Egress Secure Workspace

Administration 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 Secure Workspace
Administration Guide

Egress Secure Workspace is a secure, cloud-based collaboration platform designed to help users share files and collaborate effectively. It ensures that data is kept secure both at rest and in transit, integrates seamlessly with existing document management systems, and does all of this whilst maintaining Egress' award-winning ease of use.

Secure Workspace makes managing complex projects easier and more efficient, bringing together file sharing, inline document editing and messaging functionality and enabling multiple stakeholders to organise workflow and stay on track. Fine-grained control of user permissions and extensive auditing features mean that administrators retain full control of their files and folders, even while sharing with and external partners.

This guide explains how to use the administration features in Egress Secure Workspace, helping business administrators set up and manage their users and zones.

As an administrator you can:

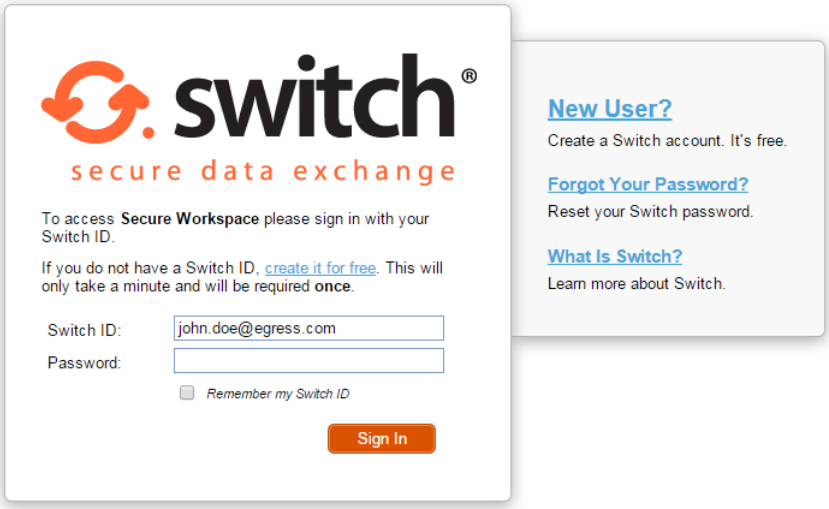
- Manage users, groups and roles
    - Invite users
    - Add users to groups
    - Change user roles
    - Disable user access to zones
- Manage zones
    - Create and delete zones
    - Share zones
    - Create and edit zone templates
- View system audit events
    - View logs of user actions
- View statistics
    - Bandwidth statistics
    - File statistics
    - User statistics
- Create and edit web page documents
- Manage Server Settings

To understand the general-usage features of Secure Workspace, please refer to *Egress Secure Workspace User Guide.*

Getting started

Signing in to Secure Workspace

- Navigate to your Secure Workspace web address. This should have been issued to you by your Egress Support representative.
- At the Egress sign-in page, sign in with your Egress ID. Alternatively, Egress supports single-sign-on and so if you have Active Directory Federation Services (ADFS) enabled, you can sign in using your usual system username and password. For information about using other Identity Providers please contact your Egress technical account manager.



Using Secure Workspace for the first time

When you first arrive at Secure Workspace you can start creating and managing zones for yourself and other users.

The steps you need to take when using Secure Workspace for the first time are:

1. Invite users through the ESI or workspace
2. Choose a zone template and create a new zone
3. Add files to the zone
4. Share the zone with a user OR
   Create a user group to share the zone with multiple users

