FREQUENTLY
ASKED
QUESTIONS

FAQs

SMARTENCRYPT™
by rhipe

FILE ENCRYPTION

How does SmartEncrypt secure my files?

Files are encrypted with industry standard AES 256-bit encryption, using the company created encryption keys. Files encrypted with SmartEncrypt cannot be viewed without the correct encryption key. To access an encrypted file, a user logs in and once successfully authenticated, their device automatically receives the encryption key to open the encrypted file.

How does the file encryption and decryption process work?

SmartEncrypt encrypts and decrypts your data on-the-fly. There is no need for bulk decryption when working with encrypted files as users can simply double click on encrypted files and the client software will automatically decrypt before opening, or open them directly in the associated application with no change in user experience. Files will automatically re-encrypt even if edited outside encrypted folder locations, now file is automatically encrypted again when any changes are saved so data is protected without worrying about the cryptographic process behind it.

How do I open encrypted files?

After successfully logging into the SmartEncrypt software, you can open your encrypted files the same way you would open any other file – double-click it when browsing, open from your recent files, or just open it from within the application. SmartEncrypt automatically sends the necessary encryption keys to your device so **no manual decryption is needed – ever.**

How do I encrypt my files?

Once successfully logged into the SmartEncrypt software, the user simply selects and right-clicks the files and folders and selects 'Encrypt' from the SmartEncrypt context menu and then click the Start button.

How does the software decrypt files without any input?

Our Microsoft Windows client uses a driver that intercepts open requests and checks if the file is encrypted. If it is encrypted, the client software decrypts the file and then passes it through to the application opening the file. This process takes just milliseconds for typical Office documents.

The format of my files looks normal, so are they actually encrypted?

This is part of the magic SmartEncrypt delivers. We make your encrypted files as easy to work with as possible and unlike other complicated encryption products, we do not rename or change the file type or file extensions. Once the user logs out of the SmartEncrypt software, they will not be able to open encrypted files and can only decrypt them when the user is logged in.

Can multiple users access the encrypted data?

Yes, the software has been designed for multi-user environments. Files are encrypted with company encryption keys and these keys are assigned to users and/or groups of users where the subscription permits, making the sharing of encryption keys simple among users in the organisation.

What if a user leaves the company with encrypted files?

When an employee or contractor leaves the organisation, their access can be disabled in the Management Console so that they cannot log in, preventing them from receiving the encryption keys and decrypting files. Data remains encrypted and therefore unusable to them.

FAQs

ENCRYPTED DATA ACCESS

Offline access to encrypted data

Users can be granted offline access to enable logging in while travelling. Offline access is a privilege that is controlled by the administrator and can be configured to expire after a specified period. Offline access temporarily stores and encrypts the encryption keys locally with a user-generated PIN and automatically removes them on expiry. Users must log in to the software locally using their PIN before offline access to encrypted files is granted.

What happens if I forget my password?

SmartEncrypt is designed for businesses of all sizes, and with that in mind, we understand passwords sometimes get forgotten. Passwords are not the encryption keys, so if the password is forgotten, it can easily be reset by the user via the client software.

Does SmartEncrypt have access to our data?

We do not have access to any customer data. SmartEncrypt is data protection as a service rather than a cloud storage provider. We never transmit or store your files so we can never access your data. You have full control of your data and we only pass the encryption keys to your device on successful login authentication.

Do you have zero knowledge?

Zero knowledge refers to a vendor having access to encrypted data. Zero knowledge applies to cloud providers that host data or service providers that transmit data (i.e. take possession of your data).

Zero knowledge is not applicable to SmartEncrypt because at no point do we store, transmit or take possession of your data. Your data is always kept in your own environment; therefore, **we can never access or view your data.**

Do you have any 'backdoors' to access data?

No, we do not have any backdoors and because we create and store our customer encryption keys, we have no reason to create a backdoor. We do manage and distribute your encryption keys, it is the vital technology enabling a company controlled multi-user encryption product to function, **however, we don't possess your data, so a backdoor is of absolutely no value to us.**

FA
Qs

ENCRYPTION KEYS

How are the encryption keys created?

Encryption keys use AES 256-bit encryption and are 32 bytes in size and are controlled by the company administrator. They are not user passwords. Administrators create symmetric encryption keys via the web-based Management Console using entropy from an OpenSSL pseudo-random byte generator.

Where are the encryption keys stored?

We secure, store and tightly control access to encryption keys in *HashiCorp* vaults. The Vault encrypts the key prior to writing to persistent storage, so gaining access to the raw storage doesn't enable access to your encryption keys. These *HashiCorp* vaults are hosted and secured in a tightly controlled Azure environment, which is also backed-up and configured for high availability.

Are the encryption keys stored on the device?

Encryption keys are not saved to disk or stored locally unless the user has been granted offline access, users are required to be online to log in and receive the encryption keys from the server.

How does the Key transfer work?

Keys are transferred from the key vault to the client software via an encrypted OpenSSL TLS 1.2 tunnel. If the client detects an issue with the tunnel, it will not proceed with the transmission of the encryption key.

How is the login process secured?

Client username and password are transmitted via an OpenSSL Secure TLS 1.2 tunnel. On successful authentication, an encrypted reply token is generated and transmitted via the OpenSSL Secure TLS 1.2 tunnel back to the device.

Can users create their own encryption keys?

