

Security Procedures Egress Protect



National Cyber
Security Centre

a part of GCHQ

Security Procedures

Egress Protect

Issue No: 1.9
October 2020

The copyright of this document is reserved and vested in the Crown.

This document describes the manner in which this product should be implemented to ensure it complies with the requirements of the CPA SC that it was assessed against. The intended audience for this document is HMG implementers, and as such they should have access to the documents referenced within. If you do not have access to these documents but believe that you have an HMG focused business need, please contact NCSC Enquiries.

Document history

Version	Date	Comment
1.7	27 May 2020	First Issue, for Egress Protect, based on "Egress Switch Security Procedures", Issue 1.6, December 2017. Note that the product name has been changed from "Egress Switch" to "Egress Protect".
1.8	24 June 2020	QA
1.9	21 October 2020	Added information regarding account activity notification for previous authentication attempts (whether failed or successful). Added requirement for administrative users to be trusted in their roles and responsibilities.

Egress Protect

About this document

These Security Procedures provide guidance in the secure operation of Egress Protect.

This document is intended for System Designers, Risk Managers and Accreditors. NCSC recommend you establish whether any departmental or local standards, which may be more rigorous than national policy, should be followed in preference to those given in these Security Procedures.

The Security Procedures come from detailed technical assessment carried out by NCSC. They do not replace

tailored technical or legal advice on specific systems or issues. NCSC and its advisors accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed on this guidance.

Related documents

The documents listed in the References section are also relevant to the secure deployment of this product. For detailed information about device operation, refer to the Egress Protect product documentation.

Points of Contact

For additional hard copies of this document and general queries, please contact NCSC using the following details.

NCSC Customer Support Office

A2b
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

enquiries@ncsc.gov.uk
Tel: 01242-709141
Fax: 01242-709193
(UNCLASSIFIED faxes only)

We welcome feedback, positive or negative, about this document. Please mark your comments for the attention of the **IA Policy Development Team**.



THIS PAGE IS INTENTIONALLY LEFT BLANK

Egress Protect

Contents

Chapter 1 - Outline Description	7
Certification	7
Components	7
Administrative Users	9
Change of Name and Terminology	10
Chapter 2 - Security Functionality	11
Chapter 3 - Secure Operation	14
Pre-Installation	14
Segregate the Physical Server Hardware	14
Installation	18
Configuration	20
Operation	25
System Logs	26
Maintenance and Updates	27
User Education	27
Chapter 4 - Security Incidents	28
Incident Management	28
Tampering and Other Compromises	28
Chapter 5 - Disposal and Destruction	31
References	32
Glossary	33



THIS PAGE IS INTENTIONALLY LEFT BLANK

Egress Protect

Chapter 1 - Outline Description

1. Egress Protect version **19.10.30727** has been certified as satisfying the requirements of NCSC's Commercial Product Assurance (CPA) Foundation Grade.
2. Egress Protect's CPA certification is for its email encryption functionality, which enables the user to send information securely via email and attachments. These Security Procedures are specifically for that functionality. Note that CPA Certification covers the Egress Protect Microsoft Outlook Addin, but Certification does not cover Egress Prevent on mobile, Egress Web Access (EWA), or Outlook Web Access (OWA).
3. All other functionality of Egress Protect, including other media (e.g. CD/DVD, USB stick, FTP site, cloud storage) and other modes of transmission (e.g. web, FTP, in person, by post), is outside the scope of the CPA certification and is therefore excluded from these Security Procedures.
4. Egress Protect includes an offline package feature, which allows entitled recipients to access encrypted packages whilst they are offline. However, once the recipient has received the password-protected package and knows the password, it is not possible to revoke access or to change their access permissions. Therefore, for CPA Foundation Grade, the offline package **must remain disabled** and it is therefore excluded from these Security Procedures.

Certification

5. Egress Protect version **19.10.30727** has undergone CPA Foundation Grade assessment and has been certified as meeting the Foundation Grade requirements as described in the following:
 - a. CPA Security Characteristic: Gateway Email Encryption [a]
 - b. CPA Security Characteristic: Desktop Email Encryption [b]
6. Later versions of Egress Protect are automatically covered by this certification until the certificate expires or is revoked, as stated on Egress Protect CPA Certificate and on the CPA website.

Components

7. Table 1 below indicates the components of Egress Protect and Table 2 below indicates which of those components are in or out of scope of Certification.
8. Egress Protect consists of the following components:



Component	Protective Marking	Comments
Egress Server Infrastructure (ESI)	(See the *Note below.)	ESI consists of these 4 components: <ul style="list-style-type: none"> • External Connection Point (ECP) Server • Internal Connection Point (ICP) Server • Authentication Server • Database Server with the ECP placed into the Demilitarised Zone (DMZ) according to Diagram 4 below. For low-scale deployments, all components can be installed on a single server instance.
Egress Protect Gateway (EG)	(See the *Note below.)	(None)
Egress Protect Client (EPC)	(See the *Note below.)	(None)

Table 1 – Components of Egress Protect

***Note:** The Protective Marking of each component is the maximum classification level of the data stored or processed on it.