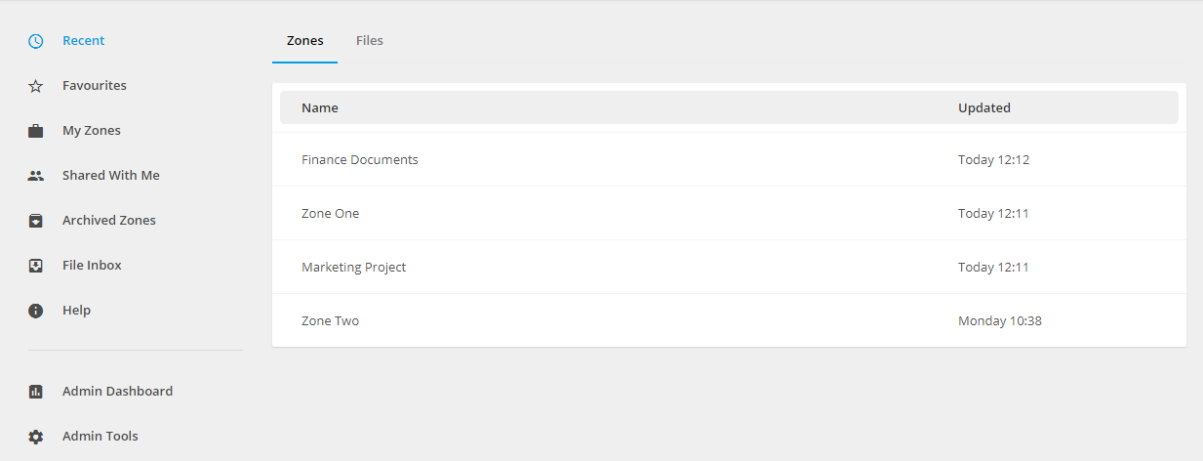
Once your zone is created you may want to:

1. Edit files
2. Manage user roles
3. Revoke user access
4. View zone statistics
5. View audit logs

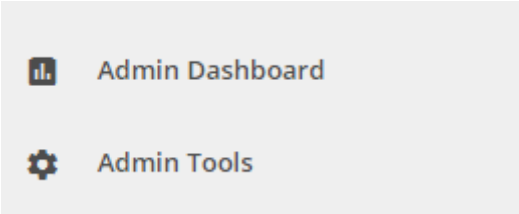
Using the dashboard

After signing in with your Egress ID you are presented with the Secure Workspace recent page. On the navigation sidebar you will find all the tools you need to create and share Zones and perform administrative functions, also included is a help section and file inbox.

Note: the file inbox feature is not a default feature. Your business administrator can opt to make it available to users.



If you are listed as an administrator, you will have access to the Admin Dashboard and the Admin Tools.



Administration Tools

- Select the **Admin Tools** link on the sidebar to access various tools for managing users and zones. There are six different sections in Administration Tools:
    - **User and Group Management**
    - **Roles**
    - **Zones**
    - **Audit Events**
    - **Miscellaneous (Web Page Management)**
    - **Server Settings**

Adding new users

There are two ways to add new users to Secure Workspace, depending on whether the users are internal or external to your business account.

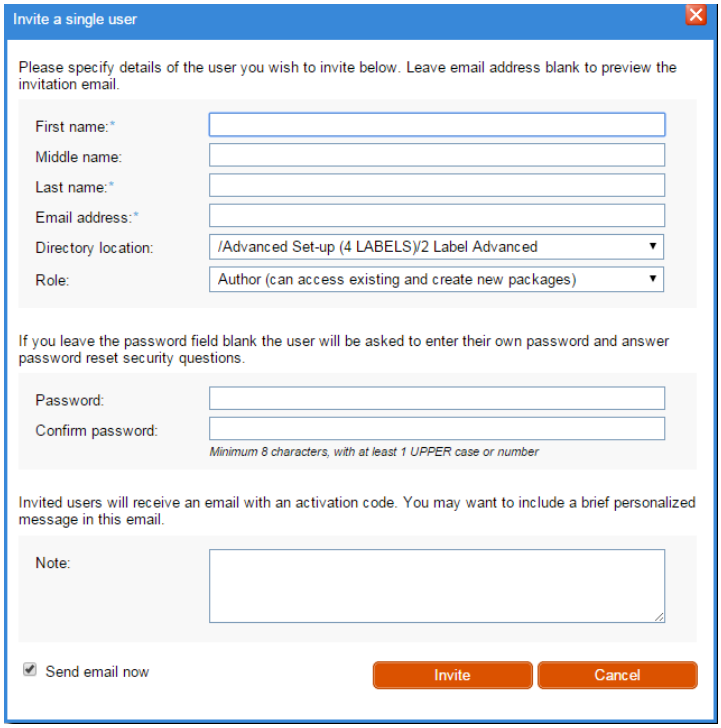
The Secure Workspace auto-enrolment policy means that external users you share zones with are automatically granted access and so do not require you to create an account for them. If you want to add multiple third-party users in bulk without first sharing zones with them, you can do so in Secure Workspace by uploading a CSV file.

Internal users are automatically enrolled in Secure Workspace via the Egress Server Infrastructure (ESI) or Active Directory if using ADFS. They can be added and managed through your organisation's ESI by visiting switch.egress.com (or local address) and signing in to the administration panel.

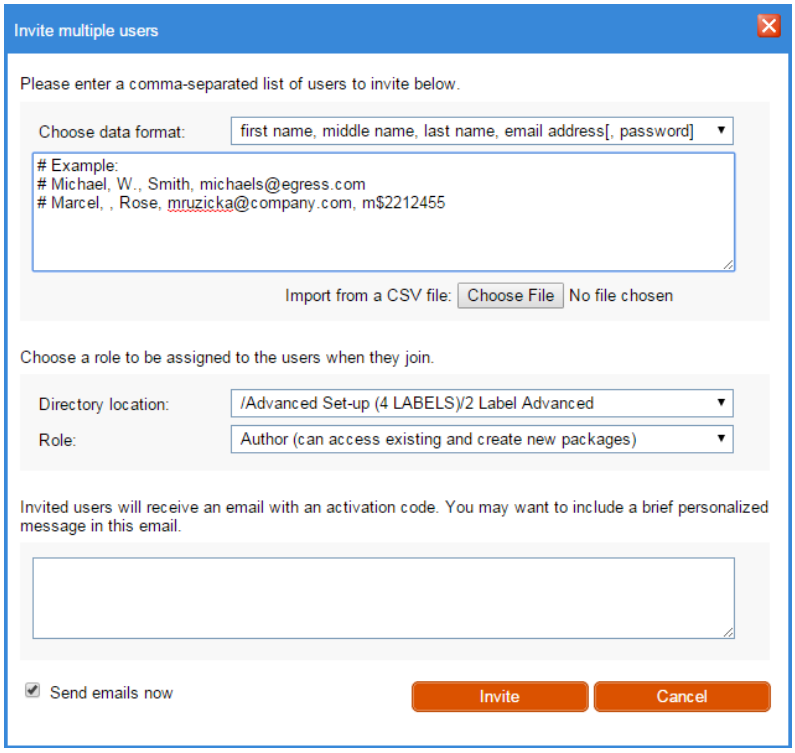
Adding internal users

1. Go to switch.egress.com (or local address) and sign in with your Egress ID. This opens the Egress Administration Panel.
2. Select **Invite Users.** You can invite a single user or multiple users.

3. If you select **Invite Single User**, simple fill out the form with their details and assign them a system role. You have the option to pre-assign them a password too. Press **Invite** to send the invitation to join your Egress Business Account.



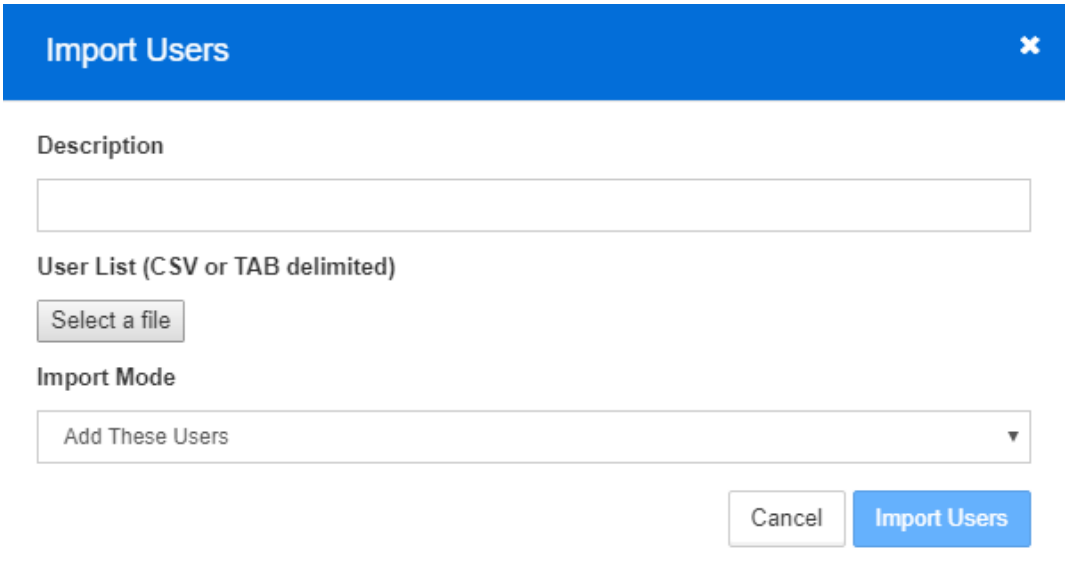
4. If you select **Invite Multiple Users**, you can either type in the user details into the text box in the window, or import the user details from a CSV file. You can choose the format the user data comes in but make sure when importing a CSV file that the data is arranged according to your chosen format.



