Egress Switch Gateway

Cloud & On-Premise Email Security

Satisfying regulatory compliance and achieving best practice Information Assurance remains an essential requirement when sharing confidential or personal data with third parties. This is why Egress has developed an integrated management suite offering organisations the ability to enhance existing email security quickly and easily without the need to change end user behaviour.

Flexible Perimeter Security
Designed to integrate seamlessly with anti-virus, anti-spam, archiving and content filtering products, Egress Switch Gateway encryption complements network edge technology enabling customers to deliver ‘follow the data’ protection without changing user behaviour or existing processes.

Desktop Integration
The Egress Switch Client software can be configured to transparently integrate with Switch Gateway by providing client based policy and an enriched end user experience. The Switch client apps include an add-in for MS Outlook, Outlook Web Access, Lotus Notes and Google Chrome. Using the client apps, emails are tagged for encryption by adding specific security headers. This not only provides a simplified user experience but also offers the ability to place policy and time based restrictions around confidential data prior to encryption at the gateway. This advanced desktop component also enables organisations to protect sensitive information distributed internally using the hybrid local encryption and policy engine.

Mail Flow Architecture
The Switch Gateway is built on the SMTP protocol and can be integrated at any point within an organisation’s email topology.

Benefits of Egress Switch Gateway

- **Centralised Policy Management**
  Centrally manage and enforce email encryption policies for both inbound and outbound email.

- **Integrate with content scanners**
  Enable encrypted email to be scanned by existing gateway content scanners.

- **Gateway encryption / decryption**
  Encrypt and decrypt email at the gateway on behalf of the user and without requiring client software installation.

- **Protect and control sensitive information**
  Control who can access information and how it is used – no matter where it goes or how it gets there.

- **Full audit trail**
  Compliance and reporting needs are satisfied for every authorised or unauthorised access attempt.

- **Multi layered security platform**
  Multi-layered authentication maximises data security and stops information being accessed by the wrong recipient.

- **Highly Scalable**
  Highly scalable modular architecture can seamlessly integrate with email topology.
Outbound Encryption
Switch Gateway can automatically and transparently encrypt outbound email based on defined policy. With the optional Switch Client software installed and specifically the MS Outlook or Lotus Notes add-ins users are able to mark messages to be encrypted by the Switch Gateway. In addition, policies can be configured so that the Switch Gateway will scan outgoing email and attachments for specific keywords, phrases and content and make automated decisions based on policy. This not only acts as a safeguard against users accidentally sending out potentially sensitive information but can also negate the need for any client software on the desktop.

Appropriate security can be applied to messages based on author, content, recipient(s) and restrictions defining how the information can be accessed by the recipient. Unlike other gateway based encryption solutions, Switch Gateway sends on behalf of the user rather than using a generic account. This provides users with the ability to manage their own secure email including processing access requests, managing recipient lists, performing revocation and viewing detailed audit events.

Using Switch to encrypt outbound messages, organisations can tightly integrate encryption into existing business practices and workflow. Switch Gateway has been designed to route and split messages based on domain, data classification and recipient. Additionally, there may be specific requirements to create a white list of domains that enforces encryption.

Conversely, when sending information to trusted Government networks, it may be necessary to ensure that emails are routed in clear text. In either instance, the author simply creates a secure email in the normal way and Switch Gateway will automatically process and split messages centrally as defined by administrator policy.

Inbound Decryption
Depending on the security applied by the information owner, Switch Gateway can be configured to automatically decrypt incoming messages on behalf of the recipient, offering a seamless desktop user experience when receiving confidential data. The decrypted messages have a new header added showing the time and date when the message was securely decrypted by the Switch Gateway.

Messages that are automatically decrypted can be routed through standard email filtering applications including anti-virus, anti-spam, archiving and content filtering products prior to delivery. Alternatively, messages marked with a higher level of security, requiring protection throughout the lifecycle of the information, can be decrypted locally by the authorised recipient or using the secure enveloping technology.

Switch Gateway On Premise
For organisations that host all of their email infrastructure internally Switch Gateway On Premise provides seamless integration into existing email topology. The Switch Gateway Server is an SMTP server that can be configured either inline or alongside the existing email infrastructure.
Switch Gateway Hosted

For organisations that want to avoid costly infrastructure charges and embrace cloud technology Switch Gateway Hosted is available. Switch Gateway Hosted is a fully managed server infrastructure that allows organisations to route sensitive information for encryption and decryption and is preferable for organisations that already outsource other email services like anti-virus, anti-spam and archiving.

