DEPLOYMENT SCENARIOS

SMARTENCRYPT™
by rhipe

DEPLOYMENT SCENARIOS

SMARTENCRYPT™ by rhipe

There are several deployment scenarios that are supported by SmartEncrypt to ensure that implementation of the product into an organisation's ecosystem is successful. The following document summarises common deployment scenarios.

DEPLOYMENT WITH AZURE ACTIVE DIRECTORY AND INTUNE

Configure SSO and user synchronisation with Azure Active Directory and use Microsoft Intune to deploy and configure SmartEncrypt client software to devices managed by Microsoft 365.

This allows for a fully automated deployment of the SmartEncrypt tool with configured encryption rules and keys applied as soon as the user logs into the device.

Recommended for

- Organisations with existing Microsoft 365 investment
- Technical resources available to configure and manage Azure AD and Intune policies
- Organisations with a larger fleet of devices.

Deployment requirements

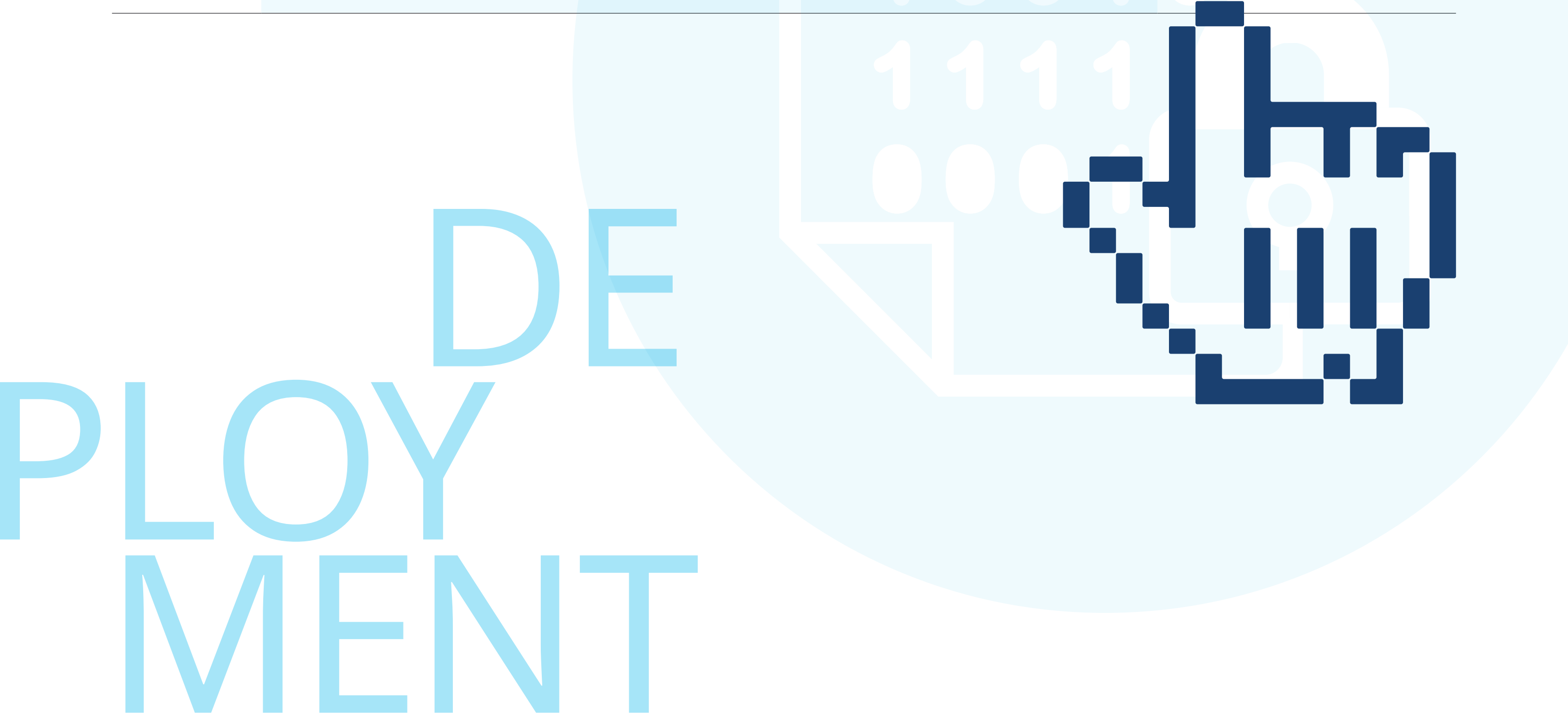
- Active Microsoft 365 subscription with Intune licences
- Global administrator privileges to the Microsoft 365 Tenant
- Active SmartEncrypt subscription
- SmartEncrypt Client SSO Deployment PowerShell
- Intune content preparation tool
- Microsoft Windows 10 operating System (build 1809 or later) on all target devices.

DEPLOYMENT

High level deployment steps

Detailed information on deploying and configuring SmartEncrypt can be found in the SmartEncrypt knowledge base.

Step	Description	KB Article
1	Configure SmartEncrypt security settings	Learn more
2	Create encryption keys	Learn more
3	Setup user groups	Learn more
4	Configure encryption rules	Learn more
5	Register SmartEncrypt as an application in your Azure AD tenant	Learn more
6	Configure SSO settings in the Smart Encrypt management portal	Learn more
7	Download and convert the SmartEncrypt installer as an Intune app package	Learn more
8	Upload the app package into Intune and configure device assignment	Learn more
9	Configure the SmartEncrypt Client SSO Deployment PowerShell script to suit your environment	Learn more
10	Configure Intune to deploy the SmartEncrypt SSO configuration PowerShell script to all devices using SmartEncrypt	Learn more



STANDALONE DEPLOYMENT

Users and groups are created manually or uploaded via a CSV file in the SmartEncrypt management console.

The client will need to be manually deployed on each device by logging into the SmartEncrypt nanagement console to download and install the SmartEncrypt client.

End users will be requested to log into the SmartEncrypt service via the client when they want to access encrypted information.

Recommended for

- Organisations with unmanaged BYO devices
- Organisations that do not use a centralised identity management system
- Organisations with a small fleet of devices

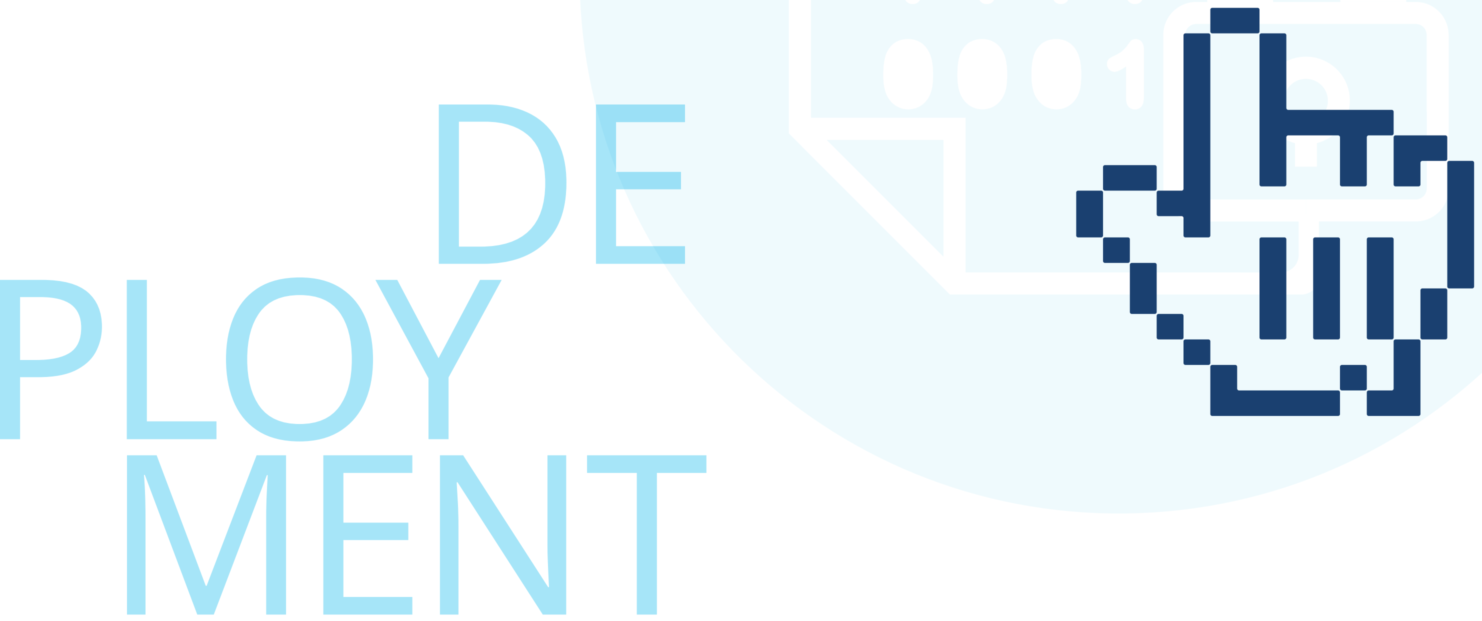
Deployment requirements:

- Active SmartEncrypt aubscription
- Microsoft Windows 10 operating system (build 1809 or later) on all target devices

High level deployment steps

Detailed information on deploying and configuring SmartEncrypt can be found in the SmartEncrypt knowledge base.

Step	Description	KB Article
1	Configure SmartEncrypt organisation account	Learn more
2	Create encryption keys	Learn more
3	Create users	Learn more
4	Setup user groups	Learn more
5	Configure encryption rules	Learn more
6	Download and install the SmartEncrypt client on protected devices	Learn more



CONTACT US

Australia 1300 751 723
New Zealand 0800 493 633

SMARTENCRYPT™
by rhipe

SMARTENCRYPT

A solution that provides certainty that your files will be protected against imminent and developing cyber security risks. Whether intentional or not, data is at risk from those who wish malicious intent. Departing employees, contractors, service providers and temporary workers are all threats to an organisation's data security.

What is encryption?	Encryption is the process of encoding or scrambling data so that it is unreadable and completely unusable unless a user has the correct encryption key.
What is an endpoint encryption product?	Endpoint encryption alters the form of data so that it is indecipherable to anyone other than the intended recipient across any endpoint device. This prevents the data from being readable and misused should that data fall in the wrong hands.
The importance of endpoint encryption	Security products such as firewalls, intrusion prevention, and role-based access control applications all help protect data within the organisation. However, breaches and data theft have become increasingly common, and file encryption can protect files even after they leave an organisation.

INTRODUCING SMARTENCRYPT

SmartEncrypt is a SaaS an enterprise grade encryption solution for businesses of all sizes providing certainty that data is protected in the event of a data breach, file access, or data theft.

Features

- Fast and seamless deployment that typically takes no more than an hour
- Cloud-based file encryption solution that can be managed, and installed by anyone
- Affordable, low cost monthly investment
- An automated and invisible solution that has zero impact on productivity
- Protects all file types
- Encrypt files stored in OneDrive and SharePoint – also works with OneDrive files on-demand
- Blacklist countries where login is prohibited, or whitelist for allowed

Benefits

- **Affordable security:** Cost effective data security versus the costs and damages from unprotected file exposure and lost IP.
- **Protects against unauthorised access to data:** Such as customer lists, high value IP, and protected Personal Identifiable Information (PII).
- **File-level protection:** File encryption is the last line of defence - encrypted content cannot be decrypted without the encryption key.
- **Protection certainty:** Always on persistent encryption, regardless of data movement; files are not accessible even if stolen or exfiltrated by malware.
- **Secure remote working:** Beyond-the-firewall controls enabling use of BYOD computers, cloud storage applications and USBs.
- **Seamless user experience:** 'Invisible' and seamless encryption/decryption process with no impact on user workflows.