he wants to run Symantec PGP Command Line.

The SKUs to license would be:

2 licenses of ENC-CMD-NEW-8 Command Line Powered By PGP Technology, License, 8 CPUs Per Server

25 licenses of ENC-CMD-NEW-2 Command Line Powered By PGP Technology, License, 2 CPUs Per Server

Other PGP Command Line Licensing Considerations

Licensing For Redundancy

Customers may install additional “non-production” copies of software for redundancy, staging and testing purposes at no-cost provided they own at least an equal number of production licenses. These “non-production” licenses may only be used when their production counterparts are not in use (that is, the production and non-production licenses may not be used simultaneously).

1-Key License

There are a number of restrictions for using this license, and a customer’s planned usage must comply with all of the following restrictions:

- use no more than one asymmetric Key pair (excluding the Additional Decryption Key “ADK” as described in the Documentation)
- use PGP Command Line to (i) send files to and receive files from one Server which uses PGP Command Line and is not subject to the “1 Key” limitation; (ii) sign or decrypt a file with Your private key; (iii) encrypt a file or verify a signature on a file with a public key from one Server which uses PGP Command Line and is not subject to the “1 Key” limitation; and (iv) create self-decrypting archives.

For purposes of this section, “Key” means either or both components of a public/private cryptographic key pair.

Mainframe Platform Support

PGP Command Line Mainframe (for IBM System i and IBM System z platforms), for license and maintenance/support, are available directly from Townsend Security. New sales opportunities can be registered via Townsend's dedicated partner portal: https://www.townsendsecurity.com/product/pgp-enterprise-encryption-IBM . Townsend will respond within one business day. If a more immediate response or direct support is needed, contact:

Robbn Miller, Partner Manager
robbn.miller@townsendsecurity.com
360-359-4405

Managing PGP Command Line (Optional Add-On)

For keys to be managed with Key Management Server, customers need licenses for Key Management Server and appropriate Client Access Licenses. Key Management Server comes with Encryption Management Server and a license key to use within Encryption Management Server to unlock this capability.

Step 1: Determine the # of Client Access Licenses Needed

The number of client access licenses should match the number of PGP Command Line licenses. The licenses may be for:

- Symantec PGP Key Management Client Access and CLI API – Command Line Interface (most common use case)
- Symantec PGP Key Management Client Access and C++ API – Software Development Kit (SDK)

Step 2: Determine the # of Key Management Server Licenses Needed

The number of Key Management Server licenses is determined by how many servers are communicating with PGP Command Line. For most customers, this will only be one server, however some customers may have multiple, often for redundancy.

Chapter 4: Trials and Evaluations

Evaluation keys and links to trialware for Symantec Encryption products are posted in the "Internal Tools" section of the Encryption page on SalesCentral[1]. If our prospective customer needs to extend their evaluation time, the Extended Evaluation Period Keys are posted on the same SalesCentral document.

Please note, Symantec Endpoint Encryption (SEE) does **not** require a license key.

Chapter 5: License Migrations Summaries from Oct. 2014

Following the acquisition of PGP and GuardianEdge in June 2010, Symantec maintained two distinct endpoint encryption platforms. In October 2014, Symantec combined these two solutions into one best-of-breed offering that included endpoint and removable media encryption *with* management.

With this move, Symantec greatly simplified the licensing process, rolling up many products previously licensed separately into a single license and entitling customers to the following:

Symantec Endpoint Encryption Migrations
PLEASE NOTE: More detailed license migration information can be found here
http://www.symantec.com/docs/HOWTO101492

Customers current on maintenance of the below product categories were automatically migrated to Symantec Endpoint Encryption on a 1:1 ratio:

- Symantec Drive Encryption
- Symantec Drive Encryption with Encryption Management Server Limited
- Symantec Drive Encryption with Encryption Management Server
- Symantec Drive Encryption FlexChoice with Encryption Server Limited
- Symantec Drive Encryption FlexChoice with Encryption Server
- Symantec Drive and Removable Storage Encryption FlexChoice with Encryption Server Limited
- Symantec Endpoint Encryption Removable Storage Edition
- Symantec CAPS Activation Package for Whole Disk Encryption
- Symantec PGP Universal Server and Whole Disk Encryption for Servers

[1] https://syminfo.symantec.com/content/salescentral/SalesCentralHome/products-services/information-protection/encryption.html

Symantec Product Bundle Migrations

PLEASE NOTE: More detailed license migration information can be found here http://www.symantec.com/docs/HOWTO101493

Previously, Symantec offered bundle licenses that included multiple encryption products. In October 2014, customers with current maintenance of these licenses saw their bundles broken into their respective component products and Symantec Encryption Management Server was included with each new component license entitlement.

Old License	New License Entitlement
Symantec Encryption Desktop Corporate	Symantec Endpoint Encryption
	Symantec Desktop Email Encryption
	Symantec File Share Encryption

Old License	New License Entitlement
Symantec Encryption Desktop Professional	Symantec Endpoint Encryption
	Symantec Desktop Email Encryption

Old License	New License Entitlement
Symantec Encryption Desktop Storage	Symantec Endpoint Encryption
	Symantec File Share Encryption

Chapter 6: Additional Resources

PartnerNet: https://www.symantec.com/partners

Sales Central Encryption page: https://syminfo.symantec.com/content/salescentral/SalesCentralHome/products-services/information-protection/encryption.html

Chapter 7: Key Contacts

If you are a Symantec Partner, please contact your Symantec Partner Account Manager with any questions.

If you are a Symantec employee, contact Sales Support (contact details below) or the Encryption Product Management Team using the distribution list **DL-SYMC-Encryption-Ask-PM**.

Americas: salessupportamericas@symantec.com
EMEA: https://symantecb2b.my.salesforce.com/_ui/core/chatter/groups/GroupProfilePage?g=0F950000000L1Sc
APJ:
- Japan: xrm-slssuptjp@symantec.com
- ASEAN: salessupportasr@symantec.com
- Korea: XRM-SLSSPTKOREA@symantec.com
- Pacific: salessupportpac@symantec.com
- India: salessupportindia@symantec.com
- Greater China Region: Salessupportgcr@symantec.com