Egress Desktop Client

User Guide

Confidentiality statement

This document contains information confidential and proprietary to Egress Software Technologies. It shall not be disclosed in whole or part by the recipient to any third party or to any employees other than those who have a need to know such information. It shall not be duplicated or used by the recipient for any purpose other than to evaluate Egress Software Technologies products and services.

No part of this document may be reproduced, distributed, stored in a database or retrieval system, or transmitted in any form or by any means, without the exclusive and written permission of Egress Software Technologies. No liability is assumed for damages resulting from the use of the information contained herein.

Copyright notice

Contents

Egress Desktop Client

User guide

Egress Software Technologies is the leading provider of data privacy and risk management tools designed to secure all forms of electronic information and delivered to customers in both the Public and Private Sectors via a single platform: **Egress**.

As the first, and currently only, NCSC CPA IL3 Foundation Grade-certified email encryption product on the market, **Egress Email and File Protection** enables customers to share highly sensitive information over the internet, without the need to manage external third party credentials.

This guide details the installation and use of the **Egress Desktop Client** version 5.12 for Microsoft Windows, including the Microsoft Outlook Add-in, Large File Transfer, Classification and Threat Protection features. Also explained is integration with Egress Secure Workspace.

Installation

System requirements

Please ensure that the following minimum requirements are met before installing the Egress Desktop Client:

- Microsoft Windows Vista/7/8/10
- Microsoft Office 2010/13/16/ProPlus
- Microsoft .NET 4.5 or later
- Microsoft Visual Studio 2010 Tools for Office Runtime (VSTO)

The Desktop Client can run on 32-bit and 64-bit versions of Windows.

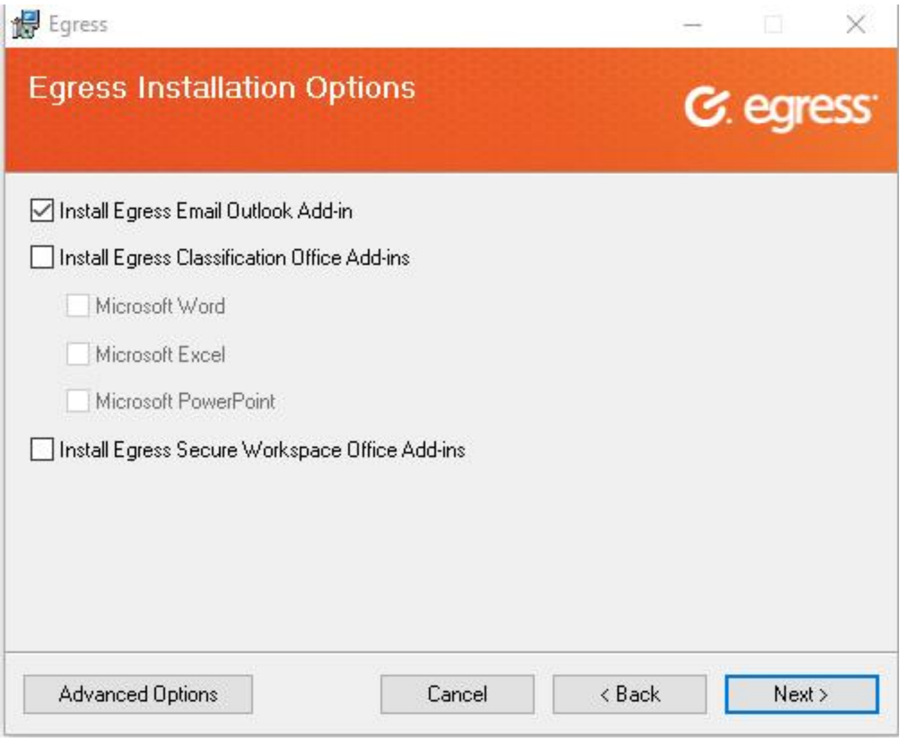
Installing the Desktop Client

- The installation files are available to download free of charge from the Egress website (www.egress.com) or can be obtained from a member of the Egress Support team.
- The installation process is a simple click-through installer delivered in an .exe package. The .exe package includes the prerequisites .NET 4.5 and VSTO 2010.
- To run the installer, you must have administrator privileges on the target machine. Local administration rights are sufficient.
- The Desktop Client can also be provided as an .msi package and deployed silently using any software deployment application, including Active Directory Group Policy and MS SCCM. For further information, please see the Egress Desktop Client Deployment Guide, available from your Egress Technical Account Manager.

To install the Desktop Client software, complete the following steps:

1. Sign in to the target machine as an administrator and run the Egress installer. The following dialogue will be displayed. Press **Next**.
2. Select **I Agree** to accept the Egress Software Technologies Ltd license agreement and then press **Next** to continue.
3. Choose the preferred installation path and press **Next** to continue.

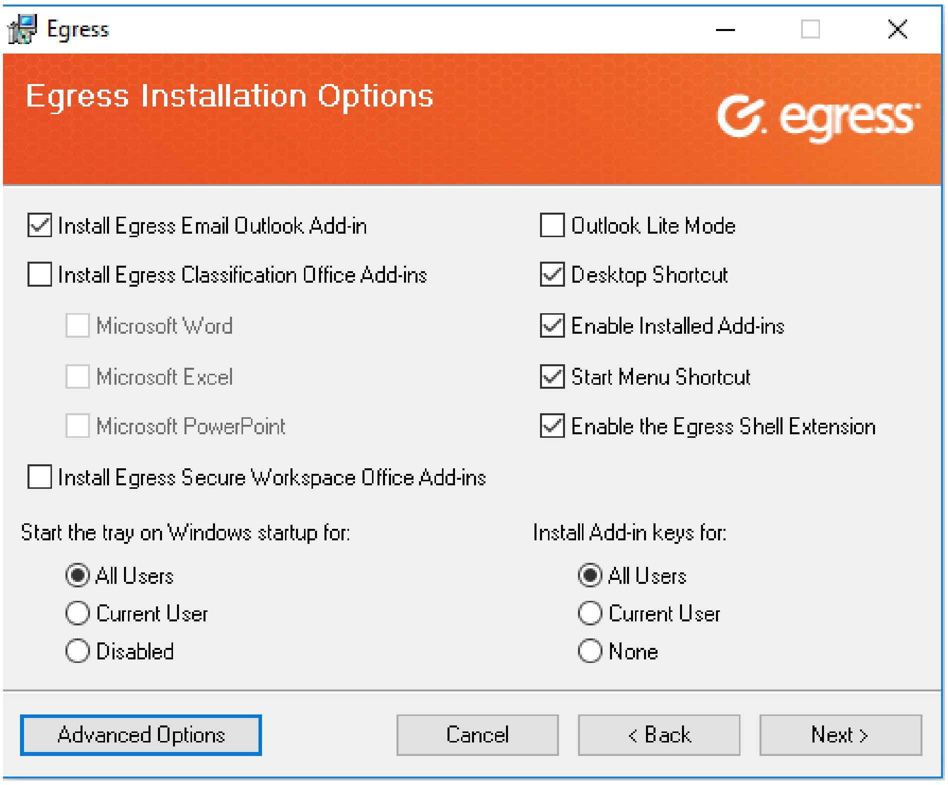
You are given the option to install the Egress Outlook Add-in. The Outlook Add-in provides seamless integration with Microsoft Outlook and its installation is highly recommended. This option will only be available if Microsoft Outlook is detected during the installation.



☑ Install Egress Email Outlook Add-in
☐ Install Egress Classification Office Add-ins
☐ Microsoft Word
☐ Microsoft Excel
☐ Microsoft PowerPoint
☐ Install Egress Secure Workspace Office Add-ins

You are also given the option to install Egress Discovery and Classification Add-ins and Secure Workspace Office Add-ins at this stage.

4. Select the tick boxes next to the features you wish to install.
5. Select **Advanced Options** to choose to install additional features. Press **Next** to begin the installation.



☑ Install Egress Email Outlook Add-in
☐ Install Egress Classification Office Add-ins
☐ Microsoft Word
☐ Microsoft Excel
☐ Microsoft PowerPoint
☐ Install Egress Secure Workspace Office Add-ins

☐ Outlook Lite Mode
☑ Desktop Shortcut
☑ Enable Installed Add-ins
☑ Start Menu Shortcut
☑ Enable the Egress Shell Extension

Start the tray on Windows startup for:
● All Users
○ Current User
○ Disabled

Install Add-in keys for:
● All Users
○ Current User
○ None

6. Press **Close** to complete the installation. The Egress icon should now appear in your system tray.

Welcome screen

The welcome screen is displayed once the installer has finished and after the first sign-in. It presents two main options. You can hide the welcome screen by deselecting **Show this window when you sign in**.

- **Create account**: Click this link to register for a Account if you do not already have an Egress ID.
- **Sign in**: if you already have an ID, click this link to sign into the Client with your credentials.

Getting started

You should now have installed the primary components of the Egress platform on to your workstation:

1. **Package Creator**: Enables you to create secure packages.
2. **Package Library**: Allows you to view previously created packages and change their properties, as well as providing delivery reports and a full audit trail.
3. **Outlook Add-in**: Provides seamless integration with Microsoft Outlook 2010/2013/16/ProPlus. (Optional. Recommended.)
4. **Classification Office Add-in**: Provides classification integration with Word, Excel and PowerPoint using the Ribbon. (Optional)
5. **Secure Workspace Office Add-in**: Provides integration between the desktop and Secure Workspace, for secure file storage, sharing and collaboration. (Optional)

Creating a account

Before you can use Egress you need to create an Account by doing one of the following:

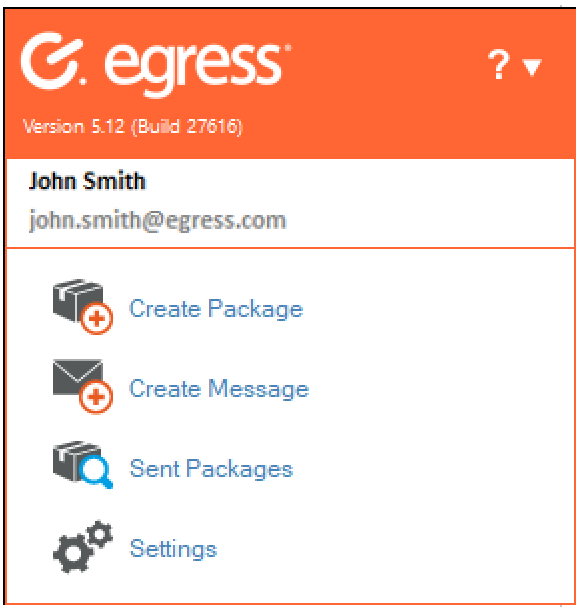
- Visiting http://www.egress.com/register/ and signing up.
- Using the Client and selecting **Create account** from the welcome screen or system tray.
- Receiving an invitation from the Egress account administrator within your organisation.

Business users with a paying subscription to Egress can send an unlimited number of secure packages. To use the service free of charge, you must include a paying subscriber in the To or Cc field. Free users are also provided with 25 credits when they sign up to the service, enabling them to send secure packages to 25 other non-paying users.

Signing in

If you have not signed in to the Client software via the welcome screen you can sign in using the system tray icon.

- Select the icon in the tray and choose **Sign in**. Enter your credentials into the window that opens.



Alternatively, you may have been signed in automatically if your organisation is using Active Directory Federation Services (ADFS).

Using Egress in the system tray

The System Tray allows quick access to the main features of the software. To access it, select the icon in the Windows system tray.

- **Create package** – opens the Package Creator and enables you to create new secure packages.
- **Create message** – if MS Outlook is installed, this opens a new Outlook message. If MS Outlook is not installed, it will open a new secure message via Web Access.
- **Sent packages** – Allows you to browse previously created secure packages and configure their properties.
- **Settings** – update your personal information and configure transfer settings for uploads.
- **Sign out** – sign out of the software. This option will not be available if you are signed in via Active Directory Federation Services.

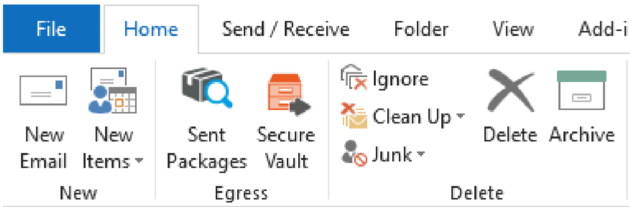
A notification displays below the **Sign Out** button on the System Tray if you have any pending access requests to secure packages.

- Click on the link to review these pending access requests within the **Package Library**.

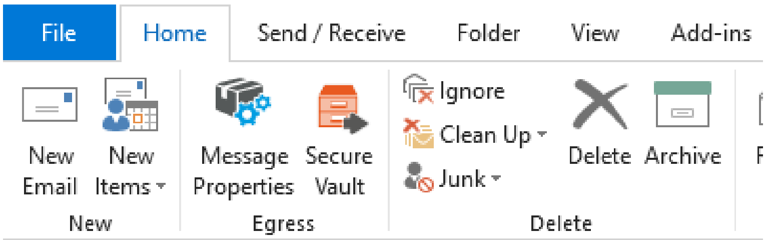
Using the Microsoft Outlook add-in

The Egress Outlook add-in provides transparent package creation from within Outlook 2010 and 2013. When the Outlook Add-in is installed, extra buttons become available in the ribbon:

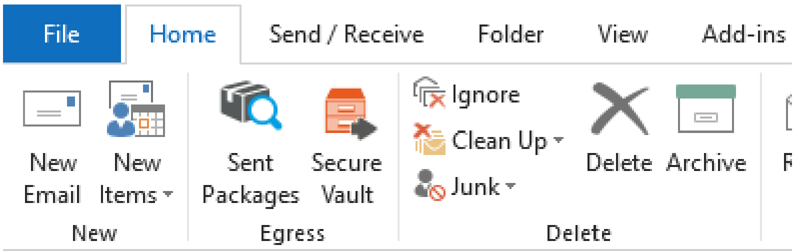
- When viewing a received message, use the **Sent Packages** icon to access the Package Library.



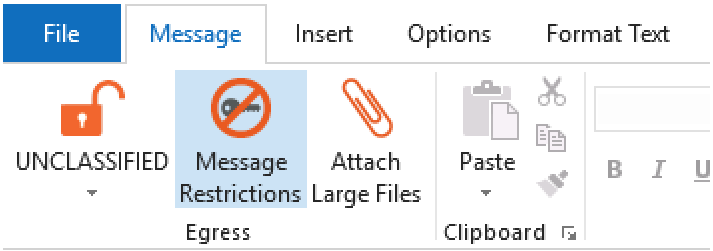
- When viewing a sent encrypted message, use the **Message Properties** icon to view the package properties of the package you are currently viewing



- When viewing your inbox or sent items, under the **Home** tab you will also see **Sent Packages**. In addition if you have any pending access requests you will see an extra button showing how many pending requests you currently have.

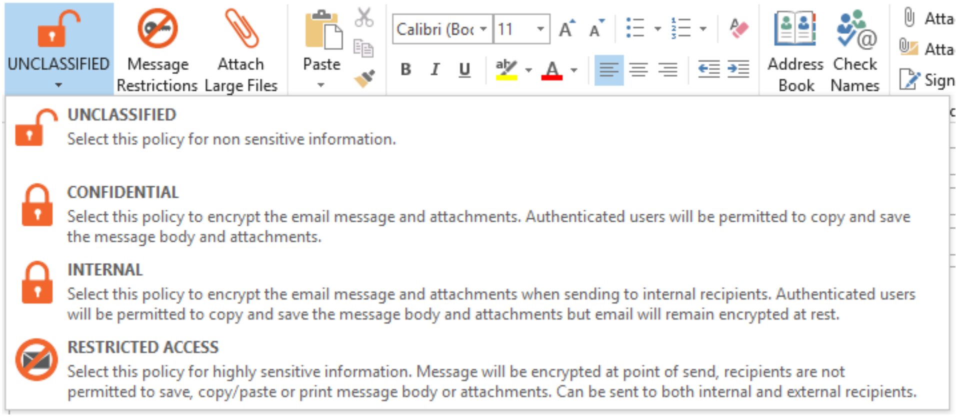


- When composing a new email, three buttons are available under the **Message** tab, for choosing the email classification, message restrictions and for attaching large files.



Sending a secure email

1. Open a new message in Outlook, completing the **To**, **Cc** and **Subject** fields and composing your message as normal.
2. To send the email securely, click on the dropdown menu and choose your desired encryption type. The options available here are dictated by your business account's policy and so some options may not be available.



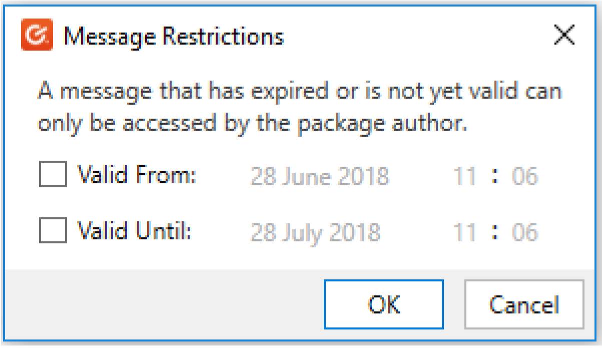
UNCLASSIFIED
Select this policy for non sensitive information.

CONFIDENTIAL
Select this policy to encrypt the email message and attachments. Authenticated users will be permitted to copy and save the message body and attachments.

INTERNAL
Select this policy to encrypt the email message and attachments when sending to internal recipients. Authenticated users will be permitted to copy and save the message body and attachments but email will remain encrypted at rest.

RESTRICTED ACCESS
Select this policy for highly sensitive information. Message will be encrypted at point of send, recipients are not permitted to save, copy/paste or print message body or attachments. Can be sent to both internal and external recipients.

3. Press **Message Restrictions** to configure time restrictions for the secure email. These restrictions are optional and can be changed at any point, even after the email has been sent.



A message that has expired or is not yet valid can only be accessed by the package author.

□ Valid From: 28 June 2018 11 : 06

□ Valid Until: 28 July 2018 11 : 06

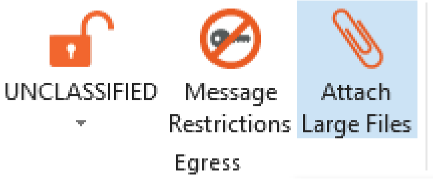
4. Press **Send** as usual once your message is complete.

