COMMVAULT®

Endpoint SaaS Encryption

OVERVIEW

Enterprise security, governance and compliance is a major concern to most organizations, especially in this connected world where personal devices are used to access corporate data, which is frequently shared using free public file sharing services.

Commvault software provides comprehensive enterprise class security including full multi-tenancy support across all of its solutions such as enterprise data protection and recovery, endpoint protection, file sharing, as well as data and application archiving, ensuring that your organization's data is secure, private and protected whether hosted on premises or in the cloud.

Data encryption provides the ability to encrypt data both for transmission over non-secure networks and for storage on media. The flexibility of key management schemes makes data encryption useful in a wide variety of configurations. Commvault supports the Key Management Interoperability Protocol (KMIP), which is a communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server.

ENCRYPTION METHODS

As a data management company, Commvault understands that securing data is not only prominent on back-end storage, but also during data transfer operations. Commvault provides the ability to encrypt data both for transmission over non-secure networks (in transit) and for storage on media (at rest). The highest level of encryption of 256-bit AES is offered in order to provide enterprise grade security.

ENCRYPTION KEY GENERATION AND SECURITY

Encryption keys are generated using the CTR_DRBG random number generator. Various random OS-supplied data is used to provide a dynamic seed for the random number generator. Keys are generated using a random 128-bit or 256-bit data encryption key (DEK) for every data chunk/archive file and initial vectors (IV) for CBC chaining during data encryption.

Encryption keys are encrypted using the AES Key Wrap Specification, and stored securely within the database.

A third party key management server can also be implemented to allow a customer to create their own custom encryption key, and store this within the key management server. The key management server and custom encryption key are managed by the customer.

See below for further details into the different encryption key management options:

	COMMVAULT	THIRD PARTY KEY MANAGEMENT SERVER
Location	CommServe® database	Onsite – Safenet, Vormetric DSM Cloud - AWS
Details	CommServe acts as a key management server Key securely stored in the CommServe database with CRC32 embedded	Key securely stored using a third party key management server Customer managed encryption key
Strengths	No additional management of an external key management server No additional cost of an external key management server No connectivity reliance on an external key management server for data protection or restore operations	Data and encryption key stored in separate entities (may provide additional legal protection) Customer controlled data protection and restore operations
Considerations	Both data and encryption key stored within a single entity	Additional management of an external key management server Additional cost of an external key management server Cannot conduct data protection or restore operations without connectivity to the key management server

DATA ENCRYPTION ALGORITHMS

The following table lists supported algorithms and key lengths that are available to use for encryption. All algorithms meet the U.S. National Institute of Standards and Technology (NIST) Advanced Encryption standard.

CIPHER	DETAILS	BLOCK SIZE	KEY LENGTH OPTIONS
Blowfish	• Symmetric Key Block Cipher • Fast (fastest of the ciphers supported) • Secure	64 bit	128, 256 bit
GOST	• Symmetric Key Block Cipher	64 bit	256 bit
AES (Advanced Encryption Standard) or Rijndael	• Symmetric Key Block Cipher • Fast • Secure • Winner of the Advanced Encryption Standard Content • Adopted as the Government Standard (Only cipher approved by the National Security Agency to be used for top secret information.) • AES 256 - CBC mode	128 bit	128, 256 bit
Twofish	• Symmetric Key Block Cipher • Fast • Secure • Not standardized • Finalist in the Advanced Encryption Standard Content	128 bit	128, 256 bit
3-DES (Triple Data Encryption Standard)	• Symmetric Key Block Cipher • Slow • May be susceptible to certain attacks	64 bit	192 bit

PRIVACY

Commvault understands that a company's data can be sensitive, and may need to be kept confidential from external vendors. The privacy feature is enabled by default, ensuring only the company's admin is able to view and control their company's protected data. This prevents Commvault's MSP admin from viewing or accessing a company's sensitive data.

The privacy feature allows for the following behavior:

- Only the customer admin may lock and unlock a client
- Only the customer admin may access data protected on a client, for example, perform Browse and Restore, Find, and Reference Copy operations
- Only the customer admin may add or remove client owners
- Only the customer admin may change their own user properties

SUMMARY

In a highly connected world where personal devices are accessing corporate data and using free public file sharing services, data security, governance and compliance are a major and ever growing concern of most organizations. Data security and role based access is of the highest priority at Commvault, allowing our customers to access the power of their data, no matter where it resides, with full confidence that it is safe and protected.

Commvault endpoint protection solutions provide comprehensive enterprise-class security whether the data is hosted onsite or in the cloud. For more information, please visit commvault.com/endpoint.

COMMVAULT

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM