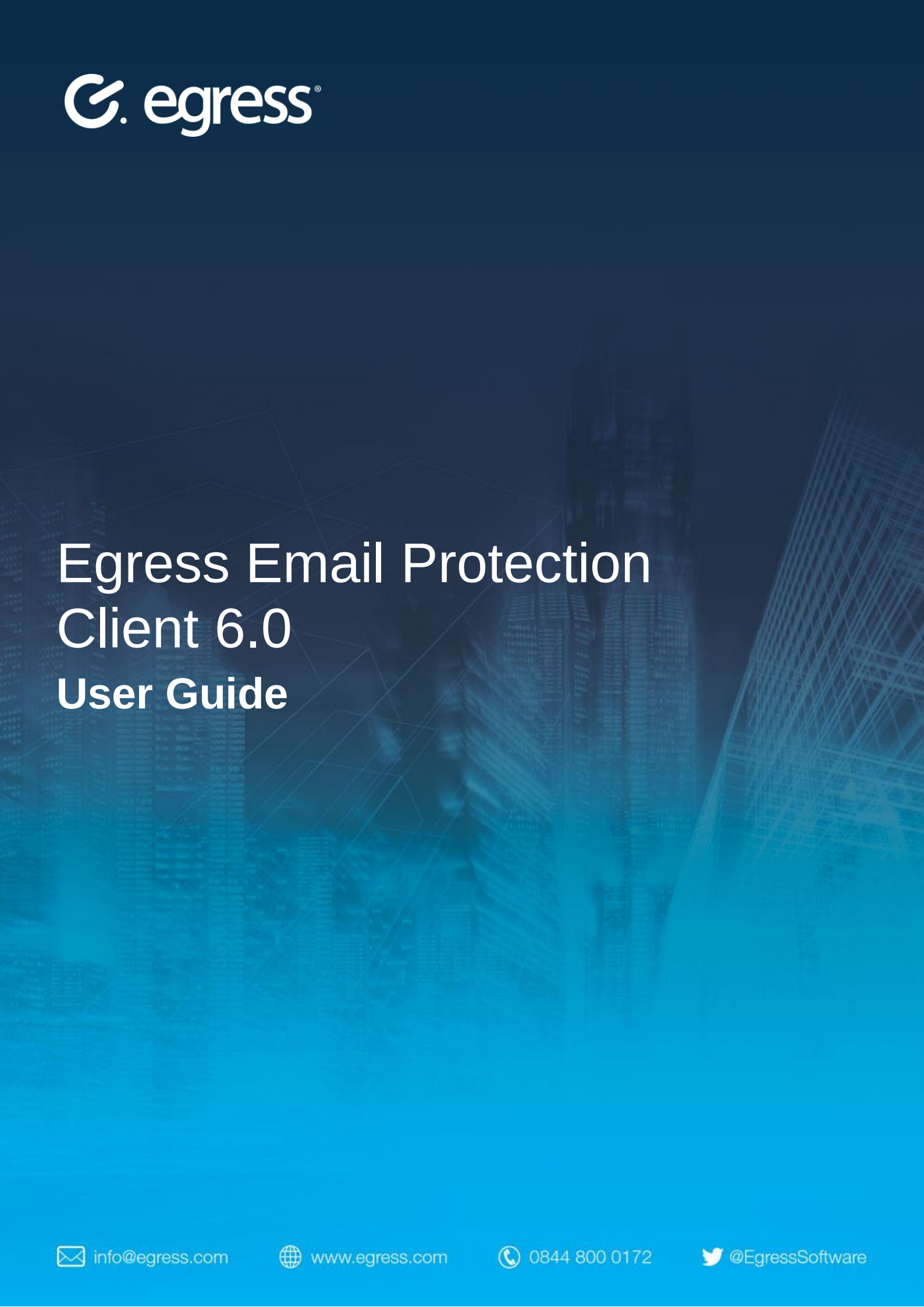


Egress Email Protection Client 6.0

User Guide

info@egress.com www.egress.com 0844 800 0172 @EgressSoftware

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 Email Protection Client 6.0 3
What's new in Email Protection 6.0? 3
Installation 4
System requirements 4
Getting the Email Protection Client 4
Getting started 5
Creating an account 5
Signing in 5
Using the Microsoft Outlook add-in 6
Sending a secure email 6
Egress Large File Transfer 8
Using the LFT sidebar in Outlook to send large files 8
Sending large files without the Outlook sidebar 8
Managing secure messages 9
Viewing and editing message properties 9
Disabling access to a secure message 10
Changing secure message classification 10
Adding time restrictions to a secure message 10
Editing secure message tags 10
Managing access privileges 11
Viewing message delivery reports 11
Viewing audit events 11
Secure Access Viewer 13
Setting up secure access 13
Viewing restricted secure emails and attachments 13
Egress Risk-based Protection 15
How Risk-based Protection works 15

Suggested recipients 15
Accidental send prevention 15
Advanced spear phishing protection 17
Policy configuration 18
Egress support centre 19
Useful contact information 19
Follow Egress online 19

Egress Email Protection Client 6.0

User guide

Egress helps protect unstructured data to meet compliance requirements and drive business productivity. Our AI-powered platform enables users to control and secure the data they share.

As the first, and currently only, NCSC CPA IL3 Foundation Grade-certified email encryption product on the market, **Egress Email 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 Email Protection Client 6.0** for Microsoft Windows, including the Microsoft Outlook Add-in, Large File Transfer, and support for Egress Risk-based Protection.

What's new in Email Protection 6.0?

Email Protection 6.0 is significantly different from previous versions of the Egress desktop software. Major changes are summarised below. For more information, please read the Egress *Email Protection Client 6.0 – FAQ* document.

- **Support for Egress Risk-based Protection** (*Note: this functionality is not enabled by default and is not included as standard within Egress Secure Email deployments.)*
- **Support for WSFED and SAML authentication**
- **New installer**
    - Includes Secure Email, Large File Transfer and Risk-based Protection
    - Previous versions will need to be uninstalled first
    - Your Egress Technical Account Manager will manage this process completely
- **Email Protection now completely based within MS Outlook**
    - No System Tray menu
    - No Package Creator
    - No Sent Packages
    - Does not include Egress Document Classification or Egress Secure Workspace integrations for Microsoft Word, Excel and PowerPoint
- **Support for DLP playback**
- **NET 4.6.2 required**

Note: Email Protection 6.0 does not support Large File Transfer through Outlook when Outlook is running in online or non-cached mode

Installation

System requirements

Your system will need to meet the following requirements before installing the Email Protection 6.0 client:

- Microsoft Windows 7/8/10
- Microsoft Office 2010/13/16/ProPlus
- Microsoft .NET 4.6.2 or later
- Microsoft Visual Studio 2010 Tools for Office Runtime (VSTO)

Email Protection 6.0 can run on 32-bit and 64-bit versions of Windows.

Getting the Email Protection Client

Your Egress Technical Account Manager will be able to provide you with the Email Protection Client 6.0 installation files and complete guidance on setting up the software across your organisation. This includes silent installations using a software deployment application such as Active Directory Group Policy and MS SCCM.

Getting started

Creating an account

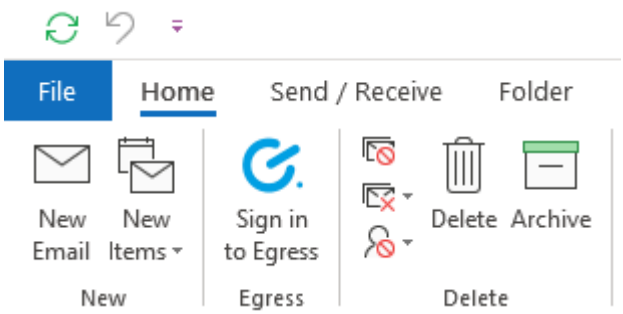
Before you can use Egress, you need to create an account by doing one of the following:

- Visiting http://www.egress.com/register/ and signing up.
- Receiving an invitation from the Egress account administrator within your organisation.

