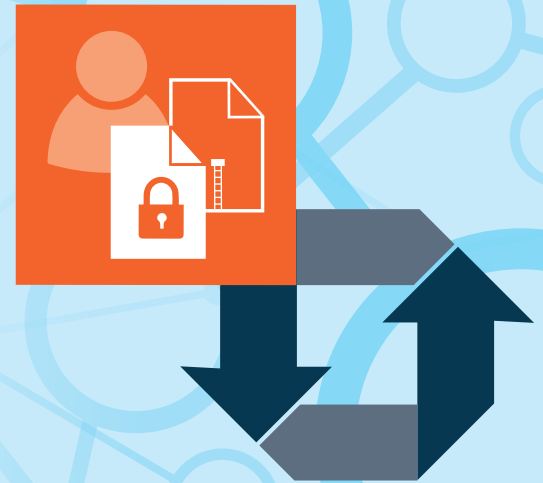


# Egress Switch Secure Workspace

Offering internal users and external third parties access to documents and information, collaboration tools enable content to be shared easily and collectively worked on – delivering efficiency gains and cost-saving potential.

However, if inadequate encryption and access control mechanisms are put in place to safeguard the data, the risks can also be significant, resulting in costly fines and damaged reputation. Without audit functionality and lifecycle control over shared information, organisations have little or no visibility over precisely what has left their corporate network.



## The benefits

- Collaborate with confidence – secure data throughout its lifecycle
- Detailed audits and reports so you can track who is accessing your data
- Free for your third parties to use
- Real-time control over what a recipient can do with shared content
- Flexible secure access across desktop and mobile devices
- Secure shared data regardless of file size
- Take decision-making away from end-users by enforcing centralised data protection policies including content control
- No infrastructure required in hosted implementations
- Brand in line with corporate guidelines
- Enhanced efficiency and cost saving by reducing the time taken to share data
- Role based security policies

## Secure collaboration made easy

Switch Secure Workspace has been designed to offer end-to-end data protection without compromising collaboration functionality. The service can be used to create open or closed communities of users, able to securely share files and work together on joint projects, protected by sophisticated encryption and user permission management.

Offering document version control, annotation of inline content and discussion board functionality, Switch Secure Workspace can be accessed from the desktop and also via mobile devices to support flexible working. In addition, the customisable user interface and branding options ensures that every workspace reflects both an individual project's data sharing requirement and also corporate guidelines.

## Sophisticated control over shared information

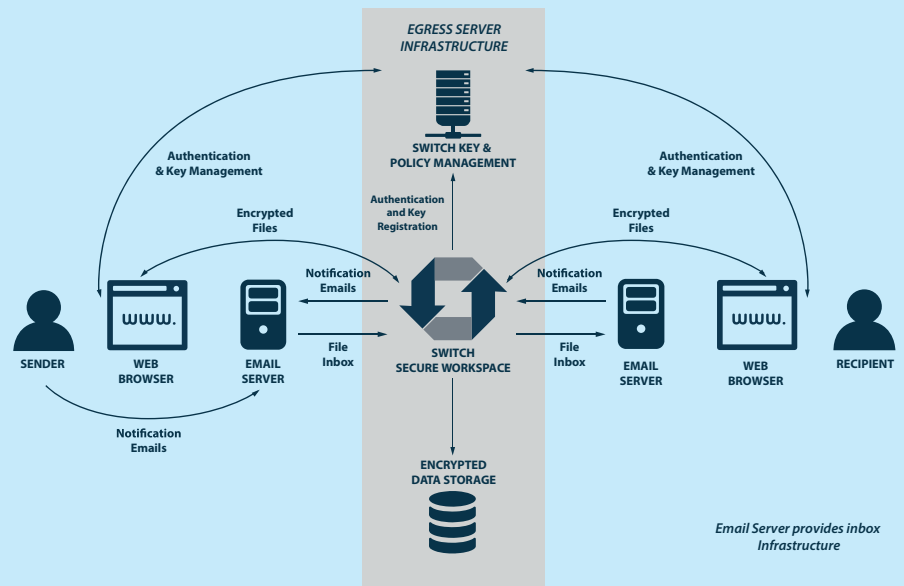
Switch Secure Workspace offers flexible granular permissions for individual users, as well as read-only and rights management control, to ensure only the intended recipients can access and edit shared information. Users can be added or removed from a secure workspace at any point throughout the collaborative lifecycle.

Files can also be shared from within a workspace using a secure link that offers real-time control, including the ability to revoke a user's access. In addition, control over the file types that can be uploaded to a workspace extends the internal management and assurance over the information being shared from within an organisation's network.

### Internal management and control

Each individual secure workspace offers detailed auditing and reporting functionality, including the date and times that users access, download, upload and annotate files. To meet compliance and regulatory rules, this information can be exported to a report.

Role-based security, meanwhile, means system administrators can remain in control of their users and their content at all times. These individual user permissions can be altered throughout the lifecycle of shared information as projects develop.



### Flexible system integration

Switch Secure Workspace integrates seamlessly with DMS and CMS systems – including iManage, MS Dynamics, MS SharePoint and OpenText – and email clients such as MS Outlook and Lotus Notes. In addition, the unique email address provided to each secure workspace enables content to be sent to the Secure File Inbox, from where it can be manually or automatically processed.

In addition, Switch Secure Workspace supports single sign-on via Microsoft Active Directory using ADFS (Active Directory Federation Services) for internal users and for external third parties to provide unified identity management and streamlined access to secure collaboration functionality.

### Security overview

- Secures data at rest and in transit using AES-256 bit encryption
- Secure authentication and user enrolment
- ISO 27001:2013 accredited
- Cyber Essentials Plus certified
- Skyhigh Cloud Trust™ rating of Enterprise-Ready
- Uses data centres accredited to ISO 27001/9001
- Listed under Cyber Security Supplier to Government Scheme

### About Egress Software Technologies

Egress Software Technologies is the leading provider of hosted and on-premise encryption services designed to secure all forms of electronic information and delivered to customers in both the Public and Private Sectors via a single platform: Egress Switch.

The award-winning Switch portfolio of products includes Secure Email, Secure File Transfer, Secure Web Form and the latest online collaboration offering, Secure Workspace.

[www.egress.com](http://www.egress.com)

### About Platform Encryption Services

Platform Encryption Services is proud to have been appointed Channel Partner and Reseller for Egress Software Technologies Ltd. Egress Switch's Award winning encryption platform enables organisations to protect all forms of electronic information shared both internally and externally. Leveraging core expertise in email and file encryption services and UK Government certified key management, the platform includes, Switch Secure Web Form and the latest online collaboration offering; Switch Secure Workspace.