9. Egress Protect components are in or out of scope as follows:

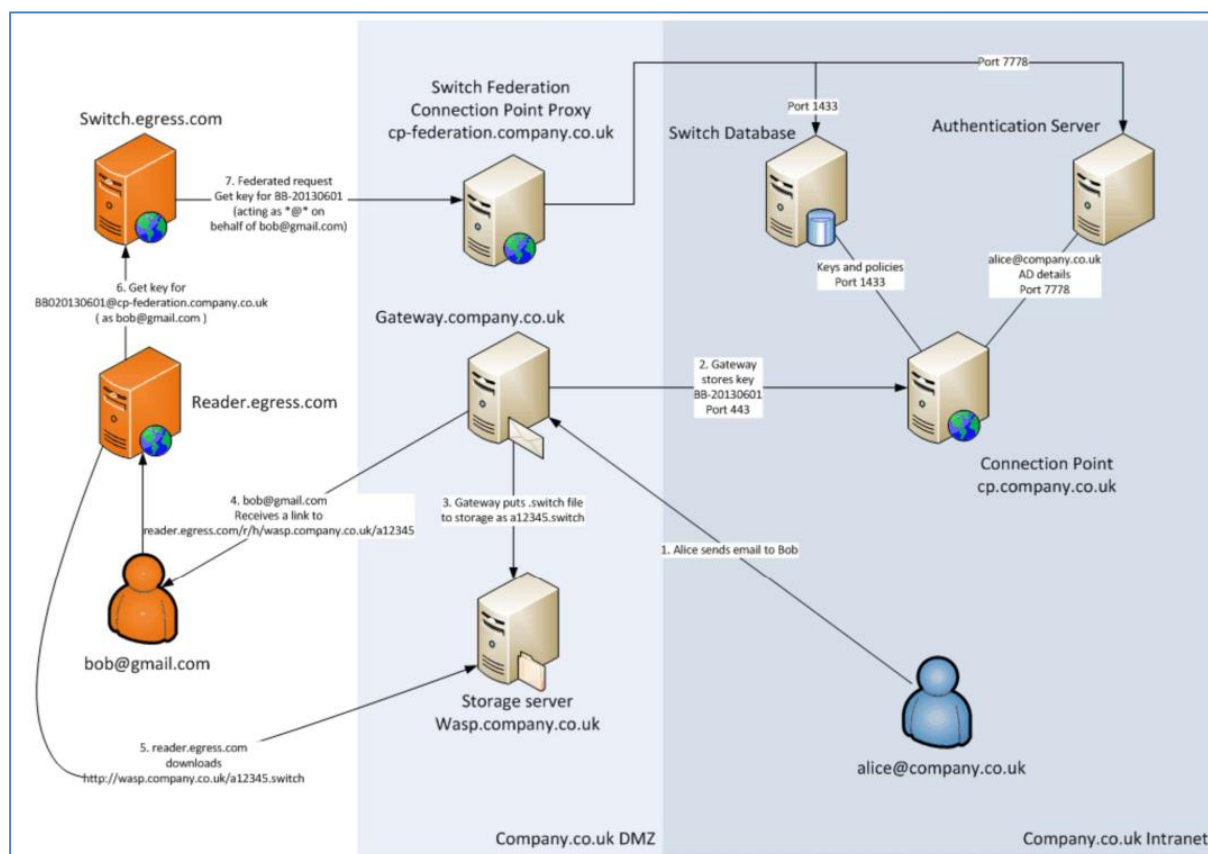
Component	In Scope?	Component was CPA Evaluated on this Operating System:	Component is CPA Certified on this Operating System*:
Servers (ESI & EG)	Yes	Microsoft Windows Server 2012 R2 (64-bit)	Microsoft Windows Server 2012 R2 (64-bit)
Client (EPC)	Yes	Microsoft Windows 10 Enterprise v1607 (64-bit)	Microsoft Windows 10 Enterprise v1607 (64-bit)
Mobile Client	No	N/A	N/A

Table 2 – Components In Scope and Out of Scope of Evaluation/Certification

***Note:** The latest compatible Operating System must be used and must be regularly updated with the manufacturer's security patches and hotfixes.

Egress Protect

10. Diagram 1 below outlines the workflow for Egress Protect. Creating, sending and receiving Egress Protect encrypted email can be traced by following the numbered processes in the diagram (starting with Alice in the lower right).



**Diagram 1 – The Egress Protect Workflow
(numbered process illustrated above)**

11. Any future security patches for Egress Protect must be promptly applied.

Administrative Users

12. It is a fundamental requirement that administrative users are suitably and adequately trusted in terms of their security roles and responsibilities.
13. There are three levels of Administrator in Egress Protect:
- a) **Database Owner.** This is a Windows account, with administrative access to all components of the Egress Protect installation, which is permitted to directly access and modify the structure of system databases or binary files. This



level of access permits the Database Owner to assign an Egress Protect Super User. Access is controlled and audited by the host Operating System.

- b) **Super User.** This is an Account permitted to access the system through the Web Interface, modify the default server policy and create the internal tenant (“organisation”) accounts inside Egress Protect, as well as modify the advanced properties of these accounts. Access is controlled by the Egress Protect Connection Point, by comparing the User identities to the list of Super Users configured by the Database Owner. Audit events are stored in the Egress Protect database.
 - c) **Administrator.** An Administrator of individual “organisational” accounts, who is permitted to create User accounts. Access is controlled by the Egress Protect policies. Audit events are stored in the Egress Protect database.
14. Departmental and local policies must also be consulted before implementing Egress Protect, as those policies may be more rigorous than national policy or these Security Procedures.

Change of Name and Terminology

15. The name of the product has changed from “Egress Switch” to “Egress Protect”. Consequently, the Egress terminology has been changed as follows:

Previous Egress Switch Term	Current Egress Protect Term
Egress Switch Client (ESC)	Egress Protect Client (EPC)
Egress Switch Gateway (ESG)	Egress Gateway (EG)
Egress Switch Server Infrastructure (ESI)	Egress Server Infrastructure (ESI)

16. This document uses the current Egress Protect terminology.

Egress Protect

Chapter 2 - Security Functionality

17. The Egress Protect Client (EPC) permits the user to send encrypted emails using Microsoft Outlook. Each email is encrypted by EPC with a randomly generated symmetric key; this key is then uploaded to the Egress Server Infrastructure (ESI) Server.
18. The EPC allows the user to decrypt an email sent by another user, by requesting the decryption key from the ESI Server. If the user is permitted access by the sender, the key is transferred to the EPC and the email is decrypted automatically.
19. The EPC also allows the user to control who has access to the encrypted email, even after it has been sent. This access information is stored as a policy on the ESI Server.
20. The Egress Protect Gateway (EG) Server sits at the boundary of a secured network, where it encrypts outbound emails and decrypts inbound emails. The EG Server enforces corporate policies for sensitive emails, e.g. if a user did not encrypt a sensitive email using their EPC (or does not have the EPC installed), then the EG Server will automatically encrypt the email. See Diagram 2 below.
21. The encryption and decryption actions of the EG Server are controlled by policies which are downloaded from the ESI Server. Encryption and decryption may happen at either the Gateway or Client, depending on policies and installation options. When performing encryption, the EG encrypts emails with a randomly generated symmetric key, which is then uploaded to the ESI Server.
22. The ESI Server stores the symmetric email encryption keys uploaded to it by the EPC and EG. Each key is linked to a policy which controls who has access to the encrypted email secured by that particular key.
23. When an EPC or EG requests a key to decrypt an email, the ESI Server first checks if the policy permits the user to have access. If the policy permits access, the key is retrieved and sent to the EPC or EG.
24. The ESI Server logs all access requests for keys, allowing the sender of an encrypted email to monitor when and by whom the encrypted email was accessed.

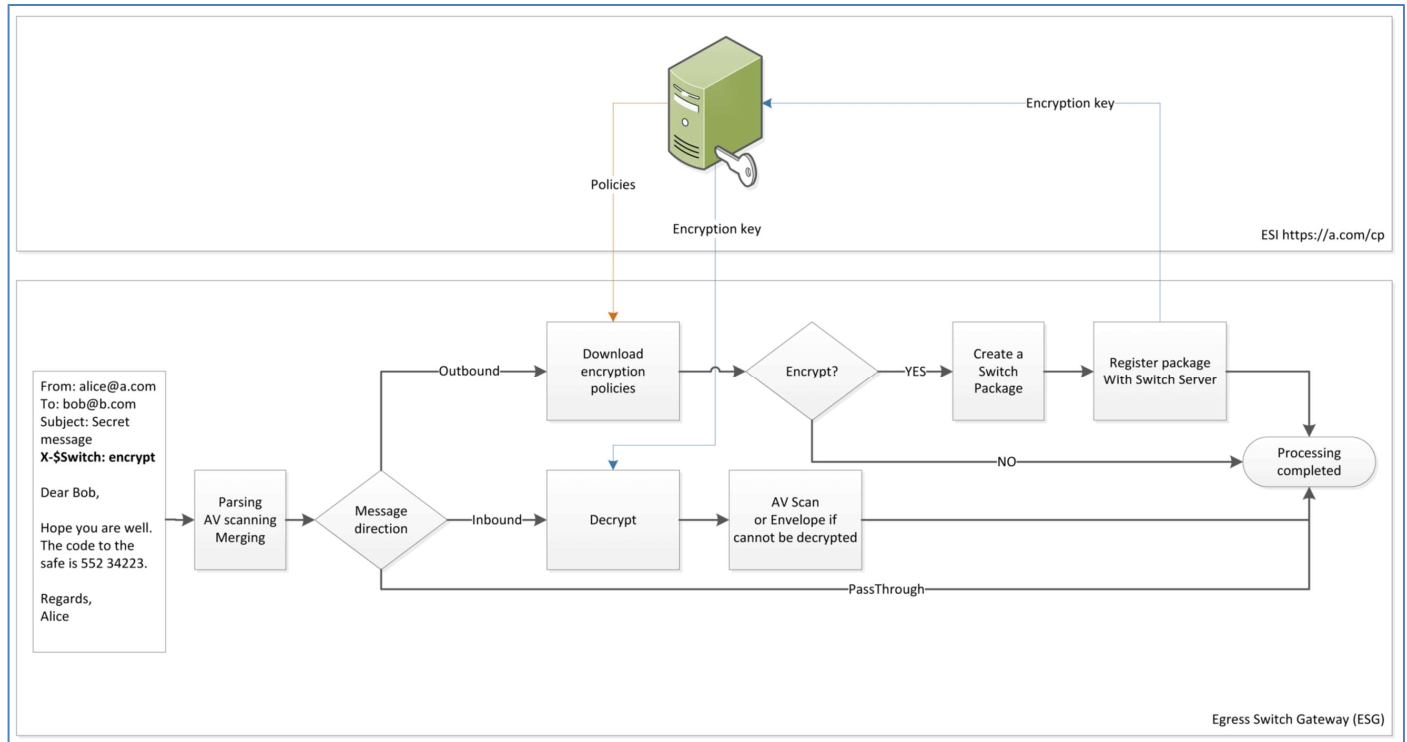


Diagram 2 – The Egress Protect Gateway Message Flow

25. To illustrate Egress Protect's security functionality between subscribers and nonsubscribers, refer to the flow in Diagram 3 below which shows the case where users alice@a.com (with EPC) and bob@a.com (without EPC) are both sending messages A1 and B1 to a different installation of Egress Protect, hosting users clark@c.com (without EPC) and diana@c.com (with EPC).
26. **Note:** diana@c.com is expected to have an EG/ESI at @c.com. If there is no such software, diana@c.com is expected to obtain a set of credentials with one of the publicly available EG/ESI, and use them to obtain the package key according to the diagram. The exact mechanism that Diana would follow to obtain such credentials is not within the scope of this document.