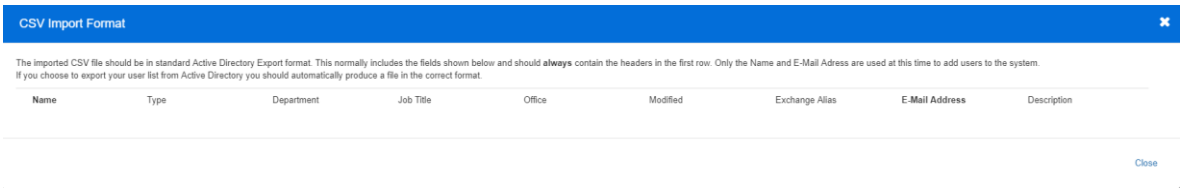
5. After typing in or importing the user details, choose a directory location and role for the imported users.
6. Optionally include a personalised message for the email these invited users will receive. Press **Invite**.

Adding external users (bulk import)

1. On the Administration Tools Users/Groups tab, go to **Bulk User Import (From CSV).**
2. Select icon in the top right of the page.
3. In the **Import Users** window, choose the CSV file to import, and give the import a description. You can also choose here whether to add the users or archive them. Archiving the users means that they will not be able to sign in.



4. Make sure that the file you choose is in the correct format. To see what this looks like, press the **CSV Import Format** button. If you choose to export your user list from Active Directory it should automatically produce a file in the correct format. Secure Workspace only uses the **Name** and **Email Address** fields to add users to the system.



5. Press **Import Users** to import your user list.

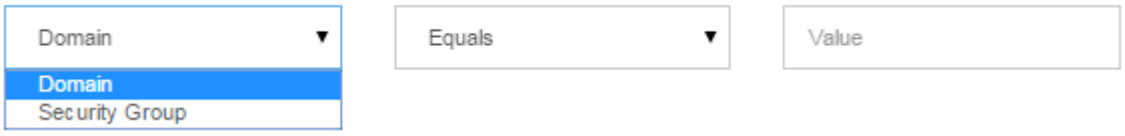
Clicking on **Bulk User Import Tool (From CSV)** also displays a list of previously imported CSV's. It shows the upload name, the date created, and whether the upload was a success or failure.

Creating auto-enrolment policies

Note: to use this feature you require SSO configuration for the service via ADFS or SAML.

You may wish to auto-enrol users from specific groups or Organisational Units in your Active Directory into a similar group in Secure Workspace. As an administrator you can set this up by creating an auto-enrolment policy. Having an auto-enrolment policy in place means that when you add someone to a group in your Active Directory, they are automatically added to the corresponding workspace group without any additional manual steps.

1. Go to **Administration Tools** and select **Manage Enrolment Policies** from the **Users/Groups** tab**.**
2. Click ✚ to create a new policy.
3. Give the policy a name and a description.
4. Set the policy condition using the drop-down menus underneath **Policy Condition.** For example, choose **Domain** or **Security Group** and then set it as **Equals to** and then write in the name of the AD group you wish to set the policy for, e.g. **Security Group > equals > Finance.** Using **Domain** lets you use the domain name of the user's Egress ID (email



address) to create groups.
5. Use the **Assign to Group** drop-down menu to choose which workspace group to enrol these AD users into.
6. Press **Save and Close**.