Business users with a paid subscription to Egress can send an unlimited number of secure messages. 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 messages to 25 other non-paying users.

Signing in

After Email Protection 6.0 is installed on your machine, it will appear in the Microsoft Outlook ribbon when you launch Outlook.



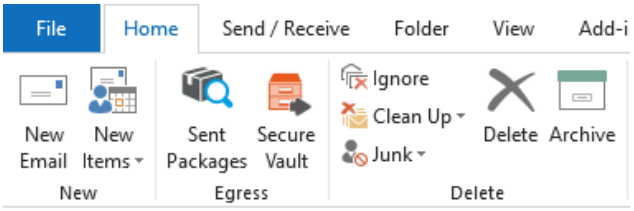
- Select the **Sign in to Egress** button to sign in. Enter your Egress ID credentials into the window that opens.

Alternatively, you may have been signed in automatically if your organisation is using a SAML 2.0 identity provider or another authentication service.

Using the Microsoft Outlook add-in

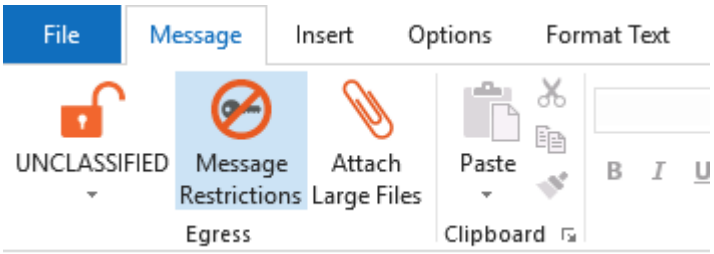
The Email Protection Outlook add-in lets you send secure emails and attachments from within Outlook. When the Outlook Add-in is installed, additional buttons become available in the ribbon:

- When viewing your inbox or sent items, use the **Sent Packages** button to access the Package Library in your web browser, which displays secure messages you have sent previously and enables you to access individual message properties and access lists.

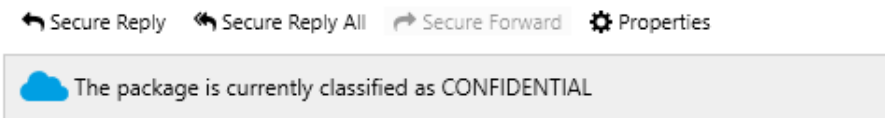


- In addition, if you have any pending access requests you will see an extra button showing how many pending requests you currently have.

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

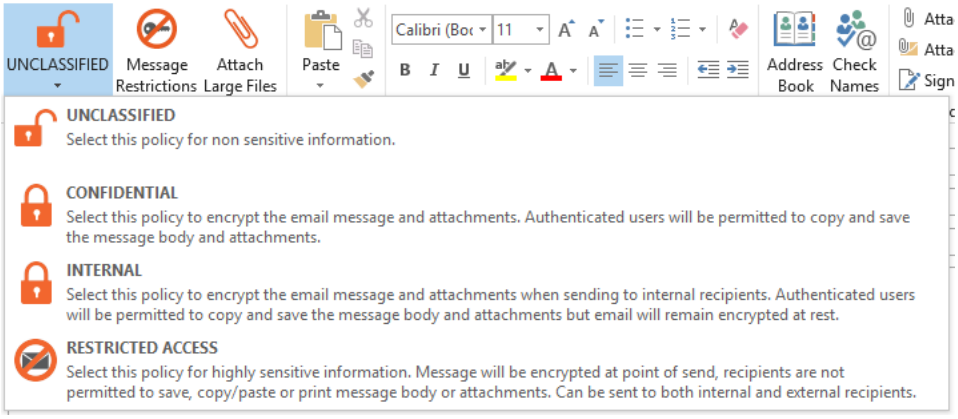


- When viewing a secure message, you have sent in the past, press **Properties** to view and change the properties of the secure message. (*Note: depending on the Egress infrastructure your organisation is using, this option may not be available to you*)