Egress Protect

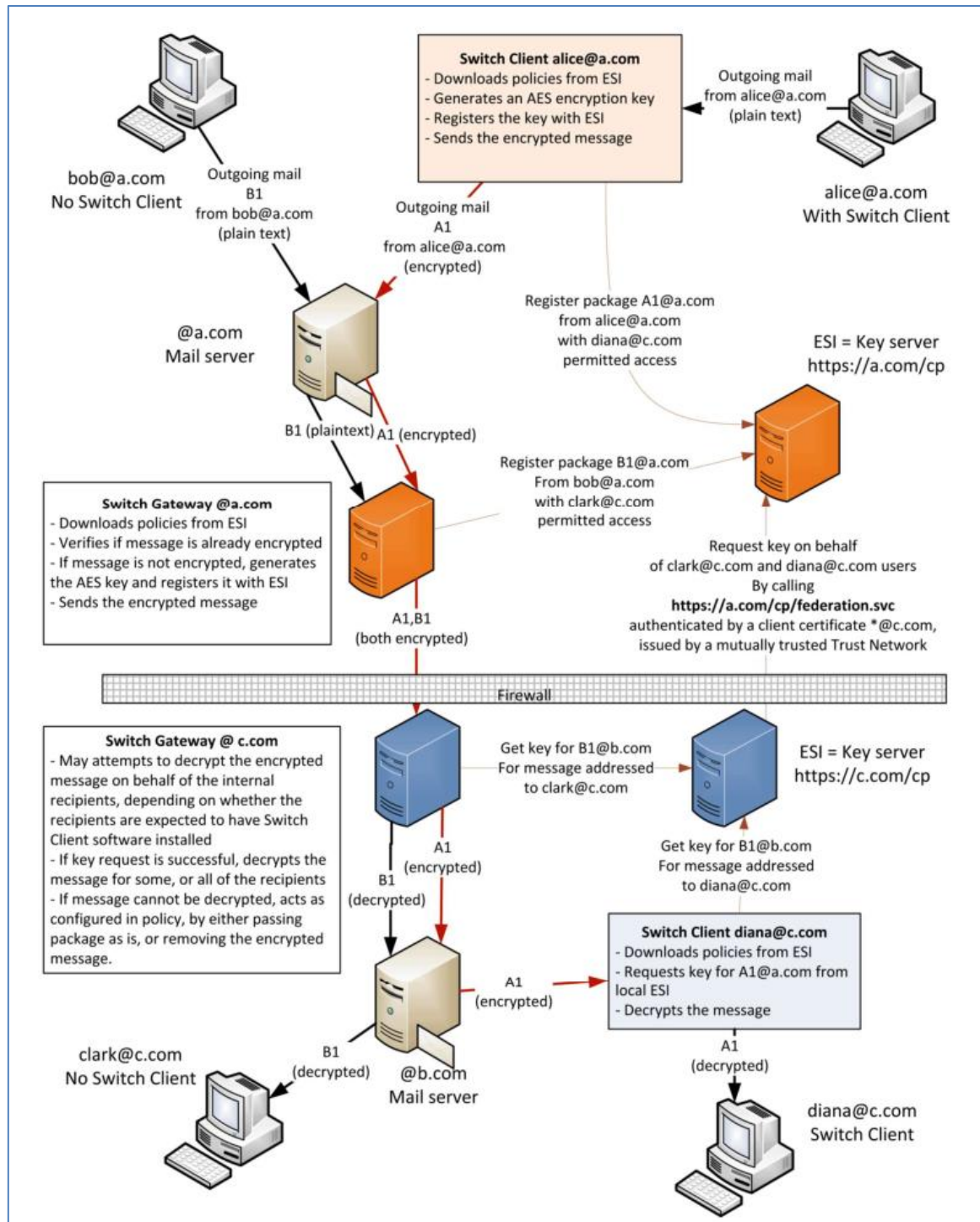


Diagram 3 – Egress Protect Communication Flow Example between Users and Nonusers



Chapter 3 - Secure Operation

27. The following recommendations outline a configuration for Egress Protect that is in line with the CPA Security Characteristic for Gateway Email Encryption [a] and Desktop Email Encryption [b]. These requirements should be followed unless there is a strong business requirement not to do so. Such instances should be discussed with your Accreditor.
28. To meet the needs of the Accreditor, an installation of Egress Protect should be updated if any critical changes occur, as outlined in the Egress Protect CPA Assurance Maintenance Plan [c].

Pre-Installation

29. Before installing Egress Protect server software, in addition to following good practice, you must take the following actions:
 - a. Ensure that the latest updates for Microsoft Windows and Microsoft Outlook have been installed;
 - b. Ensure that any option to use Address Space Layout Randomisation (ASLR), or other security features, adheres to Microsoft guidance.
30. Subsequently, perform all the actions in the rest of this Chapter.

Segregate the Physical Server Hardware

31. The physical hardware hosting the ESI Server and the EG Server must be segregated into their own dedicated network segment (DMZ or VLAN) and be protected by a firewall. This is illustrated (at a high level) in Diagram 1 in Chapter 1 and (at a low level) in Diagram 4 below.
32. The only ports that need to be opened on the firewall are listed in Tables 3 and 4 below. Also see the *Internet Access* section below.
33. All hardware used to deliver the email service must be installed according to the data classification being handled, including installation of the hardware in a physically secured location with access restricted to only administrative users.

Egress Protect

Egress Protect Infrastructure Server Ports			
Direction	Port Name	Port Number	Comments
Inbound	HTTPS	tcp/443	Connections must be limited to the internal network. However, external connections are permitted from federated ESI Servers run by other organisations.
	RDP	tcp/3389	Optional, for remote administration. RDP connections must only be accepted from trusted VPN/IP addresses. (<i>See the *Note below</i>)
Outbound	SMTP	tcp/25	Connections can be restricted to an SMTP smarthost ¹ on the internal network. NB: Outbound SMTP port is enabled on the ESI to send messages to users, such as invitations, access requests etc.
	HTTPS	tcp/443	Connections must be restricted to the Microsoft Windows Update Servers, AV Update Servers and external federated ESI Servers.

Table 3 – Egress Protect Infrastructure Server Ports

***Note:** RDP is shown as an example. Other management protocols and tools can be used for managing ESI from trusted VPN/IP addresses (whether inbound and/or outbound) but must be covered by the Security Policy of the deployment.

¹ A smarthost is an email server whereby third parties can send emails to be forwarded on to the email recipients' email servers.



Egress Protect Gateway Server Ports			
Direction	Port Name	Port Number	Comments
Inbound	HTTPS	tcp/443	Connections can be restricted to an SMTP smarthost on the internal network.
	RDP	tcp/3389	Optional, for remote administration. RDP connections must only be accepted from trusted VPN/IP addresses. (<i>See the *Note below</i>)
Outbound	SMTP	tcp/25	Connections can be restricted to an SMTP smarthost on the internal network.
	HTTPS	tcp/443	Connections must be restricted to the ESI Server, Microsoft Windows Update Servers and AV Update Servers.

Table 4 – Egress Protect Gateway Server Ports

***Note:** RDP is shown as an example. Other management protocols and tools can be used for managing EG from trusted VPN/IP addresses (whether inbound and/or outbound) but must be covered by the Security Policy of the deployment.