In Secure Workspace you can create new user groups with customised user permissions. Please see Creating a user group for details. Once you have created a workspace user group to correspond with a group in your Active Directory, you can use the auto-enrolment policy feature to link them together.

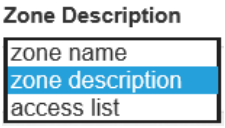
Creating Zones

Creating zones in bulk

You can create multiple zones simultaneously by importing a CSV file. This is useful if you want to give multiple users their own specific zone. The file should contain column headers for zone names, descriptions and access lists. The user details in the access list should be email addresses separated by commas.

	A	B	C
1	Zone Name	Zone Description	Access List

1. Select **Bulk Zone Creation (from CSV)** from the Zones tab on the Administration Tools page.
2. Click ✚ to import a new CSV.
3. Choose the file to import and give the bulk creation task a description. Press **Create.**
4. In the **Create** window, map the zone fields to the headers in your CSV file. E.g. match the required zone fields, **Name, Description, Access List,** to the column headers in your CSV file. Do this by choosing each header from the drop-down menus.



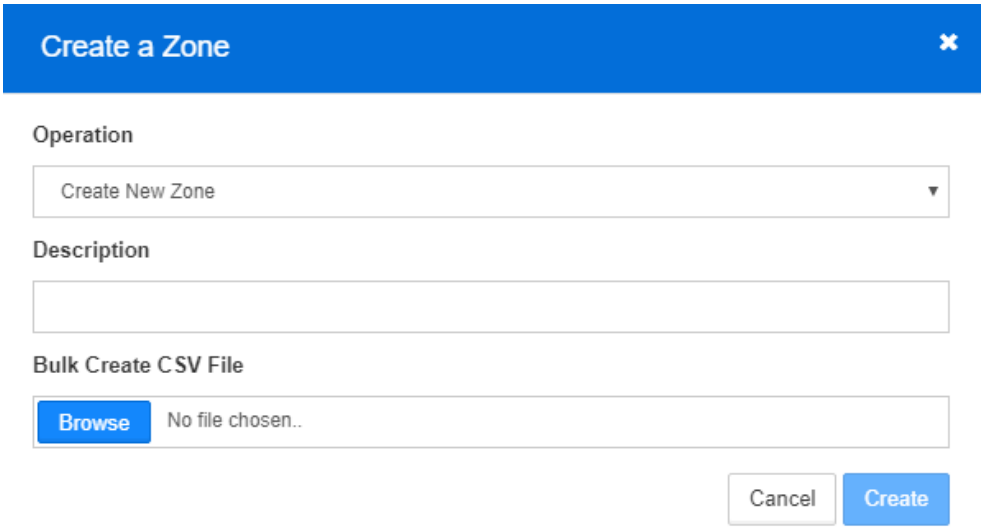
5. Choose the zone role to give the members in your zone access lists. zone roles are fully customisable, see the Changing role features section for details.
6. Choose who owns the new zone. This can be you, or the first name in the access list.
7. Select **Create** to create the zones from your CSV file.

For example, if you want to create a separate zone for each customer:

1. Create a CSV file containing columns for the zone name, description and the customer's name, e.g.:

	A	B	C
1	Zone Name	Zone Description	Access List
2	John Doe's Zone	A place to store John's files	john.doe@egress.com
3	Jane Doe's Zone	A place to store Jane's files	jane.doe@egress.com

2. Go to **Bulk Zone Creation (from CSV)** in the Administration Tools page and choose this file to import.



3. Map the zone fields to the headers.
4. Choose whether your customers have owner privileges or only limited access permissions.
5. Select **Create.** Each zone will be available for its intended user from their dashboard by going to **Zones – My Zones**.

In the **Bulk Zone Creation (from CSV)** window you can also view a list of previous bulk zone operations and the date each bulk zone creation took place.