Egress Large File Transfer

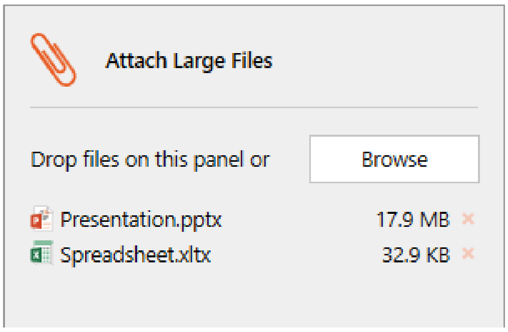
Often, email clients limit the maximum file size of attachments. Egress Large File Transfer (LFT) lets you send large files securely by uploading them to hosted Cloud storage. You can use the integrated sidebar in Outlook or the downloadable Egress Client.

Using the LFT sidebar in Outlook to send large files

If LFT is enabled, attachments greater than 10MB will be added to LFT by default and the **Attach large files** icon is displayed in the Outlook ribbon of an email.



1. Open a new email in Outlook and select **Attach Large Files** to open the LFT sidebar.
2. Select files to attach by dragging and dropping them into the sidebar or manually select them by pressing **Browse**.
3. To send the email with the large files attached, simply press **Send** as normal.



Attach Large Files

Drop files on this panel or

Presentation.pptx	17.9 MB
Spreadsheet.xltx	32.9 KB

Note: Once the LFT sidebar is opened, any files attached to the email will be sent via large file transfer regardless of size.

- To remove any files attached to the sidebar, either press the **X** button next to the specific file or select the file and press the **Delete** button on your keyboard.

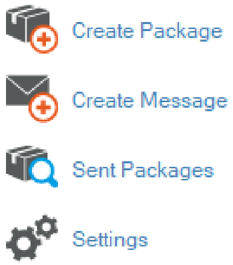
Sending large files without the Outlook sidebar

Large File Transfer can also be configured so that the sidebar is disabled while the LFT function remains enabled. The **Attach large files button** will not be displayed and there will be no sidebar, but the total attachment size will be displayed. In this mode, if the attachments are under the default size limit for large file transfer (10MB), they will still be sent as a normal email attachment. As soon as the size limit is exceeded, the files will be converted to **.** files and sent by large file transfer.

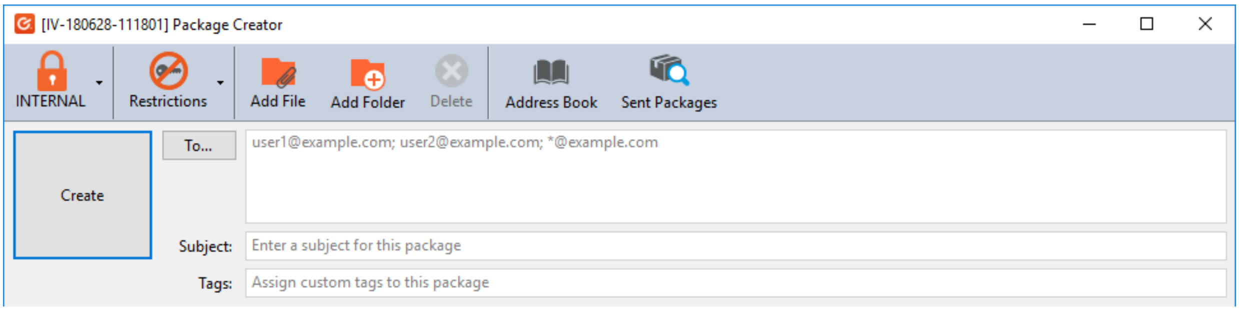
Using the Egress Client to send large files

You can also use the package creator to send large files.

1. Press the Egress icon in the system tray to open the Client, then press **Create Package**.



2. In the **Package Creator** window, use the **Add File** and **Add Folder** buttons to attach the files you wish to send.
3. Fill in the **To** and **Subject** fields.

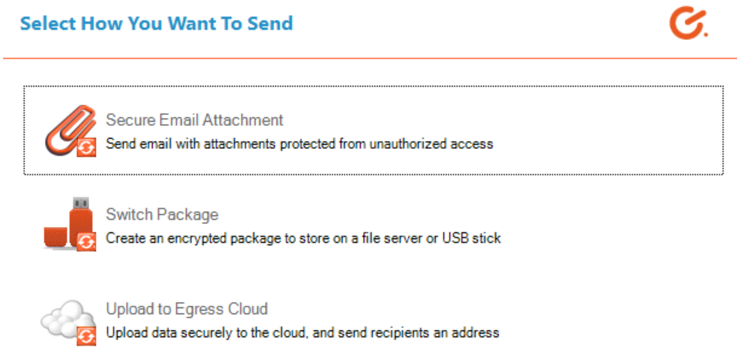


user1@example.com; user2@example.com; *@example.com

Enter a subject for this package

Assign custom tags to this package

4. Add date and time restrictions if required by selecting **Restrictions**. Select **Protect** to choose the type of security policy you wish to use.
5. Once complete, press **Create**.
6. In the window that opens, choose **Upload to Egress Cloud**.



Secure Email Attachment
Send email with attachments protected from unauthorized access

Switch Package
Create an encrypted package to store on a file server or USB stick

Upload to Egress Cloud
Upload data securely to the cloud, and send recipients an address

7. To notify recipients of the large files you have sent, check the **Send notification email to package recipients** in the **Package creation complete** window and press **Finish**. A new Outlook email will open, containing a link to access the secured package. Customise the message as required and press **Send**.

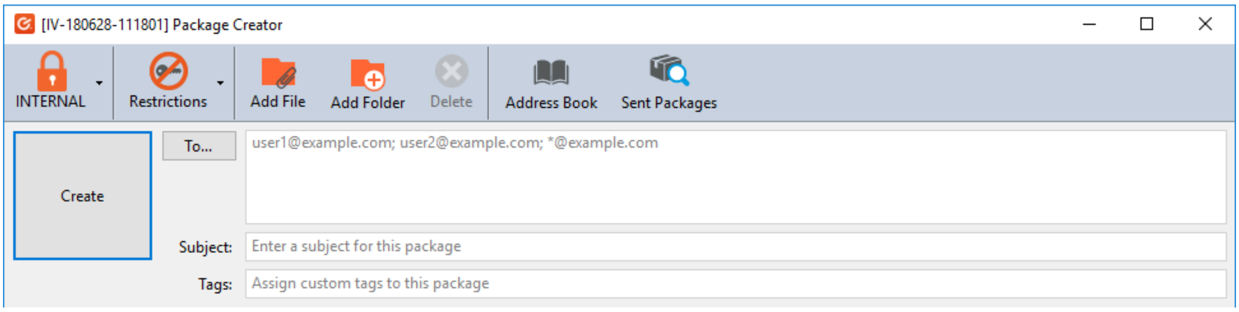
8. Alternatively, you can send the download URL manually. Press the icon in the system tray and select **Sent Packages**. Open the specific package and select the **Package properties** tab to access the link.

You can also transfer large files securely by burning them onto a disc or copying them onto a USB stick. The package creator compresses the large data as a **.** file.

Creating a secure package

The Package Creator lets you create secure packages and assign access rights to that package. To create a secure package:

1. Select **Create Package** from the system tray menu, or right click any file or folder and select **Secure with** .
2. In the **Package Creator** window, use the **Add File** and **Add Folder** buttons to attach the files you wish to include in the secure package.
3. You can fill in the **To** and **Subject** fields if you wish to send the package or you can leave them blank. Recipients can also be added after creating the package.



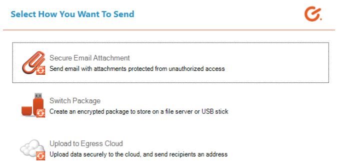
[IV-180628-111801] Package Creator

To...: user1@example.com; user2@example.com; *@example.com

Subject: Enter a subject for this package

Tags: Assign custom tags to this package

4. Add date and time restrictions if required by selecting **Restrictions**. Also, select **Protect** to choose the type of security policy you wish to use.
5. Once complete, press **Create**.
6. In the window that opens, you can choose how you want to use the secure package. is very flexible, and you can:
   - ○ **Attach it to an email**
   - ○ **Store it on a file server or USB**
   - ○ **Upload it to the Egress Cloud**



Select How You Want To Send

Secure Email Attachment
Send email with attachments protected from unauthorized access

Switch Package
Create an encrypted package to store on a file server or USB stick

Upload to Egress Cloud
Upload data securely to the cloud, and send recipients an address

Please note, the options displayed in this window are configurable by your system administrator, so you may not see all of these features.

Sending a secure package as an email attachment

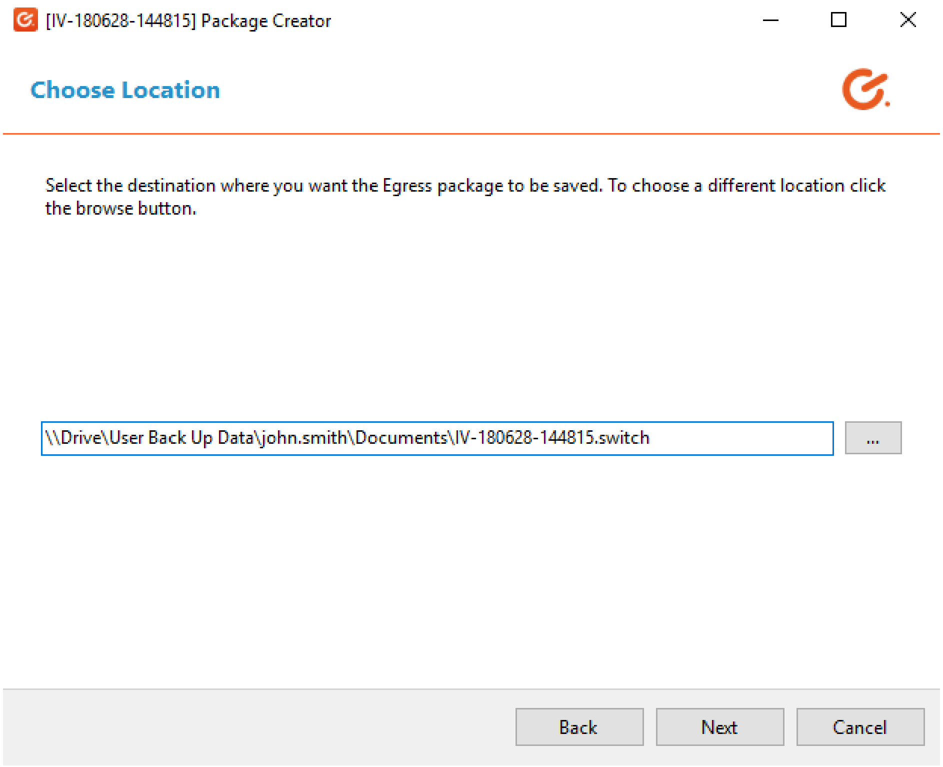
Select **Secure Email Attachment** to encrypt files and send them as a secure attachment in an encrypted email. A progress bar is displayed as the package is created. Once complete, a summary of the package creation is shown.

1. Select **Secure Email Attachment** in the options window that appears when creating a secure package. Press **Finish** to open a new email within Outlook. The recipients and subject will be populated with the recipients and subject defined when creating the package if you chose to define them then. If you left those fields blank in the package creator, add the recipients and subject now.
2. Click **Send** to send the attachment. The email contains instructions on how to open the secure attachment via the Client, Reader or using Web Access. The recipients will need to create an Egress ID to access secure attachments.

Storing a secure package

On the package options window, choose **Package** to encrypt files and save them as a secure package on your computer or removable media. Use this option if you want to save the secure package for now, with the option to send it at a later date.

1. On the **Choose Location** screen, browse to your preferred save location for the package. This can be a drive on your computer or on removable media such as a USB stick. Once selected, press **Next**.



Select the destination where you want the Egress package to be saved. To choose a different location click the browse button.

\\Drive\User Back Up Data\john.smith\Documents\IV-180628-144815.switch

A progress bar is displayed as the package is created. When it completes, a summary of the package creation is shown.

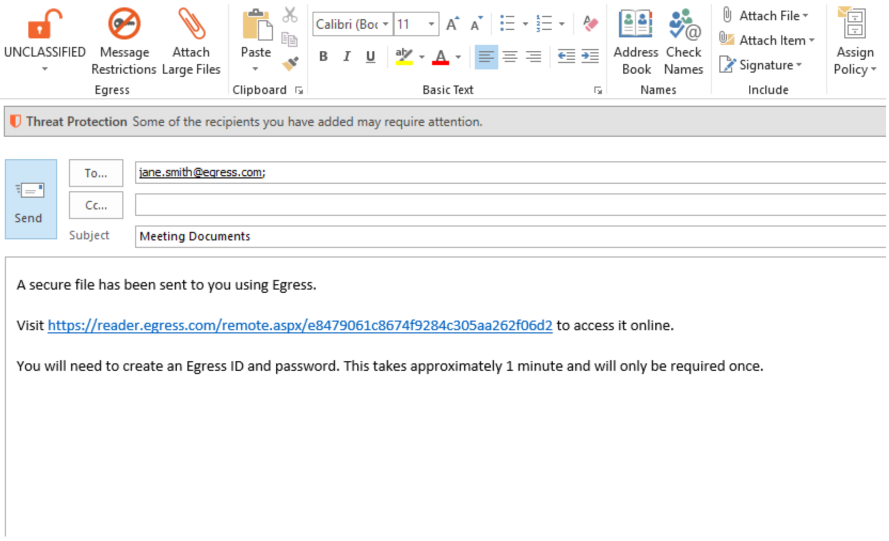
2. Click **Finish**. The file location will open in Windows Explorer if you selected this option on the summary screen.

Uploading a secure package to Egress Cloud

In the package options window, choose **Upload to Egress Cloud** to encrypt files and upload them to the Egress Cloud. After choosing this option, you are given the option of copying the link to a file or to your clipboard.

1. Select **Upload to Egress Cloud**. Choose whether to copy the link to a file or to your clipboard.
2. Press **Finish**. If you specified recipients in the initial package creation, a new email within Outlook will open when you do this. The email contains a web link which the recipient can use to retrieve the secure package online. If you did not specify recipients when creating a package then a new email will not open.

3. If you require the package at a later date you can access it by going to the system tray and choosing **Sent Packages**. This will display a list of previously created packages.



Threat Protection Some of the recipients you have added may require attention.

To... jane.smith@egress.com;

Subject Meeting Documents

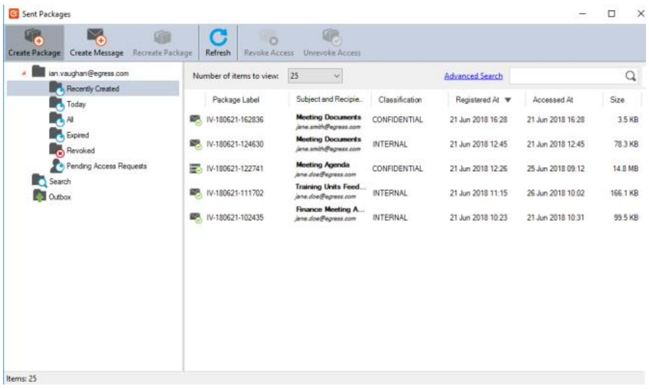
A secure file has been sent to you using Egress.

Visit https://reader.egress.com/remote.aspx/e8479061c8674f9284c305aa262f06d2 to access it online.

You will need to create an Egress ID and password. This takes approximately 1 minute and will only be required once.

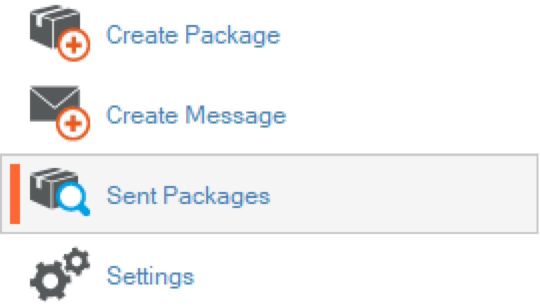
Managing secure packages

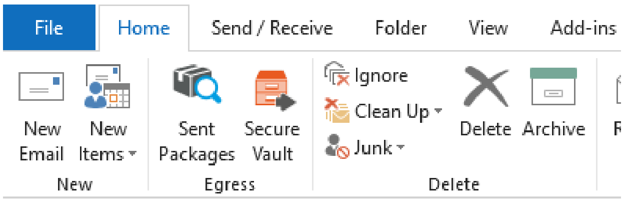
Once a Package is created, the author remains in control of that package even after it has left the network where it was created. The Package Library provides a way to manage and control the lifecycle of all packages that you have created.



Package Label	Subject and Recipie...	Classification	Registered At	Accessed At	Size
IV-180621-162836	**Meeting Documents** *jane.smith@egress.com*	CONFIDENTIAL	21 Jun 2018 16:28	21 Jun 2018 16:28	3.5 KB
IV-180621-124630	**Meeting Documents** *jane.smith@egress.com*	INTERNAL	21 Jun 2018 12:45	21 Jun 2018 12:45	78.3 KB
IV-180621-122741	**Meeting Agenda** *jane.doe@egress.com*	CONFIDENTIAL	21 Jun 2018 12:26	25 Jun 2018 09:12	14.8 MB
IV-180621-111702	**Training Units Feed...** *jane.doe@egress.com*	INTERNAL	21 Jun 2018 11:15	26 Jun 2018 10:02	166.1 KB
IV-180621-102435	**Finance Meeting A...** *jane.doe@egress.com*	INTERNAL	21 Jun 2018 10:23	21 Jun 2018 10:31	99.5 KB

Access the package library by selecting **Sent packages** from the system tray menu or the Outlook ribbon.