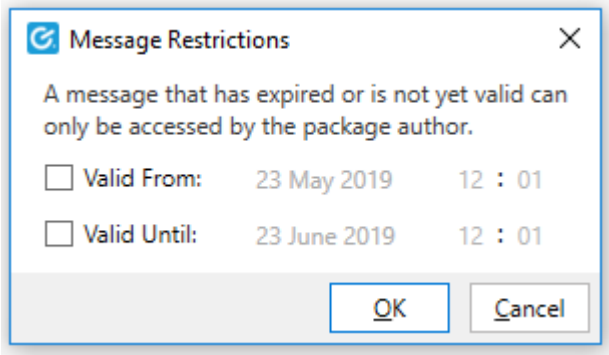


Sending a secure email

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 security type. The options available here are dictated by your business account's policy and so some options may not be available.



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



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

Egress Large File Transfer

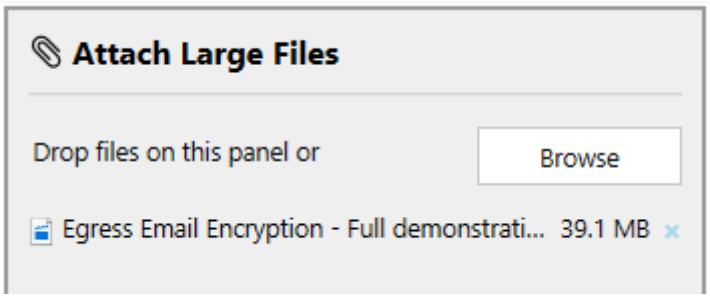
Often, email clients limit the maximum file size of attachments. Egress Large File Transfer (LFT) lets you send large files securely by uploading them to hosted Cloud storage.

Note: Client 6.0 does not support LFT through Outlook when Outlook is running in online or non-cached mode

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.



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.

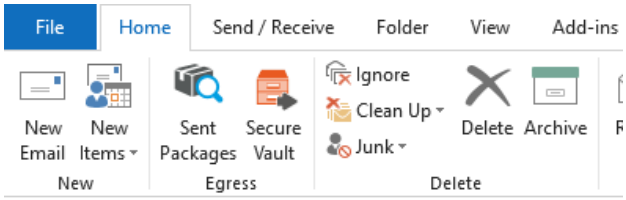
Sending large files without the Outlook sidebar

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 .switch files and sent by large file transfer.

Managing secure messages

Once a secure message is created, the author remains in control even after it has left the network where it was created. The Sent Packages library provides a way to manage and control the lifecycle of all the messages that you have created.

Access the package library by selecting **Sent packages** from the Outlook ribbon.

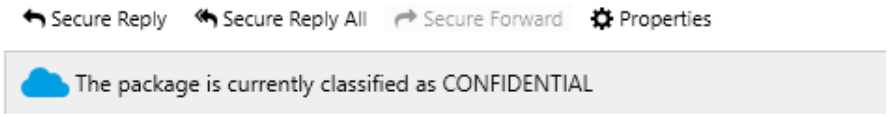


The Sent Packages menu organises secure messages into smart folders. You can easily locate messages based on date, type and classification.

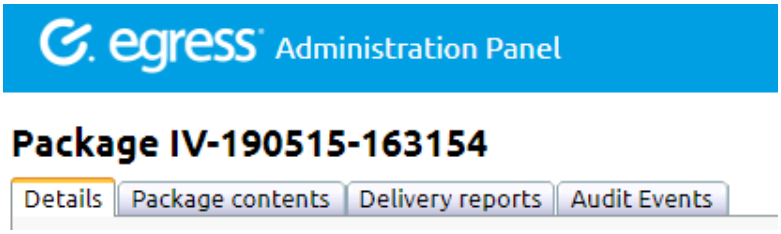
Viewing and editing message properties

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

- To access the properties of a message, click on the **Sent Packages** button and locate the message.
- Depending on the infrastructure setup your organisation is using, you may be able to reach the properties of the message directly from the message in your **Sent Items** folder. Click **Properties** and the information will appear in a sidebar.