Viewing and managing zones

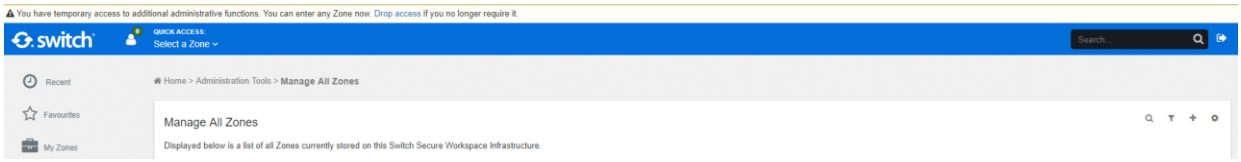
You can view a list of all the zones under your administrative control.

- Go to the Administration Tools page and select **Manage All Zones.**

This is useful if you want to view zone information such as the number of files a zone contains, the owner's name, the size or the date it was last modified. You are also able to view and modify who has access to a particular zone through the zone shares by selecting icon in the settings column.

Super admin mode

A higher level of administrator access can be enabled by clicking in the top right of **Manage All Zones.** Super admin mode enables **read only** access to **all zones** and folders/files in Workspace, any actions within a zone whilst in super admin mode will not be recorded in the Zone Audit but will be visible to administrators in System Audit. A bar will appear across the top of the page to let you know that you are using super admin mode, with the option to drop access.



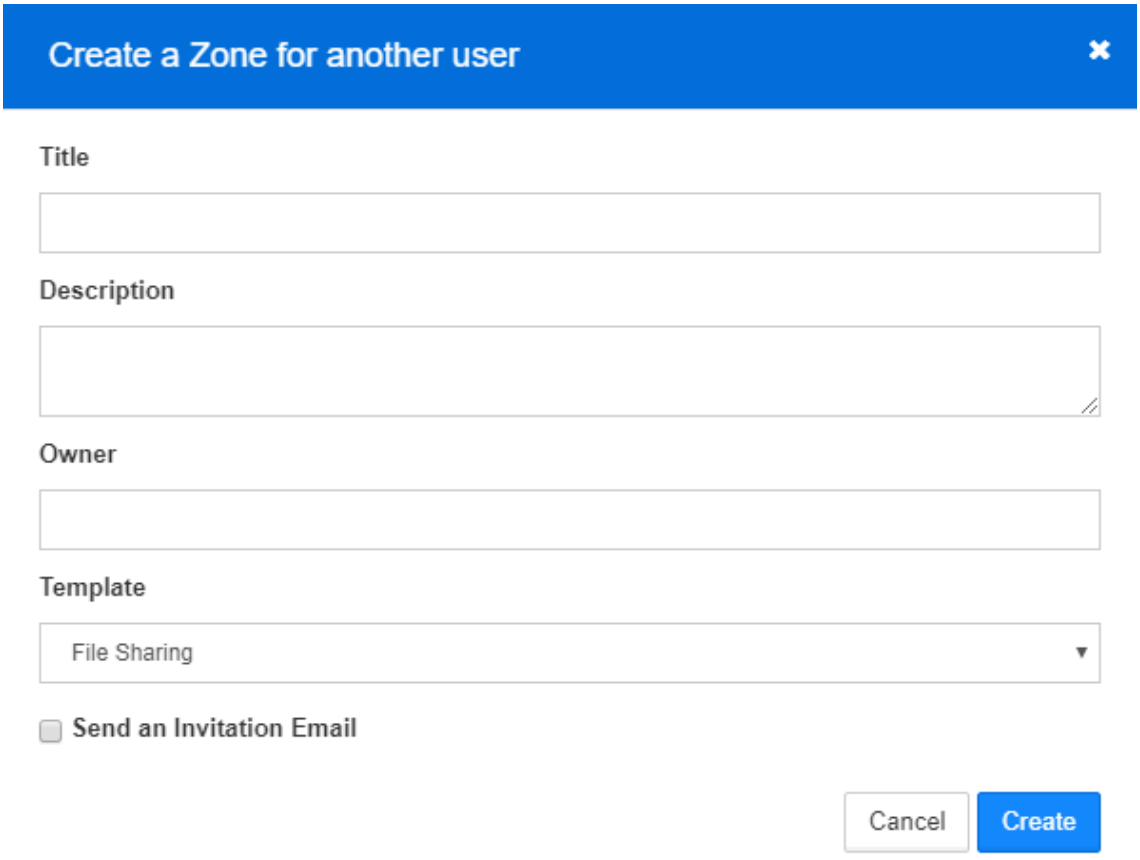
Note: *the super admin feature is not a default feature. Your business account administrator can opt to make it available to users by requesting it from an Egress engineer.*