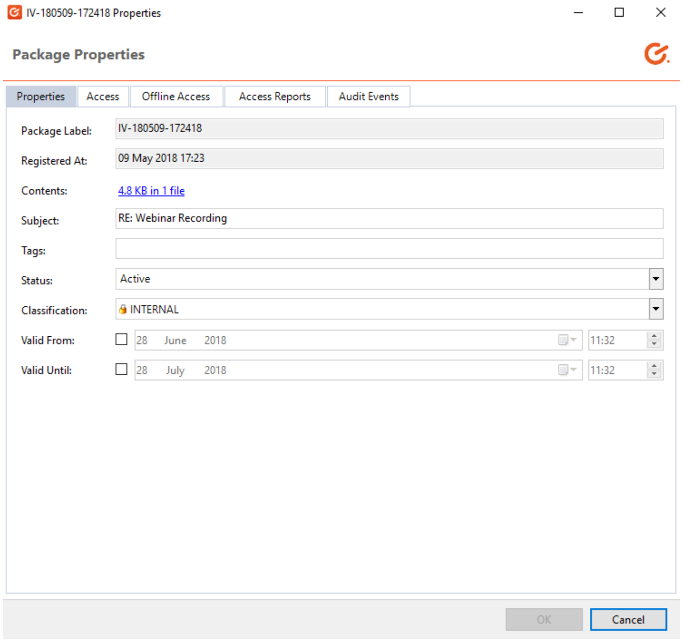


The Package Library organises packages into smart folders. You can easily locate packages based on date, type and classification.

Viewing and editing package properties

The properties (including details, validity and access rights) of a package can be controlled remotely, even if the package has left the physical network.

- To access the properties of a particular package, double click the package in **Sent Packages**, or find the sent secure message in Sent Items and press **Message Properties**.



Package Label: IV-180509-172418

Registered At: 09 May 2018 17:23

Contents: 4.8 KB in 1 file

Subject: RE: Webinar Recording

Tags:

Status: Active

Classification: INTERNAL

Valid From: □ 28 June 2018 11:32

Valid Until: □ 28 July 2018 11:32

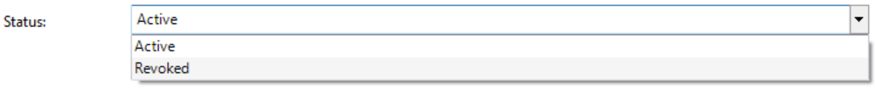
The **Properties** tab displays information about the package, and lets you perform the following actions:

- View the file contents and structure of the package.
- Copy the download URL to send to a recipient.
- Edit the subject of the package.
- Disable access to the package by changing its status.
- Control the classification level of the package.
- Modify or add time restrictions to the package.
- Edit tags assigned to the package.

Disabling access to a package

You can disable access to a package completely, preventing all recipients from accessing its contents.

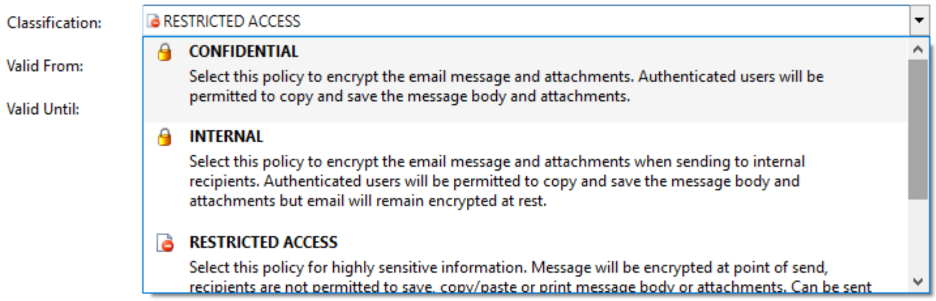
1. Go to **Sent Packages** and double click on the package you wish to disable.
2. In the properties tab, go to **Status** and use the drop-down menu to change the status from **Active** to **Revoked**. Press **OK** to confirm. You can change the status back to **Active** at any time, to re-allow recipient access.



Status: Active

Changing package classifications

You can change the classification of a package after its creation. Package classification dictates what the recipients can do with the contents of the package:



Classification: RESTRICTED ACCESS

Valid From:

Valid Until:

CONFIDENTIAL
Select this policy to encrypt the email message and attachments. Authenticated users will be permitted to copy and save the message body and attachments.

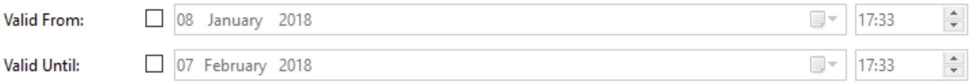
INTERNAL
Select this policy to encrypt the email message and attachments when sending to internal recipients. Authenticated users will be permitted to copy and save the message body and attachments but email will remain encrypted at rest.

RESTRICTED ACCESS
Select this policy for highly sensitive information. Message will be encrypted at point of send, recipients are not permitted to save, copy/paste or print message body or attachments. Can be sent

1. Go to **Sent Packages** and double click on the package whose classification you wish to change.
2. In the properties tab, go to **Classification** and use the drop-down menu to choose a new classification. Press **OK** to confirm.

Adding time restrictions to a package

You can add time restrictions to a package, meaning its contents are only available to recipients in a certain time frame. Use this feature when you want to disable access to a package after a certain point, or prevent access before a specific time. This feature allows you to specify both a date and exact time.



Valid From: □ 08 January 2018 17:33

Valid Until: □ 07 February 2018 17:33

1. Go to **Sent Packages** and double click on the package whose time restrictions you wish to change.
2. In the properties tab, go to **Valid From** and/or **Valid Until** and check the appropriate check box to activate the time restriction. Use the drop-down menus to choose a valid from or valid until date. Press **OK** to confirm.

Editing package tags

When you create a package, you can tag the package with keywords in order to make searching through the Package Library more straightforward. You can also edit these tags at a later date.

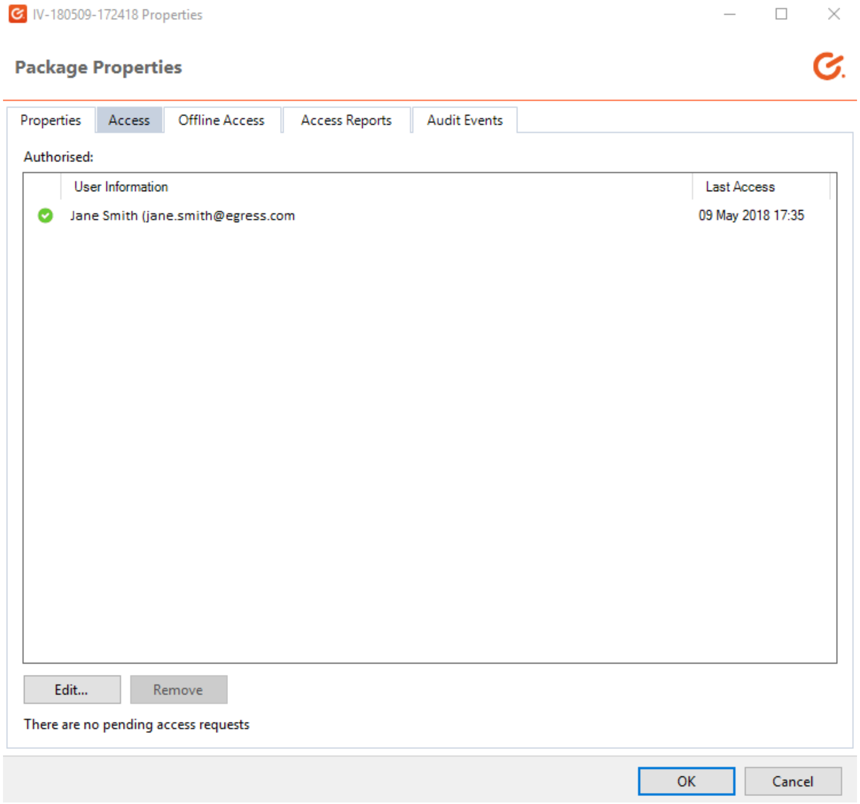
1. Go to **Sent Packages** and double click the package whose tags you wish to change.
2. In the properties tab, go to **Tags** and type in the message box the tags you wish to add to the package, or delete existing tags. Press **OK** to confirm.

Managing access privileges

Each Package has a defined list of recipients able to gain access a particular package. You can set these during package creation by adding recipients to the To field of the package creator. You can also manage this access list after package creation.

1. Go to **Sent Packages** and double click the package whose access you wish to manage.
2. Go to the **Access** tab. The recipients permitted access will be listed in the **Authorised** box.

3. To add people to the access list press **Edit**, then enter the email address of the new recipient or select them from your address book.
4. To remove recipients, select the appropriate recipient in the list and press **Remove**. Press **OK** to confirm.