The **Details** tab displays information about the message, and lets you perform the following actions:

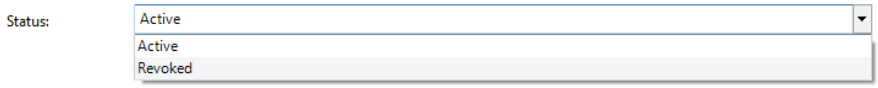


- View the file contents and structure of the message.
- Copy the download URL to send to a recipient.
- Edit the subject of the message.
- Disable access to the message by changing its status.
- Control the classification level of the message.
- Modify or add time restrictions to the message.
- Edit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

Disabling access to a secure message

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

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



Changing secure message classification

You can change the classification of a message after you have sent it. Classification dictates what the recipients can do with the contents of the message:

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

Adding time restrictions to a secure message

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

1. Go to **Sent Packages** and click on the package whose time restrictions you wish to change.
2. In the **Details** 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 **Save Changes** to confirm.

Editing secure message tags

When you send a secure message, you can tag it with keywords in order to make searching through the **Sent Packages** library more straightforward. You can also edit these tags later.

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

Managing access privileges

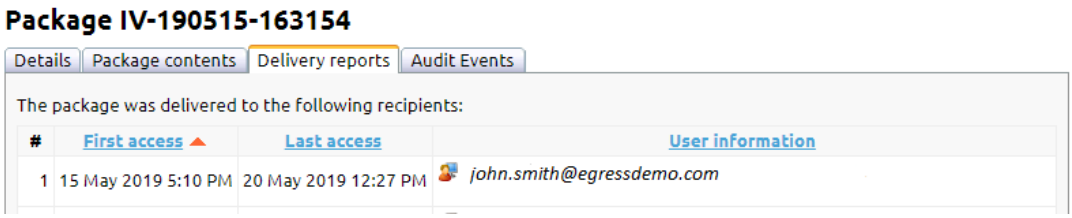
Each secure message has a defined list of recipients able to gain access. You set these before you send a secure message by adding recipients to the To field of the email. You can also manage this access list after sending.

1. Go to **Sent Packages** and click the message whose access you wish to manage.
2. In the **Details** tab, the message box in the **To** section displays who currently has access to the message.
3. To add people to the access list type their email addresses into the box, separating multiple recipients with semicolons.
4. To remove a recipient, delete their email address from the list.
5. Press **Save Changes** to confirm.

Viewing message delivery reports

Delivery reports display when a secure message was accessed and by whom it was accessed. To view a message's delivery report:

1. Go to **Sent Packages** and click on the message whose delivery report log you wish to view.
2. Go to the **Delivery 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 message.

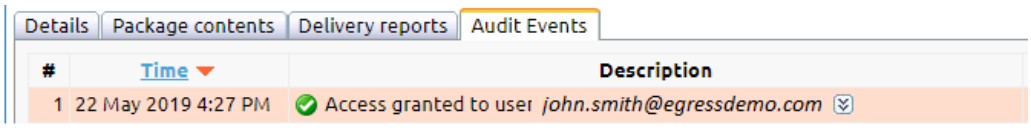


Viewing audit events

You can view detailed information about the lifecycle of a secure message. 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 secure message's audit log:

1. Go to **Sent Packages** and click on the package whose audit events you wish to view.
2. 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.