Creating a zone for another user

As a system administrator, you can create zones for other users and assign them as the zone administrator. You can assign someone as a zone administrator even if they do not exist on the system, simply enter their email address and they will be invited to create and activate their Egress ID. Additionally, if you make the owner a **Power User**, they will be able to create their own zones.

To create a zone for another user:

1. Go to the Zones tab and select **Manage All Zones,** click + in top right.
2. Fill in the boxes in the **Zone Create** page to give the new zone a name, description, owner and template. The owner you specify will be given the zone administrator role.
3. Choose whether to send an invitation email.
4. Click **Create**.



Editing zone templates

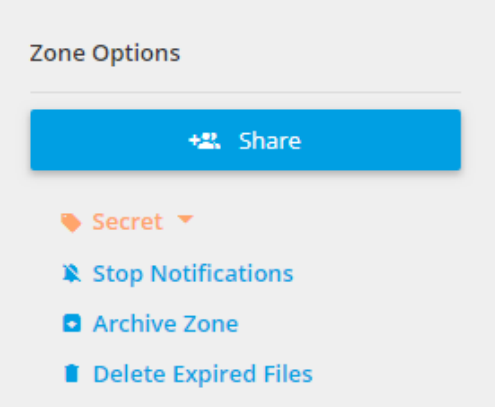
When you create a zone, you start by choosing a zone template. As an administrator you can view and edit the zone templates available to your organisation. You may want to do this to allow or disallow certain file types being used, for example.

1. Select **View/Edit zone Templates** on the Administration Tools page.
2. Click on the **View/Edit** button next to a template to change the name, icon, description and list of allowed file types. Click **Save** to complete the template edit.

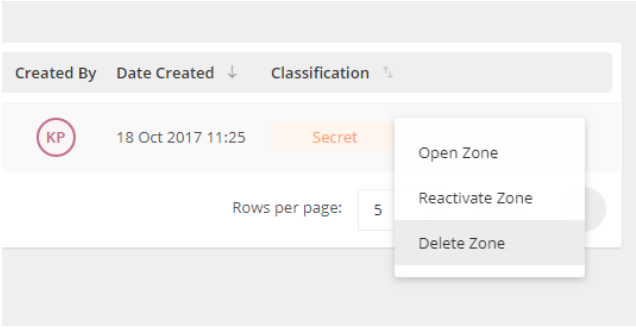
Deleting a zone

To reduce the risk of zones being deleted by accident, the process of deleting a zones contains two distinct steps.

1. Navigate to the zone you wish to delete and from Zone Options choose **Archive Zone**. You can also archive a zone from the **My Zones** menu by selecting the **Action (•••)** drop-down menu.



2. Go to **Archived Zones** from the left-hand menu**, l**ocate the zone to delete, and select **Action (•••)**, **Delete Zone**.



Managing users and groups

You can manage users through the ESI and through Secure Workspace itself. Use Secure Workspace to manage external users, create user groups all users, and disable access for any user.

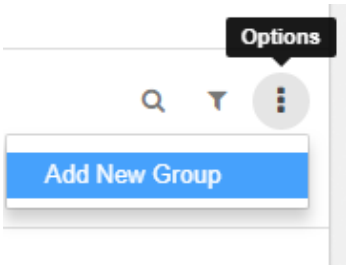
Use the ESI when managing internal users of your business account. The user details in the ESI are taken from your Active Directory (If SSO is used). Any changes you make to internal users in Secure Workspace will not affect their entry in the directory, so will only have an effect until they next sign in to their zones.