User Information	Last Access
Jane Smith (jane.smith@egress.com	09 May 2018 17:35

There are no pending access requests

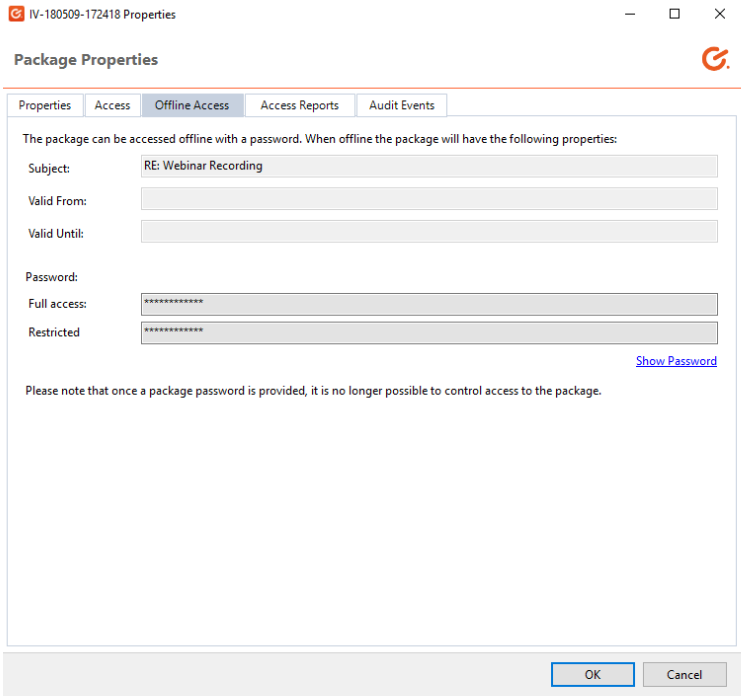
Enabling offline access

The ability to enable offline access to a package is determined via your security policy. It is used in the event that a recipient is unable to access a package due to being offline. You can issue a secure password to enable full offline access.

Important Note: This feature should only be used when there is no opportunity for online access. Once the offline password has been issued, it is no longer possible to change access permissions or revoke the package.

If offline access has been enabled via policy:

1. Go to **Sent Packages** and double click the package you wish to make available offline.
2. Go to the **Offline Access** tab.
3. Use the fields to set the package properties. Press **Show passwords** to reveal the secure passwords. Different levels of access can be determined by policy. Press **OK** to confirm.



The package can be accessed offline with a password. When offline the package will have the following properties:

Subject:	RE: Webinar Recording
Valid From:	
Valid Until:	

Password:

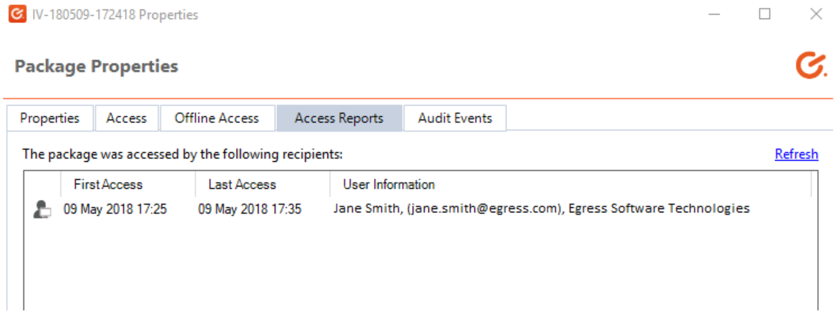
Full access:	************
Restricted	************

Please note that once a package password is provided, it is no longer possible to control access to the package.

Viewing package delivery reports

Delivery reports display when a package was accessed and by whom it was accessed. To view a packages delivery report log:

1. Go to **Sent Packages** and double click on the package whose delivery report log you wish to view.
2. In the package properties window, go to the **Access Reports** tab. The ID and the time of first and last access is displayed for each recipient. Under this is another list showing the recipients who have not yet accessed the secure email.



The package was accessed by the following recipients:

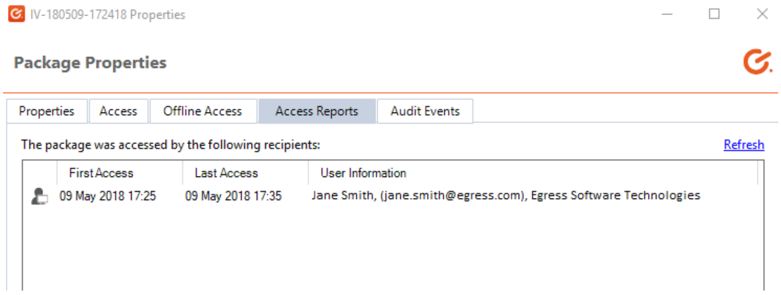
First Access	Last Access	User Information
09 May 2018 17:25	09 May 2018 17:35	Jane Smith, (jane.smith@egress.com), Egress Software Technologies

Viewing package audit events

You can view detailed information about the lifecycle of a secure package. The audit events log shows details of authorised and unauthorised access attempts, with authorised attempts showing as a green tick and failed attempts showing as a red cross. To view a package’s audit events log:

1. Go to **Sent Packages** and double click on the package whose audit events you wish to view.

2. In the package properties window go to the **Audit Events** tab. The events log here displays the following information:
   - **Time**: the date and time when the audit event occurred
   - **Description**: details of the event, including the user and their ID
   - **IP address**: Select an audit event to display in the bottom field the IP address of where the event occurred and which version of the software was used. Press the IP address to view a geographic summary of the location.



The package was accessed by the following recipients:

	First Access	Last Access	User Information
	09 May 2018 17:25	09 May 2018 17:35	Jane Smith, (jane.smith@egress.com), Egress Software Technologies

Secure Access Viewer

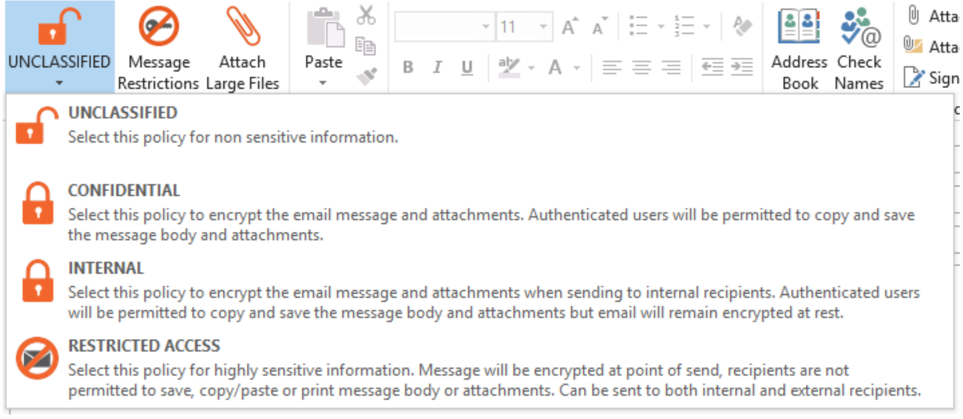
Client version 4.5 and above includes a Secure Access Viewer. The Secure Access Viewer restricts the following recipient actions:

- **Copy / Paste**
- **Save / Save as**
- **Drag & Drop**
- **Print screen**
- **Print**

The Secure Access Viewer is supported on both 32 and 64 bit versions of Windows 7, 8 and 10, and is compatible with Microsoft Office 2010 and above.

Setting up secure access

1. If your policy is set up to enable secure access, open a new email and fill in the **To** and **Subject** fields and write the message body as usual, then select the **Classification** button in the Outlook ribbon.
2. Choose **Confidential – Restricted Access** to prevent recipients from saving, copying or printing the message body or attachments. Send the email.



UNCLASSIFIED
Select this policy for non sensitive information.

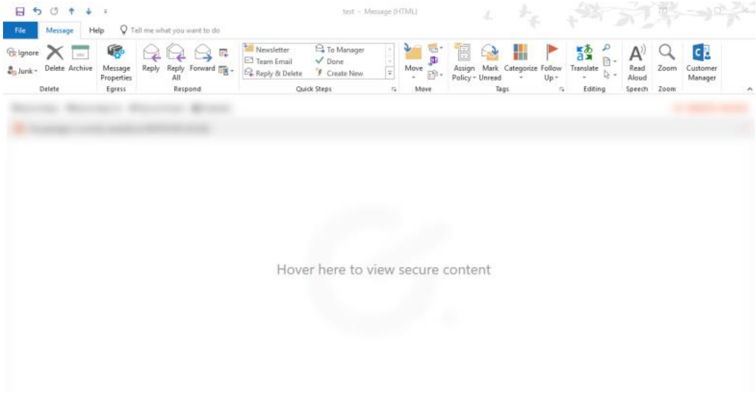
CONFIDENTIAL
Select this policy to encrypt the email message and attachments. Authenticated users will be permitted to copy and save the message body and attachments.

INTERNAL
Select this policy to encrypt the email message and attachments when sending to internal recipients. Authenticated users will be permitted to copy and save the message body and attachments but email will remain encrypted at rest.

RESTRICTED ACCESS
Select this policy for highly sensitive information. Message will be encrypted at point of send, recipients are not permitted to save, copy/paste or print message body or attachments. Can be sent to both internal and external recipients.

Viewing restricted secure emails and attachments

When viewing a restricted access message within Outlook, moving the cursor outside of the message window will cause the window to blur so you can no longer see the contents of the message. Moving the mouse back over the window re-displays the message.



Hover here to view secure content

Any files attached to a restricted access secure message are viewable only within a secure viewer. Recipients are only able to view the document; they cannot copy any text or save the document. A watermark of the recipient’s email address is added to the document in order to mitigate the risk of data leaks.

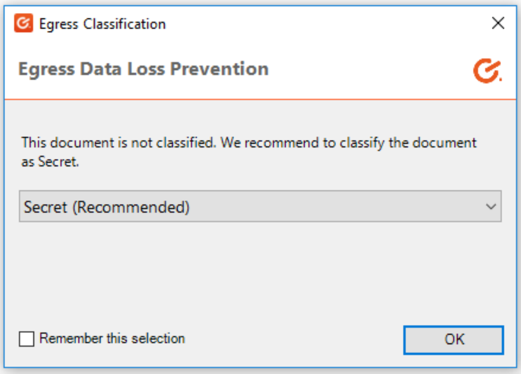
- Double click on the attachment to open it within the secure viewer

Moving the mouse away from the secure viewer window will hide the contents of the attachment.