Secure Access Viewer

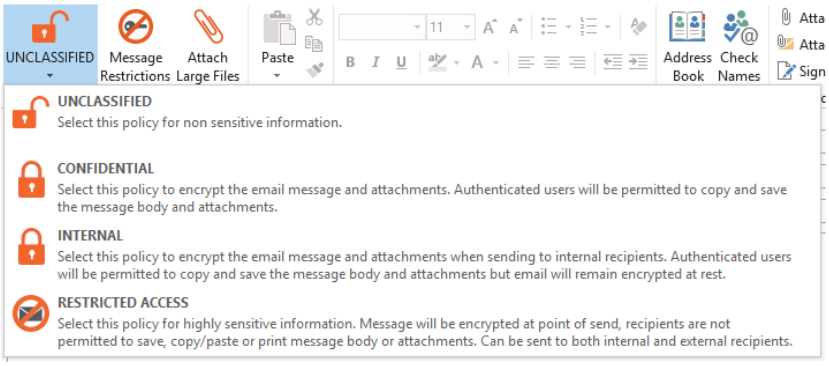
Versions 4.5 and above include a Secure Access Viewer. The Secure Access Viewer restricts the following recipient actions:

- **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.

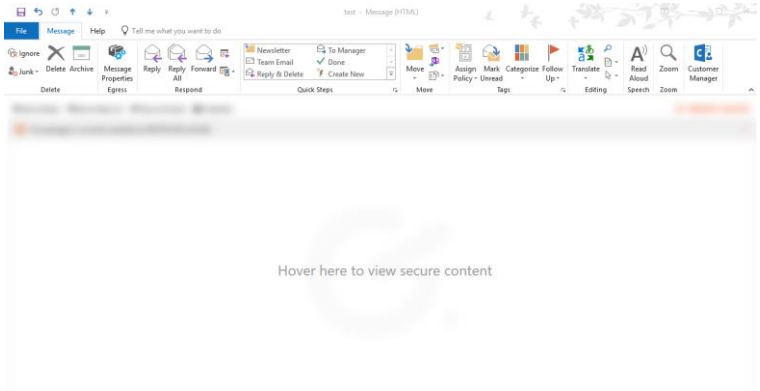
Setting up secure access

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 **Restricted Access** to prevent recipients from saving, copying or printing the message body or attachments. Send the email.



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.



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.

Egress Risk-based Protection

Email Protection Client 6.0 includes support for Egress Risk-based Protection, a solution developed by Egress to prevent misdirected emails and ensure appropriate security is applied in every situation. It integrates into Microsoft Outlook to provide real-time advice and notifications concerning a user's choice of email recipients and security.

Note: Risk-based Protection requires an additional user subscription in order to function.

If you are a license holder of Risk-based Protection, Endpoint 6.0 contains the Outlook add-in to enable protection against the accidental send.

How Risk-based Protection works

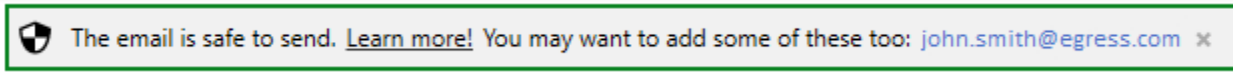
When adding recipients to an email, Risk-based Protection will automatically respond. Based on the user's selected classification and recipients that have been added, a risk score is calculated, and guidance is displayed. Further information is available by clicking "Learn more" and opening the side panel.

When a user clicks send on an email, the Risk-based Protection engine will automatically apply the correct level of security based on the recipients. This could be TLS, message-level encryption, or use of an additional third-party security tool.

Suggested recipients

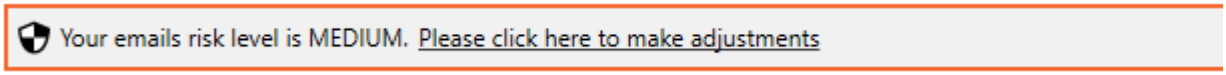
If the added recipients seem correct, Risk-based Protection will also suggest additional recipients based on groups of recipients you have previously emailed.

- 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.