Egress Protect

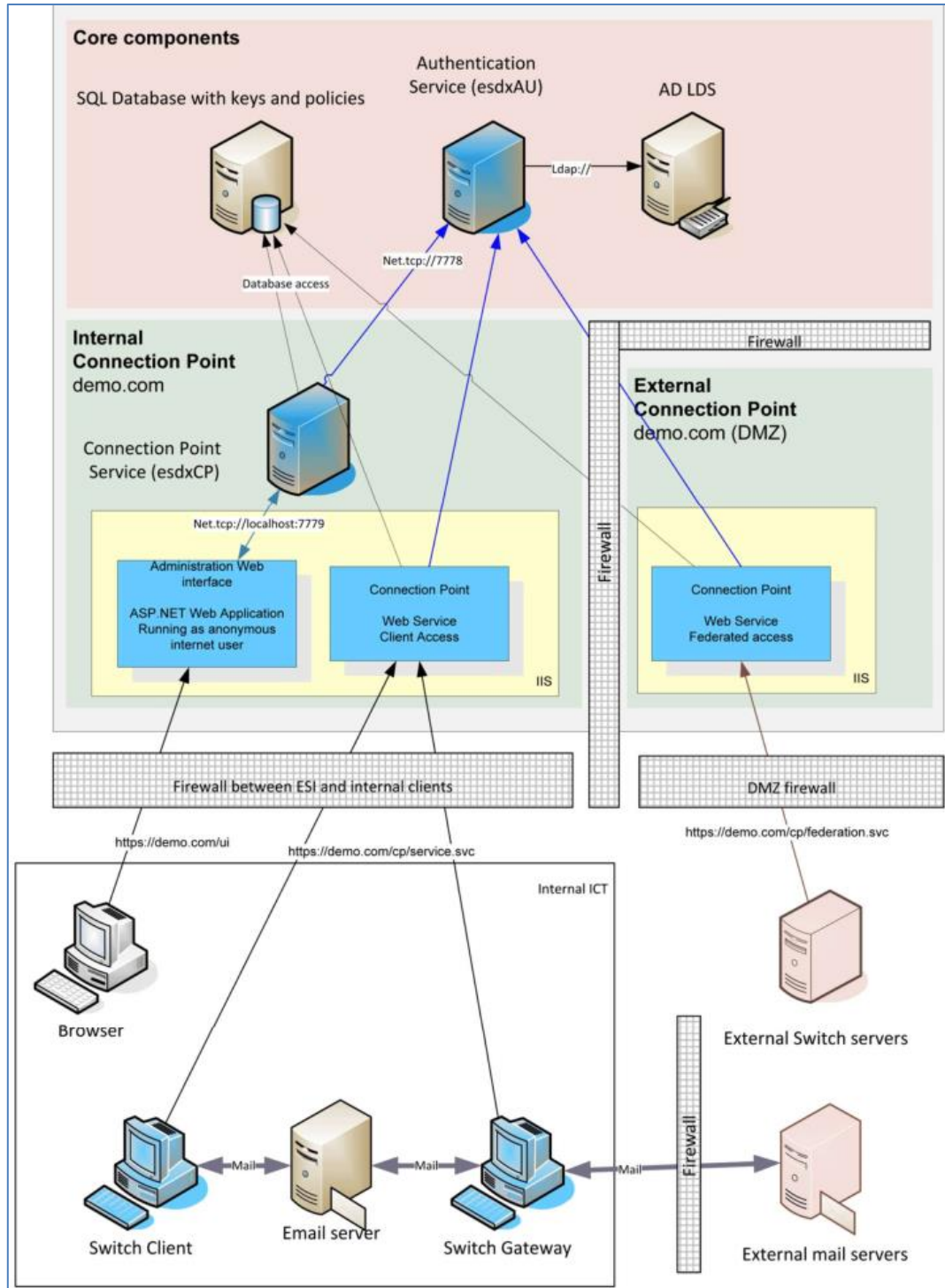


Diagram 4 – Egress’s Recommended DMZ/Component Separation



Secure Sockets Layer (SSL) Certificates

34. SSL Certificates are required as part of the core ESI installation and are used to encrypt traffic between the ESI Server and the EG/EPC.
35. Before installing either the ESI Server or the EG Server, a valid SSL Certificate must be obtained for each server.
36. The SSL Certificates must be linked to the Organisation's name and must only be obtained from a verified trusted third-party Certificate Authority. In addition, the validity of each Certificate must be no longer than one year, in order to mitigate attacks against weak SSL certificates.

Installation

37. Always follow good practice by ensuring that Operating Systems are patched with the latest Service Pack and important security hotfixes. Additionally, ensure that the digital signature Certificates on Egress Protect installation software have been verified. (For details, see Verify Egress Installation File Integrity [d].)
38. Egress digitally signs the installation files for ESI Server, EG Server and EPC using a Thawte Code Signing Certificate. This ensures that the Egress Protect installation files have not been tampered with after they leave Egress.
39. Ensure that the Egress Protect client is installed on a standard user account without any elevated privileges.

Egress Protect Installation

40. Whilst this document focuses on the Security Procedures, for reference the ESI, EG and EPC installation guides are as follows:
 - a. For ESI Server: Egress Protect Infrastructure Installation Guide [e]
 - b. For EG Server: Egress Protect Gateway Installation Guide [f]
 - c. For EPC: Egress Protect Client Deployment Guide [g]
 - d. For a list of the changes made during the installation of the Egress Protect software (ESI, EG and EPC) refer to Egress Protect Installation and Uninstallation [h]
41. The latest version of the Egress tools can be obtained from Egress Support via their website <http://www.egress.com/contact-us> or via the technical account manager who has been assigned to you. Updates must be applied manually and without delay, when they are released.

Egress Protect

Preventing External Client/Gateway Access

42. There are two ways to prevent external Client/Gateway access:

- a. Apply restrictions to IP ranges that can access Gateway accounts and Organisation accounts in the management interface.
 - i. Using the management interface, specify IP ranges from where ESI users and Gateway accounts may access ESI services. For example, it is possible to restrict EG accounts to only use the 192.168.10.0/24 IP range, and permit user access from within the organisational network. Access attempts from other IP addresses will be denied.
 - ii. In addition to IP restrictions applied at the ESI level, IP restrictions may also be applied in an Internet Information Service configuration and Windows Firewall on an ESI Server.
- b. If multiple Connection Points are deployed, with only one exposed externally, the external Connection Point may only be installed with the federated access option, specified in the setup. Alternatively, federated access may be enforced by deleting the service.svc file from SDX\Egress\cp\service.svc.

Post Installation

43. In order to speed up application start up, and improve Data Execution Prevention (DEP) protection, it is recommended to execute the following command line commands after the software installation or upgrade.

Egress Protect Client	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe install "C:\Program Files (x86)\Egress\Switch\SDXTray.exe" /queue:3 /nologo
	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe executeQueuedItems 3 /nologo
Egress Protect Gateway	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install "C:\program files\egress\sdx\gateway\bin\Egress.Sdx.Server.Gateway.Service.dll" /queue:3 /nologo
	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install "C:\program files\egress\sdx\gateway\bin\GatewaySelfHost.exe" /queue:3 /nologo
	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe executeQueuedItems 3 /nologo



Configuration

44. After the installation of the ESI Server, EG Server and EPC has been completed, several steps need to be taken to lockdown security to meet the CPA Foundation Grade requirements.
45. Good practice should always be employed when securing the deployment environment. Egress recommends the following pre-install tasks:
 - a. Install the Microsoft Windows hot fixes for those additional operating system components (e.g. Internet Information Services (IIS), .NET) that were installed as a pre-requisite prior to installing Egress software.
 - b. Run the Microsoft Security Configuration Wizard, which reduces the attack-surface of the Windows 2012 R2 Server operating system by modifying security settings for Roles, Services and Features.
 - c. Enable and configure the Windows Firewall (or another host firewall). The number of open ports must be reduced to a minimum to reduce the attack surface of the Windows Servers. The only open ports needed by the ESI Server and EG Server are shown in Tables 3 and 4.
 - d. Ensure that codesigning verification options in the Server and Client operating systems are enabled when using Egress Protect.
 - e. All communication between the components of Egress Protect is protected by Transport Layer Security (TLS). The TLS configuration on the ESI Server must be modified to prevent the use of older, weaker, cipher-suites which are enabled by the Windows 2012 R2 Server Operating System by default. For detailed information on the TLS configuration within Egress Protect, refer to Egress Protect TLS Configuration Guide [i].

Communication between internal SMTP mail servers and EG SMTP servers should be configured to use TLS. If the mail servers and Gateway are on the same trusted network, just SMTP should suffice.

Note: This is one way to configure your Egress Protect installation. Your methods and tools may be different, but you need to achieve an equivalent security-related outcome.

Egress Protect

Securing the Egress Protect Infrastructure Server

Disable the IIS Server Stack Traces

46. If a crash occurs on an IIS server, it is possible for ASP .NET applications to display a HTML page, which may contain potentially sensitive error details, to the user.
47. As the ESI Server Web User Interface (UI) is implemented as an ASP .NET application, this error page **must be disabled** via the IIS Manager.