- Click on the secure viewer to view the contents of the attachments again.

Discovery and Classification

Egress Client versions 4.5 and above includes an Egress Discovery and Classification Office Add-in. The document classifier allows classification of Word documents, Excel spreadsheets and PowerPoint presentations using the Ribbon. You can also classify PDF files on the desktop. Depending on your organisation's specific policy set up, Discovery and Classification can also automatically scan documents for sensitive content and prompt or force classification of a certain level. With policies of this sort in place, when you save an Office document you may be prompted to add a classification label before saving.


Egress Classification

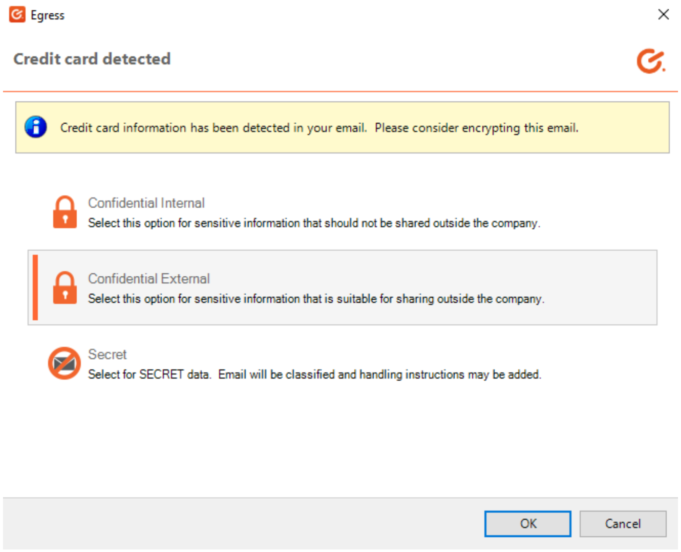
Egress Data Loss Prevention

This document is not classified. We recommend to classify the document as Secret.

Secret (Recommended)

□ Remember this selection

This feature also integrates with Microsoft Outlook, so your organisation may have policies in place to force or prompt encryption of an email if it contains a classified attachment.


Egress

Credit card detected

Credit card information has been detected in your email. Please consider encrypting this email.

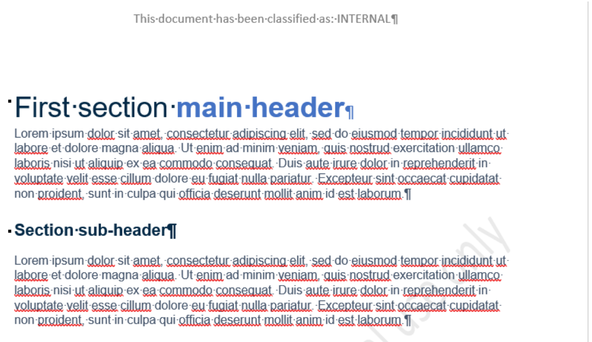
Confidential Internal
Select this option for sensitive information that should not be shared outside the company.

Confidential External
Select this option for sensitive information that is suitable for sharing outside the company.

Secret
Select for SECRET data. Email will be classified and handling instructions may be added.

Microsoft Word

Within Word documents, the specified classification will be applied to the file as banners in the header and footer sections.



This document has been classified as: INTERNAL¶

First section main header¶

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.¶

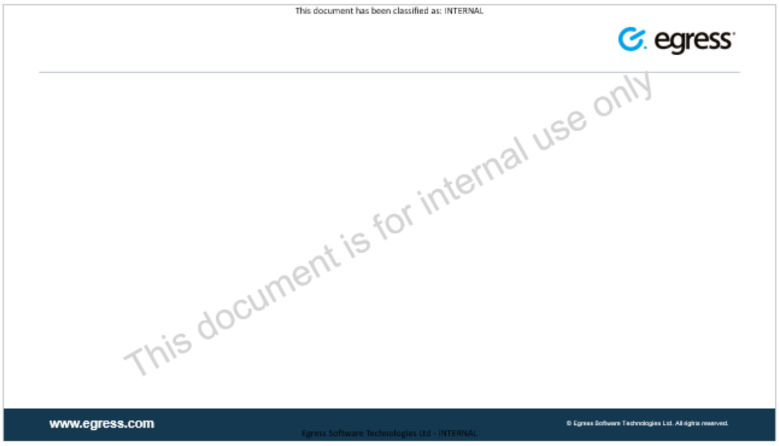
Section sub-header¶

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.¶

Banners are applied on top of anything within the document, except for shapes that have been created in the header or footer section. The banner will be applied to all sections regardless of whether **Different First Page** or **Different Odd & Even Pages** has been selected.

Microsoft PowerPoint

Within PowerPoint presentations, the classification banner is applied to the top and the bottom of each slide. Banners are inserted on top of all shapes within the slides.



This document has been classified as: INTERNAL

www.egress.com

Egress Software Technologies Ltd - INTERNAL

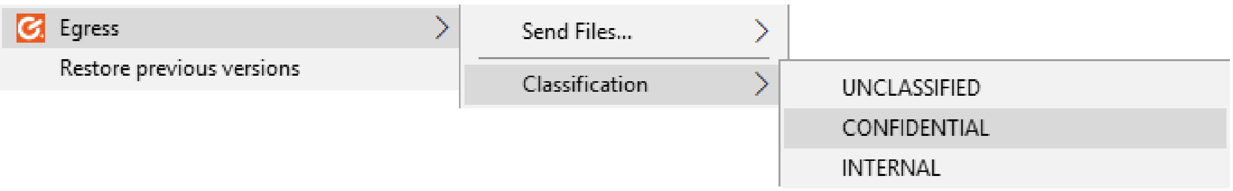
© Egress Software Technologies Ltd. All rights reserved.

Microsoft Excel

Within Excel spreadsheets, the classification banner is applied as a new sheet, inserted at the end of all sheets within the same document. The name of the classification sheet will change according to the current classification selected. If the classification sheet is deleted or the name is modified, then it will be re-created.

Classifying PDF files

Right click on a PDF file on the desktop, select **Egress** - **Classification** and from the drop down choose the classification you wish to apply.



Egress Secure Workspace integration

Users of both the Desktop Client and Secure Workspace can benefit from integration between the two solutions. During installation of the Desktop Client, tick the relevant box to also install the Secure Workspace integration features. Once the Client is installed, the following desktop functionality is available:

Opening Workspace documents in Office

You can access documents stored in a Workspace zone directly from Microsoft Office.

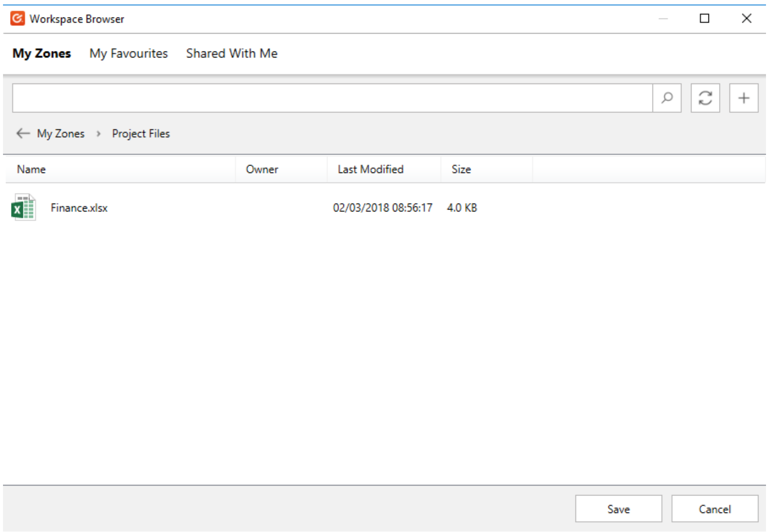
In Word, Excel and PowerPoint:

1. Go to **Open** and you will see a list of the Workspace servers you have access to.
2. Browse to the appropriate zone and search within the zone for a specific file.
3. Click the file to open it within Office.

- From the **Open** menu, you can also manage your zones, create new zones and folders right from this menu in Office.

Saving Office documents back to Secure Workspace

When you have finished working on a document in Word, Excel or PowerPoint, it possible to save it straight into Secure Workspace for sharing and collaboration.



Name	Owner	Last Modified	Size
Finance.xlsx		02/03/2018 08:56:17	4.0 KB

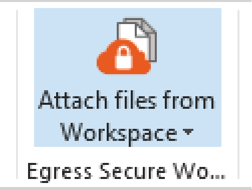
In Office:

1. Go to **Save As.**
2. Choose the Workspace server, zone and folder in which you want to save the document.

Attaching Secure Workspace files to emails

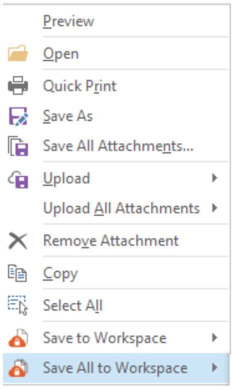
Files stored in Secure Workspace can be added to emails as attachments, as well as sent via a quick share link.