Configurable Storage Options

Switch Gateway can be configured to provide simple access to secure email and large files via a secure web page (web access). Underlying storage is fully configurable dependent on your organisation’s security requirements. All data is stored in an encrypted format when at rest but can either be located on the local Switch Gateway server or utilising the Switch Cloud infrastructure. Compliance and other regulatory requirements may mandate that all data must reside inside the organisations network boundaries.

Customisable Email Routing

Switch Gateway can be configured to perform email routing rules and exceptions. There may for example be a requirement to route emails for specific domains to a different internal or external location or SMTP server. There may also be a requirement where certain domains are not permitted to receive encrypted emails. In this instance a single email to multiple recipients can be split and routed where certain recipients may receive a clear text copy and others encrypted. The same rules can be applied to inbound emails where for example custom routing is required or a certain recipients email is not decrypted automatically.

Integration with Archiving and Case Management Software

Many organisations, particularly in the Professional Services Sector have both legal and compliance obligations to maintain stringent procedures and software to ensure that any data and email correspondence is retained. Archiving and case management systems provide this functionality. Switch Gateway can be configured to integrate transparently with these systems and depending on an organisations requirements, can store information in either encrypted or cleartext format. Switch Gateway can also be configured to automatically encrypt any external communication performed by automated processes within case management software.

Integration with Gateway Malware Protection

Switch Gateway is designed to address one of the key issues facing IT administrators where integration is required with existing gateway anti-virus/malware protection. Switch Gateway can be seamlessly integrated with existing gateway scanning technologies to ensure that the risk of encrypted email carrying virus infected code is mitigated against. Switch Gateway can be configured to securely encrypt outgoing email after a content scan has been performed and to decrypt inbound emails before virus and content checking is performed.
Transport Agent is a plugin to MS Exchange and enables Switch Exchange Transport Agent. The Switch Exchange using Microsoft Exchange 2007/2010 or 2013 using the granted access to a secure email.

It is also possible to show fully customisable policy disclaimers that a recipient must accept prior to being granted access to a secure email.

Policy Disclaimers & Data Classification
Many organisations have regulatory obligations to classify information that is sent via email. Switch Gateway can be configured to automatically add classification statements to external email based or content and/or policy.

Features & Benefits Summary

Ease of use
- Transparently encrypt email message body and attachments based on policy and/or user selection
- Policy controls can enforce encryption based on security classification and meta data
- Policies can be configured based on:
  - Data type, content & location
  - Recipient/Classification
  - Size of data/Agency type
- Maintain a full audit log of who, where and when information has been sent and access
- Supports security classification and fully customisable disclaimers
- Encrypt both internal and external email when used in conjunction with the Switch Client Apps
- Encrypt email sent and received via mobile devices
- Immediately revoke access to data/files even after they have been sent
- Control who can access the information sent in real-time
- Fully configurable user interface and recipient experience
- Encrypt and decrypt emails irrespective of email client or email server infrastructure

Integration
- Integrates with existing workflow and processes
- Seamless integration with anti-virus/malware scanners and archiving solutions
- Integration with MS Outlook Web Access (OWA)
- Integrates with Google Apps including a Google Chrome Extension
- Integrates seamlessly with case management and archiving software
- Encrypted information can be stored either inside an organisations network perimeter or utilising the highly scalable Egress secure cloud infrastructure
- Integrates with existing storage technologies
- Supports shared mailboxes and automated systems

Management
- Centrally administered and enforced user policies
- Tiered administration allows delegated management of users and policies at organisation or departmental level
- Customisable MMC Management Interface
- Detailed administrator logging and reporting

Cost Savings
- Egress hosted cloud storage provides ease of use and cost savings for sharing large files
- Available as a self hosted or fully managed hosted infrastructure utilising secure cloud technology
- Save time and money by securing existing automated business processes

Security Accreditation
- Secure authentication and user enrolment
- Automatic AES 256 bit encryption
- Utilises FIPS 140-2 certified libraries
- CESG Claims Test Mark (CCTM) Accredited
- CESG CPA Assured
- Accredited data Centre’s to ISO 27001/9001
- Patent Protected (GB 0806429.7 | US12/353,390 | GB 0907665.4)

System Requirements
- Microsoft Windows Server 2003, 2008/2012 (32/64 bit)
- Microsoft .NET framework 3.5 SP1+ Microsoft SQL Compact Edition 3.5+/SQL Express
- Connection to https://switch.egress.com (443)