Protect User Accounts

48. Egress Protect user accounts must be protected from brute-force attacks. To achieve this, a secure password policy for Egress Protect user accounts must be configured and enforced on the ESI Server.
49. To create a secure password policy, log into the ESI Server web-admin interface (https://<your_ESI_fqdn>/ui) with your Administrator account. In the left-hand pane, click 'Passwords' under the Policies section. In the right-hand pane, click the 'Show Advanced Settings' link. It is recommended that, as a minimum, a secure password policy must be as follows:
 - a. The password length must be least 8 characters;
 - b. The password must include lowercase characters, uppercase characters, numeric characters, and special characters;
 - c. The password expiration must be at most 365 days;
 - d. User account lockout must be enabled;

For Egress Protect, the user account lockout setting will lock the user account for five minutes after three failed login attempts. This protects the user account from a continuous brute-force attack attempt, whilst minimising the impact on the user of a full account lockout.

50. User accounts will typically be synchronised to an existing authentication directory system. Where this isn't the case, user accounts can be managed within the ESI, but procedures should be put in place to ensure timely granting and revocation of access, in line with policy. Once locked or revoked, a user account will no longer be able to access encrypted packages sent via Egress Protect (unless previously decrypted copies of the data were retained).
51. Where an external authentication directory isn't used, it is recommended to create users with a blank password, as this forces the user to set a password (to meet the configured complexity requirements) as part of their account



activation. Automatic account creation **must be disabled** to enforce usage only by authorised users.

ESI Server Resource Management

52. To ensure that service is maintained when resources (e.g. RAM, CPU cycles, etc) are constrained, resources must be managed to limit the amount of resources that a process can consume. This will prevent a process from consuming excessive resources and causing a Denial of Service (DoS) on the ESI Server.
53. The ESI Server relies on third party web and SMTP server software. Therefore, resource management should be aimed at the underlying IIS and SMTP software. One way of achieving this, is to use the Windows System Resource Manager.
54. For more information on using and configuring the Windows System Resource Manager, see: <http://technet.microsoft.com/en-us/library/cc755056.aspx>

Securing the Egress Protect Gateway Server

55. After following the good practice recommendations of the 'Configuration' section above, proceed with the following.

Secure the Egress Protect Gateway Logon Account

56. A strong secure password must be set for the Egress Protect account used by the EG Server to communicate with the ESI Server. Whilst it is possible to generate passwords manually (rule-based), they must be created pseudo-randomly for Gateway accounts (and must be at least 128 bits strong). The Egress Gateway account must be configured to prevent lockout (i.e. DoS).
57. To configure and enforce a very secure password for the EG account, log into the ESI Server web-admin interface (https://<your_ESI_fqdn>/ui) with your Administrator account. The security settings of an Egress Gateway account must be configured as follows:
 - a. Protect the account with a password that is machine-generated over a space of at least 2^{128} possible password values.
 - b. Lockout **must be disabled**, to protect against DoS attacks via cumulative login failures.
 - c. Software-based self-help mechanisms that could bypass the strength of the password (e.g. "What is your favourite...?") **must be disabled**.
 - d. Set password expiry to at most 365 days.

Egress Protect

Note: Passwords for Egress Protect Gateway accounts cannot be reset using self-help; an error message is displayed if this is attempted. Only an Administrator can reset the password.

58. Gateway accounts should additionally be configured with IP restriction to restrict the locations from which a brute-force attack could be carried out. To ensure that IP spoofing cannot be used to brute-force gateway accounts², the network environment should be configured with IP spoofing protection³.

Egress Protect Gateway Mode

59. As the EG Server decrypts inbound secure emails, it may occasionally fail due to, for example, the email becoming corrupted or tampered-with during transit or a policy applied by the sender that only permits the recipient to decrypt the email.
60. For CPA Foundation Grade, the EG must be configured to forward the encrypted contents to the recipient, together with a message informing them that the decryption has failed.
61. To do this, configure the EG as follows:
 - a. On the EG Server, open the Gateway Management Console.
 - b. In the left-hand pane, right-click on the Egress Protect Gateway node and select Properties from the pop-up menu.
 - c. Egress Protect Gateway Properties window will open. Click on the Inbound tab.
 - d. In the Decryption settings section, configure the following:
 - i. If Egress Protect attachment is found: 'Decrypt'.
 - ii. If decryption fails: 'Send without processing'.

² IP spoofing wouldn't return a direct result of success if a password were to be guessed correctly. However, side channel information, such as monitoring package logs, could in theory be used to monitor the success of a brute-force attack.

³ Although the network environment is outside the scope of the Security Procedures, configuring it to provide IP spoofing protection could include, for example, blocking any IP packets with a local/internal source address from entering the network at the perimeter protections, and using the MAC-address monitoring functions of the Egress Protect hardware deployed.



62. There are also loop-prevention measures in EG, where attempts to process the same message many times are automatically detected and the message is sent to bad mail.
63. By default, the EG replaces message content with instructions to use the web portal, displayed to users without EPC installed. This includes a link to the portal. The message templates should be updated to remove the clickable link, in line with good email security practices.
64. A third-party anti-virus email gateway must be installed on the unencrypted side of the gateway (typically between the gateway and internal mail server).

EG Server Resource Management

65. To ensure that service is maintained when resources (e.g. RAM, CPU cycles, etc) are constrained, resources must be managed to limit the amount of resources that a process can consume. This will prevent a process from consuming excessive resources and stopping the EG Server from processing emails thereby causing a DoS.
66. The EG Server relies on third party SMTP server software. Therefore, resource management should be aimed at the underlying IIS and SMTP software. One way of achieving this is to use the Windows System Resource Manager.
67. Egress uses Windows Error Reporting and local text files to record log information. Storage resources should be monitored to ensure that there is adequate storage available to maintain log history. This can be achieved using Windows System Resource Manager, or by integrating with existing enterprise management tools.
68. For more information on using and configuring the Windows System Resource Manager, see: <http://technet.microsoft.com/en-us/library/cc755056.aspx>

Securing the Egress Protect Client (EPC) Configuration

69. For CPA Foundation Grade, the following must be performed on the EPC:
70. The EPC has a feature for burning encrypted packages to a CD/DVD running under a service called "Egress Service". However, this service runs with SYSTEM privileges, which poses a potential security risk. Therefore, this service **must be disabled** for CPA Foundation Grade Certification.
71. FIPS-140 mode on EPC computers **must be disabled**. There are two libraries that ship with the EPC software which do not support ASLR and DEP; these two particular EPC libraries are only used when FIPS-140 is enforced on the

Egress Protect

client computer. By disabling FIPS-140 mode, those libraries will not be used. For more information on FIPS-140, please refer to:

<http://support.microsoft.com/kb/811833>

72. The EPC relies on the channel security package for outgoing TLS communications. The EPC itself must be locked down so that it uses only CPA approved cipher-suites. The lock down of the cipher-suites used by the EPC can be done without affecting other applications. The process to achieve this is described in Egress Protect TLS Configuration Guide [i].
73. EPC must only be used on endpoints with local, email-aware, Anti-Virus installed. This must be configured to update according to the manufacturer's recommendations. This is required to mitigate the risk of virus payloads being sent within Egress packages, and must be configured to scan emails after decryption and prior to rendering.