Accidental send prevention

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

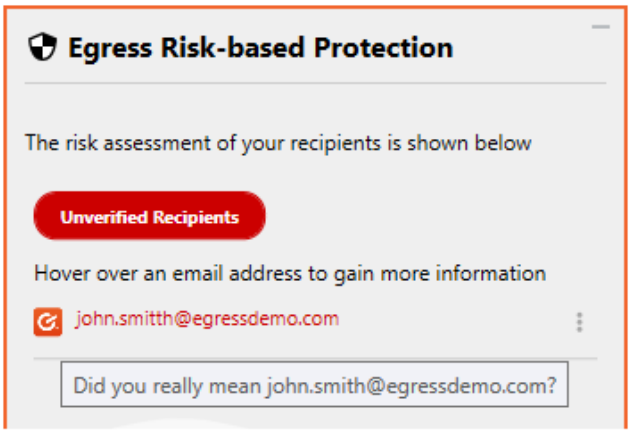


- Click on the warning to see details of the potential problems with the recipients and adjust as needed.

If no changes are made, the user may be required to add an additional level of protection to the email, such as encryption.

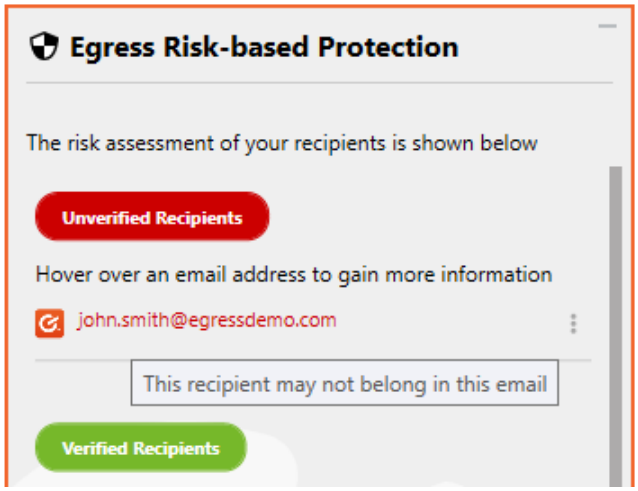
Examples of potential recipient mistakes include:

1. **Mistyped recipients**



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

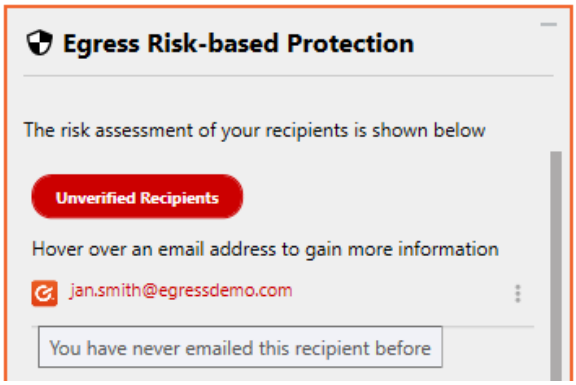
2. **Incorrect recipients**



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

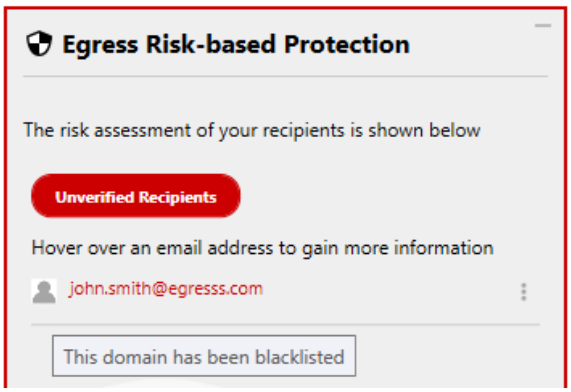
3. **New recipients**

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.



Advanced spear phishing protection

Spear phishing attacks use email addresses that look like familiar addresses but differ slightly. It is not always easy to spot this when replying to the email. When a user replies to a phished email, Risk-based Protection analyses the recipients and flags the recipient as high risk.



The user can then desist from replying. Should the user ignore all warnings and guidance, they can be blocked from sending the reply at all.

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