1. In Outlook, open a new email.
2. Use the Outlook Add-in and select **Attach files from Workspace.**
3. Navigate the menu to locate the file you wish to attach in its current Workspace, zone and folder.
4. Write your email as normal, then press **Send**.



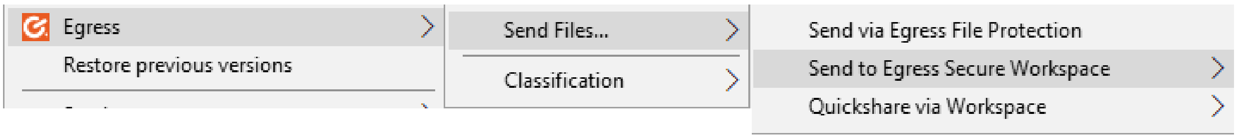
Saving attachments to Secure Workspace

You might also want to send files that you have received straight to a specific zone in Secure Workspace. On the attachment click the drop down menu and choose **Save to Workspace.** Navigate to the desired Workspace server, zone and folder. Alternatively, choose **Save All to Workspace** to save all of the attachments at once.



Sending files to Secure Workspace from the desktop

- Send any file on your desktop or in Explorer to a zone by right-clicking on the file or files and choosing **Egress – Send Files – Send to Workspace** in the menu.


Egress
Restore previous versions
Send Files...
Classification
Send via Egress File Protection
Send to Egress Secure Workspace
Quickshare via Workspace

Egress Threat Protection

Desktop Client 5.0 and above includes support for Egress Threat Protection, a solution developed by Egress to prevent the accidental send – emailing the wrong recipient. It integrates into Microsoft Outlook to provide real-time advice and notifications concerning a user's choice of email recipients.

Note: Threat Protection requires an additional user subscription in order to function.

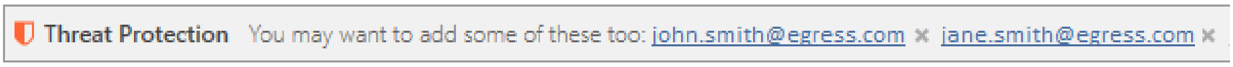
If you are a license holder of Threat Protection, Desktop Client 5.0 and above contains the Outlook add-in to enable protection against the accidental send.

When adding recipients to an email, Threat Protection will automatically respond, and the toolbar will appear. It performs various functions which you can respond to.

Suggested recipients

If the added recipients seem correct, Threat Protection will also suggest additional recipients based on groups of recipients you have previously emailed.

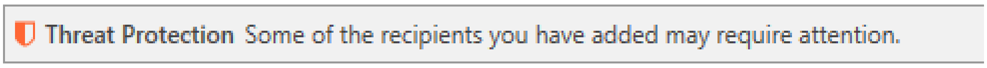
- To add any of the recommended recipients to the email, select the recipient's name from the list. The user will be added to the Cc field.



Threat Protection You may want to add some of these too: john.smith@egress.com ✖ jane.smith@egress.com ✖

Recipient mistakes

If Threat Protection detects a problem with any of the added recipients, a warning will appear.

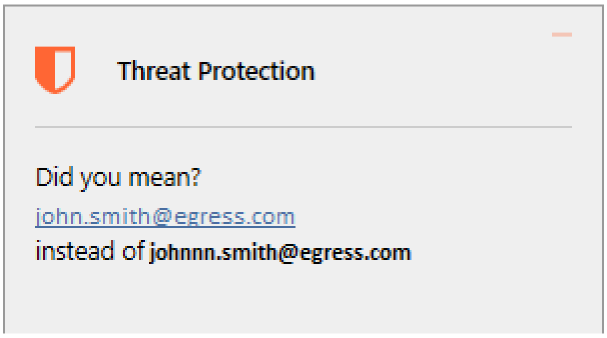


Threat Protection Some of the recipients you have added may require attention.

- Click on the warning to view the sidebar menu and see details of the potential problems with the recipients.

Examples of potential recipient mistakes include:

1. Mistyped recipients

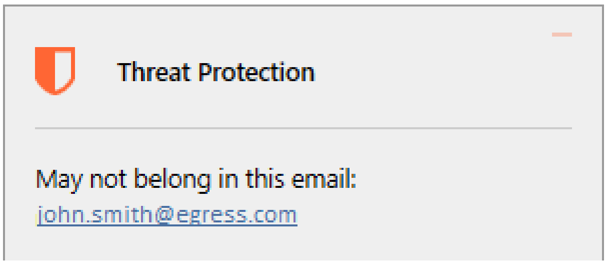


Threat Protection

Did you mean?
john.smith@egress.com
instead of **johnnn.smith@egress.com**

- In the sidebar, select the correct spelling of the recipient address to replace the recipient spelt incorrectly.

2. Incorrect recipients



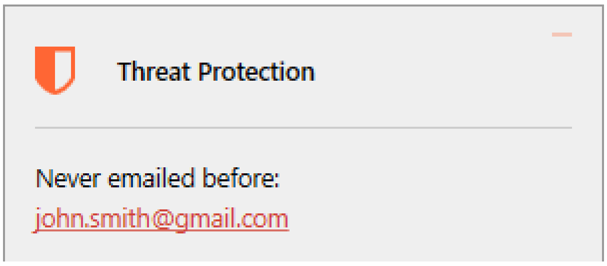
Threat Protection

May not belong in this email:
john.smith@egress.com

- In the sidebar, select the recipient that does not belong in the email to remove them from the message.

3. New recipients

If you have never emailed a recipient before, you may be notified before you send that it is recommended to double check that the recipient address is correct.

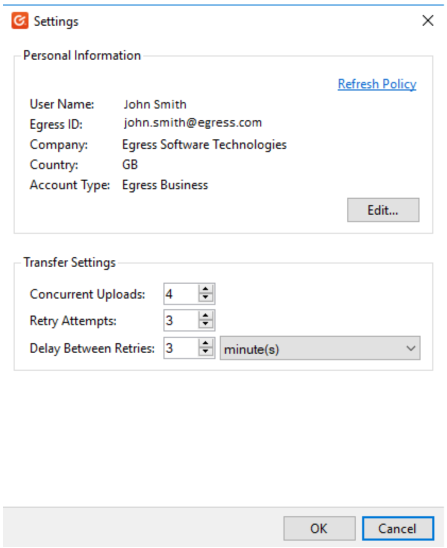


Threat Protection

Never emailed before:
john.smith@gmail.com

Managing Client settings

You can view and edit various Desktop Client settings by selecting the system tray icon and choosing Settings.



Settings

Personal Information

Refresh Policy

User Name: John Smith

Egress ID: john.smith@egress.com

Company: Egress Software Technologies

Country: GB

Account Type: Egress Business

Transfer Settings

Concurrent Uploads: 4

Retry Attempts: 3

Delay Between Retries: 3 minute(s)

The **Settings** window displays information about the current user, and lets you customise transfer settings for package uploads.

- **Refresh policy**: connect to the Egress Server Infrastructure to download the latest user policies.
- **Edit**: modify your personal information via Web Access.
- **Change password**: change the password for your Account.
- **Concurrent uploads**: change how many uploads can take place at the same time.
- **Retry attempts**: configure how many times the Client should retry uploading a package that has failed to upload.
- **Delay between retries**: set the delay between retry attempts for failed uploads.
- **Outlook Large File Mode**: configure Large File Transfer to the mode you wish to use. More information about large file transfer can be found here.

Policy configuration

At the heart of the Egress Infrastructure is a powerful policy and classification engine. This centrally-managed engine allows administrators to enforce decisions over how data should be sent, which security policies are required and how data access is audited. If permitted, users can choose their own level of security when exchanging information but this decision can be overridden by centrally defined policies.

Any number of classifications or policies can be defined to suit your organisation’s workflow. This includes: completely automating the classification process for end-users, allowing users to make decisions as to whether the information being sent is safe enough for public access, and controlling highly sensitive data so it cannot be accessed outside your organisation.

For more information on Egress policies and what is possible please refer to the *Egress Branding & Policy* document.

Egress **support centre**

Should you encounter any problems with Egress please visit the Egress Software Technologies Support Centre www.egress.com/support.

Useful contact information

Telephone numbers:

Egress Europe:	+44-844-8000-172
Egress North America:	1-888-505-8318
Egress Australia:	1-800-768-043
Egress Singapore:	800-130-2208

Website and email addresses:

Egress website address:	www.egress.com
Egress Sales:	sales@egress.com
Account Services:	accountservices@egress.com
Support:	support@egress.com

Follow Egress online

Twitter:	https://twitter.com/EgressSoftware
Facebook:	https://www.facebook.com/EgressSoftware/
LinkedIn:	https://www.linkedin.com/company/egress-software/
Egress blog:	https://www.egress.com/blog/

Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of information security services designed to secure shared data from start to finish using a single platform: Egress.

The Egress platform is made up of highly integrated and flexible service lines. These award-winning services include email and document classification, the only email and file encryption product to be CPA certified by NCSC, secure managed file transfer, secure online collaboration and secure archive.

www.egress.com

✉ info@egress.com

☎ 0844 800 0172

@EgressSoftware