Operation

Egress Protect Client

74. Where possible, all Egress Protect users in the organisation should have the EPC for Microsoft Windows installed on their computers.
75. Where the EG Server was not able to decrypt an inbound encrypted email, the EG Server will forward the encrypted email to the recipient together with a message stating that the decryption failed. The EPC itself will then attempt to decrypt the email.

Internet Access

76. Egress Protect software (i.e. ESI, EG and EPC) uses x509 certificates to secure sensitive data being sent and received over the network. Therefore, it is important that the ESI Server, the EG Server and the EPC computer have outbound access on port TCP 80 to the Internet for CRL/OCSP checking so that revoked certificates can be identified in a timely manner. The list of URLs/IP addresses that ESI may use for downloading CRL/OCSP information may be obtained from the CRL Distribution Point and Authority Information access extensions of the server certificates that ESI may communicate with.
77. CRL and OCSP checking is typically done over HTTP:80 with integrity verified on an application level rather than transport layer (CRLs and OCSP responses are signed with a CA key). For example, the current switch.egress.com certificate specifies <http://EVSSLocsp.geotrust.com> as an OCSP responder, and <http://EVSSLcrl.geotrust.com/crls/gtextvalca.crl> as a CRL Distribution Point.



78. However, inbound access to the ESI Server from the Internet must be blocked to minimise the attack surface area of the server. The only exception to this rule would be to allow port TCP 443 from federated ESI Servers run by other organisations to allow retrieval of encryption keys for emails. Connections to external federated ESI Servers are protected using mutual TLS authentication.
79. Users who need to access the ESI Server from remote locations, i.e. from locations outside the internal network, must do so only via a VPN link to the internal network.

Client/Gateway Policy

80. ESI Policy rules can be created which can, for example, enforce the use of Egress Protect for certain senders and recipients, or enforce expiry of packages. The full range of features is beyond the scope of this document, but details are provided in Egress Protect Policy Enforcement [j]. This should be reviewed, and then policies should be created to match the organisation's security requirements. These rules can be tested using the CRTester utility.

Client Rule Tester

81. The Client Rule Tester (CRTester) is a utility which allows an Administrator to test ESI policy rules in a simulated condition. This is useful for debugging situations where multiple policy rules are applied to a client. Although the CRTester allows the Administrator to create policy rules, it is recommended that the CRTester is not used to create policy rules, as the underlying XML language is complex, and mistakes may be easily made.

Password-Protected Packages

82. The password-protected package feature is disabled by default. This feature offers the ability for a recipient to access an encrypted package whilst they are offline, provided that the sender has enabled this feature for the package and has given the password to the recipient.
83. However, if a recipient has received both the password protected package and the password, it is not possible to revoke access or to change their access permissions. Therefore, for CPA Foundation Grade, the offline package feature **must remain disabled**.

System Logs

84. ESI Server and EG Server both rely on Windows Error Reporting for logging application crashes. Windows Error Reporting is enabled by default in Windows 10, Windows Server 2008R2, and higher, and **must remain enabled**.

Egress Protect

85. By default, ESI and EG provide adequate logging of policy changes, user authentication⁴, access, and package management. This logging **must remain enabled**.
86. Audit logs must be regularly reviewed for anomalies (for example crashes, excessive authentication or authorisation failures, etc). This may include integration into existing monitoring systems, as appropriate.

Maintenance and Updates

87. To maintain the security of a deployment, the latest compatible version of Egress Protect, Microsoft Windows, Microsoft Outlook, and the chosen Anti-Virus solution must be used. These must be regularly updated (automatically or manually), without undue delay with the relevant manufacturer's security patches and hotfixes.

User Education

88. As part of the EPC deployment, users should be provided with training in the appropriate usage of the Egress Protect tools, which should include at least the following topics:
 - a. Identification and mitigation of common issues;
 - b. Selection and storage of appropriate passphrases.
89. Users that do not have the EPC installed on their computers must be informed, prior to using an email system set up with the EG Server that receiving an encrypted package indicates that the gateway was unable to decrypt it.

⁴ The audit logs provide information regarding account activity notification for previous authentication attempts (whether failed or successful), in case this information is required but it is not immediately available after a successful login.



Chapter 4 - Security Incidents

Incident Management

90. In the event of a Security Incident that results in the compromise of information protected by Egress Protect, the local IT security incident management policy must ensure that the Department Security Officer (DSO) is informed.
91. NCSC must be contacted if a compromise occurs that is suspected to have resulted from a failure of Egress Protect.

Tampering and Other Compromises

92. The following table provides instructions to be followed if you suspect or identify a compromise to the ESI Server and the EG Server. The actual procedures and policies must be complied with, in conjunction with system accreditation requirements.

Component	Protective Marking	Action if lost or compromised
ESI Server	(see the *Note below)	<p>If the ESI Server becomes compromised:</p> <ol style="list-style-type: none"> 1. The ESI Server must be reformatted and reinstalled, with the ESI Server configuration restored from a back-up. 2. If the SQL database originally resided on the ESI Server, restore the database from a backup after the reinstall. Backup and restoration of the SQL database should be performed using Microsoft SQL built-in database backup and restoration tools. For further information please refer to Microsoft SQL documentation. 3. Generate a new DB key for the Egress keychain. This new DB key will be used to encrypt package keys stored in the SQL database. The old DB key must be retained in the keychain to allow previous package keys to be accessed. To generate a new DB key, use keychain.exe which is available in the following folder: c:\program files\egress\sdx\utils. 4. Restore the ESI configuration files from backup:

Egress Protect

		<p>C:\Program Files\Egress\sdx\keychain.xml C:\Program Files\Egress\sdx\au\auselfhost.exe.config C:\Program Files\Egress\sdx\cp\web.config C:\Program Files\Egress\sdx\cp\bin\cp.config C:\Program Files\Egress\sdx\cp\bin\cpselfhost.exe.config C:\Program Files\Egress\sdx\ui\web.config</p> <ol style="list-style-type: none"> 5. The existing TLS certificate must be revoked and a replacement TLS certificate issued by contacting the issuing Certificate Authority. 6. The existing Egress Federation certificate must be revoked and a replacement certificate issued by contacting the issuing Certificate Authority. 7. Reset all Egress Protect service account passwords, including the EG account password. Configure the EG Servers with the new password. 8. If user account passwords have been compromised, configure the affected user accounts as "Must Change Password on next sign in" and/or disable the affected accounts until the password is reset by the associated users.
EG Server	(see the *Note below)	<p>If the EG Server becomes compromised:</p> <ol style="list-style-type: none"> 1. Reset the EG account password. 2. Reformat and reinstall the server. Restore the Gateway configuration file from a backup. No data is stored on the EG Server, so no data will be lost during reformatting. 3. Restore the EG configuration files from backup: C:\Program Files\Egress\sdx\keychain.xml C:\Program Files\Egress\sdx\siteinfo.xml C:\Program Files\Egress\sdx\gateway\bin\gatewayselfhost.exe.config C:\Program Files\Egress\sdx\gateway\bin\config*.* 4. Contact the issuing Certificate Authority to have the TLS certificate used by the EG Server revoked and a new replacement certificate issued for use with the reinstalled EG Server.



EPC Computer	(see the *Note below)	<p>If the EPC computer becomes compromised:</p> <ol style="list-style-type: none">1. Reset the Egress Protect account password for all Egress Protect accounts that may have been accessed from the compromised computer.2. Reformat and reinstall the computer.3. Reinstall the Egress Protect Client software.
--------------	-----------------------	--

Table 5 – Actions to Take After Actual or Suspected Compromise to ESI Server, EG Server and EPC Computer

***Note:** Each component would take on the maximum classification level of the data processed on it.



Egress Protect

Chapter 5 - Disposal and Destruction

Wipe Hard Disk

4. When the ESI Server and/or the EG Server are no longer required, sensitive data will be overwritten with null bytes during the uninstallation of the Egress Protect software. However, if additional formal assurance is required, the drive should be securely erased using an application that provides a Certificate of Destruction.

Delete Remote Databases

5. Both the ESI Server and the EG Server use SQL databases to store sensitive data. The SQL database can be located either on the same server as the Egress Protect server software or on a remote server:
 - a. If the database was located on the local server, then the database will be securely erased as outlined in the Wiping the Hard Disk section above.
 - b. If the database was located on a remote server, then the Egress Protect database must be securely erased by the database server Administrator after the uninstallation of the Egress Protect server.

Routine Destruction

6. If one or more physical disks that were used to host an ESI and/or EG installation are then to be destroyed/disposed of, that process must be performed in accordance with IAS5 [k].

Emergency Destruction

7. Egress Protect does not provide any functionality for Emergency Destruction.



References

- [a] CPA Security Characteristic: Gateway Email Encryption, v1.1, 25/10/2018, https://www.ncsc.gov.uk/files/CPA-SC_Gateway_Email_Encryption_1-1.pdf
- [b] CPA Security Characteristic: Desktop Email Encryption, v1.1, 25/10/2018, https://www.ncsc.gov.uk/files/CPA-SC_Desktop_Email_Encryption_1-1.pdf
- [c] Egress Protect CPA Assurance Maintenance Plan, v0.2, June 2020
- [d] Verify Egress Installation File Integrity, v3.0, 15 May 2020
- [e] Egress Server Infrastructure and Gateway, Installation and Configuration Guide, v3.0, 15 May 2020;
Egress Gateway Configuration Guide, v3.0, 15 May 2020;
Egress Gateway Installation Guide, v3.0, 15 May 2020
- [f] Egress Protect Gateway Installation Guide, v2.0, 19 December 2019
- [g] Egress Desktop Client Deployment Guide, v19.10.30727
- [h] Egress Protect Installation and Uninstallation Support Guide, v2.0, 19 December 2019
- [i] Egress Protect TLS Configuration Guide, v2.0, 19 December 2019
- [j] Egress Protect Policy Enforcement, v2.0, 19 December 2019
- [k] HMG IA Standard No. 5, Secure Sanitisation, v5.1, December 2014

Egress documents can be requested from the Egress Support Centre
<http://www.egress.com/contact-us/>

Egress Protect

Glossary

ASLR	Address Space Layout Randomisation
AV	Anti-Virus
CA	Certificate Authority
CPA	Commercial Product Assurance
CPU	Central Processing Unit
CRL	Certificate Revocation List
DB	Database
DEP	Data Execution Prevention
DMZ	Demilitarised Zone
DoS	Denial of Service
ECP	External Connection Point
EG	Egress Gateway
EPC	Egress Protect Client
ESC	Egress Switch Client (<i>deprecated, see EPC</i>)
ESG	Egress Switch Gateway (<i>deprecated, see EG</i>)
ESI	Egress Switch Infrastructure (<i>deprecated, see ESI</i>)
ESI	Egress Server Infrastructure
EWA	Egress Web Access
FIPS	Federal Information Processing Standard
HMG	Her Majesty's Government
HTML	Hypertext Mark-up Language
ICP	Internal Connection Point
IIS	Internet Information Services
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
OWA	Outlook Web Access



RDP	Remote Desktop Protocol
SC	Security Characteristic
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UI	User Interface
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XML	Extensible Mark-up Language

Egress Protect

Customer Feedback

NCSC Information Assurance Guidance and Standards welcomes feedback and encourage readers to inform NCSC of their experiences, good or bad in this document. We would especially like to know about any inconsistencies and ambiguities. Please use this page to send your comments to:

Customer Support
NCSC
A2b
Hubble Road
Cheltenham GL51 0EX
(for the attention of IA Policy Development Team)

Fax: (01242) 709193 (for UNCLASSIFIED FAXES ONLY)

Email: enquiries@ncsc.gov.uk

For additional hard copies of this document and general queries please contact NCSC enquiries at the address above

PLEASE PRINT

Your Name:

Department/Company Name and Address:

Phone number:

Email address:

Comments:

< INSERT THE PROTECTIVE MARKING ON COMPLETION OF CUSTOMER FEEDBACK >



< INSERT THE PROTECTIVE MARKING ON COMPLETION OF CUSTOMER FEEDBACK >

OFFICIAL

IA
NCSC
A3e
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@ncsc.gov.uk

© Crown Copyright 2013. Communications on NCSC telecommunications systems may be monitored or recorded to secure the effective operation of the system and for other lawful purposes. This information is exempt under the Freedom of Information Act 2000 and may be exempt under other UK Information legislation. Refer any FOIA queries to NCSC on 01242 221491 x30306 or email ncscinfoleg@ncsc.gov.uk.

OFFICIAL