No. Only administrators can create encryption keys. Having company-generated encryption keys guarantees that IT or an organisation's management always have access to encrypted data.

FA
Qs

SECURITY

How secure is the software?

SmartEncrypt uses the AES encryption algorithm with a 32-byte key. This is commonly referred to as AES-256. In order to become the Advanced Encryption Standard (AES), the current algorithm currently underwent intense scrutiny from cryptographers around the globe and is now the most widely used symmetric encryption algorithm.

How is the Management Console secured?

The Management Console is protected against SQL Injection, Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks. Browser connections to the console are secured using HTTP and SSL/TLS (HTTPS), ensuring that any information exchange between the browser and Management Console is encrypted. Encrypted cookies are used to save both browser sessions and user preferences, as well as protect you from cookie poisoning attacks.

How is communication secured between the client software and Management Console?

OpenSSL Secure TLS 1.2 tunnel and encrypted JSON Web Tokens (JWT) – an industry standard RFC 7519 method, represents claims securely between the client and Management Console. JWT verification includes header check and validation before acceptance, with time-based expiry of encrypted tokens. Our JWT token life cycle is short-lived, severely limiting the feasibility of timing-based attacks. Once a token expires, a new token is created.

Additionally, communication between the Management Console and the SmartEncrypt client is signed with JWS digital signatures, preventing man-in-the-middle changes to policies as non-signed polices are ignored.

How are passwords protected?

Passwords are encrypted using *bcrypt,* an algorithm based on the Blowfish cipher. Bcrypt is a password hashing function which incorporates a salt value to protect against rainbow table attacks. It has a significant advantage over a simply salted SHA-256 hash as it performs key strengthening on passwords. Key strengthening increases the resource cost to attackers when attempting to guess a password, rendering brute force attacks incredibly time and resource expensive. Simply put, once a password has been created, not even we can decrypt or read them.

Does SmartEncrypt support Single Sign-On?

Single Sign-On can be configured for use with the SmartEncrypt desktop client and Azure AD. This will allow users to login to their device and not be prompted for a username and password for SmartEncrypt to decrypt the files. Please note that even with Single Sign-On enabled, SmartEncrypt administrators will still need to sign in to the SmartEncrypt Management Console with their SmartEncrypt console credentials.

FA
Qs

How secure is your infrastructure?

SmartEncrypt utilises Azure for hosting the back-end, the Management Console and the encryption key vaults.

Azure meets a range of compliance requirements for ensuring both the physical and cyber security of our environment, including:

- ISO 9001, 27001, 27017, 27018
- PCI DSS Level 1
- SOC 1, 2 & 3
- IRAP
- G-Cloud [UK]
- C5 [Germany]

For more information on Azure compliance please visit the Azure compliance page.

Our Azure segmented multi-layer, multi-region, redundant environment access is highly restricted. Access control and strong password policies prevent login from unauthorised locations that may compromise the system security. Access to the system is limited to restricted IP addresses, with forced Two-Factor Authentication (2FA). Our environment is backed-up, patched, has a high level of network security with tightly controlled Role-Based-Access-Control (RBAC) and has undergone complete penetration testing during its development, with continued penetration testing to be carried out on an on-going basis.

PRIVACY

What user data does SmartEncrypt store?

All user data stored on our servers is highly secure and meets compliance requirements. SmartEncrypt does not collect or store any sensitive personal information (PII), and the data that is collected is the minimum required to offer the SmartEncrypt Software-as-a-Service.

We store a small amount of information for each user, group and company which is necessary to authenticate users at login. Details include, but are not limited to:

- First and last name, email address and country

Data collected from devices is for security and auditing purposes only:

- IP addresses used to login (IP address & date & time)
- Devices used to login (device name, date & time), history of decryption and encryption events (audit logs such as files names and times).

FAQs

SHARING FILES

How do a I share an encrypted file?

The SmartEncrypt 'Protect and Share' feature enables users to share an encrypted file with someone outside of the organisation. The feature creates a new copy of the encrypted file as a PIN-protected encrypted HTML file, which can then be securely sent outside the organsation.

The HTML file can be emailed or shared via any cloud file sharing service or portable device. Once the recipient receives the file, they simply open the file and enter the PIN provided by the sender to decrypt it.

How fast is the encryption process?

The amount of time to encrypt or decrypt a file depend on the file size and speed of the computer. An average document takes milliseconds, but a very large file such as video may take a few minutes.

Are there file size restrictions?

SmartEncrypt has no size limits for encryption, and is limited only by available hard disk space as encrypted files are somewhat larger than their original unencrypted versions. Large files however, will take longer to encrypt and decrypt.

The Protect and Share feature has a recommended size limit of 250MB per file.

DEPLOYMENT

What are the requirements to deploy the SmartEncrypt client?

As SmartEncrypt is a cloud service there is no requirement to deploy additional server infrastructure. However, there are requirements on the devices where the SmartEncrypt is deployed:

- **Operating System:** Microsoft Windows 10 64 bit (Build 1809 and later)
- **Network Ports:** 443 outbound

Can I automate the deployment of the SmartEncrypt client?

Yes, you can use Intune to automate the deployment of the SmartEncrypt client to all supported devices enrolled in your Azure AD tenant. Once they have been deployed, any encryption rules that you have configured in the SmartEncrypt Management Console will be applied to that device.

FA
Qs

CONTACT US

Australia 1300 751 723
New Zealand 0800 493 633

SMARTENCRYPT™ by rhipe