External users, such as customers and clients of the organisation, are managed entirely through Secure Workspace itself as they do not have entries in the ESI.

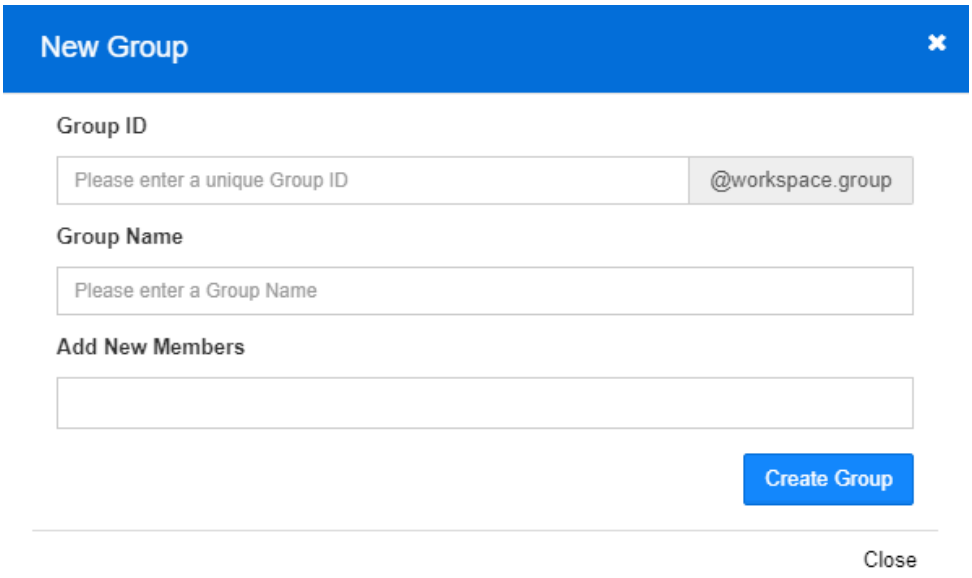
Creating a user group

On Secure Workspace you can arrange users into groups, making it very simple to add multiple users to a zone at the same time.

1. On the **Administration Tools** page, select **Manage Enrolled User and Group permissions**
2. Select the **Groups** tab and from the options menu choose the **Add New Group** option to open the **New Group** dialog box.



3. Choose a group ID and group name.
4. Press the drop down menu under **Add New Members** to choose from a list of current users.
5. Press **Create Group.**



Adding and removing users from groups

As an administrator you can view and change a user's group membership details.

1. Select **Manage Enrolled User and Group permissions** on the Administration Tools page and select the **Groups** tab.
2. Find the group you want to change, do this by using the direction arrow icons to scroll through the user list, or searching for them using the search bar.

3. Select the Group's name or the **View Account** button to open their **Group Properties** window.
4. To add the user to a group, click inside the User Membership text box. A drop-down menu appears, listing the current existing users.
5. Choose the user(s) you wish to add the group to and then press **Save.**

- To remove the user from a group, simply press the **X** symbol by the user name, then press **Save.**

Changing a user's role

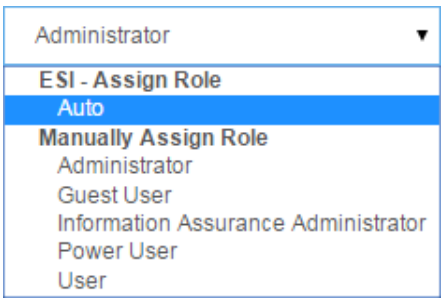
In Secure Workspace, users receive **roles,** which define the actions that they are allowed to perform. There are **System Roles** and **Zone Roles**. System roles define the core system permissions the user has, such as whether they have access to administration and auditing tools. Zone roles define the capabilities a user has on a per-zone basis.

For example, a user may be a **Guest User** in the overall system, but an **Administrator** role in a particular zone. They would not be able to create zones or perform other administrative or auditing functions, but would have full control over the functionality of the specific zone they administrate.

Roles are fully customisable and as a business account administrator you have full control over the roles that users receive. They can also be assigned automatically to invited users. The specific permissions for each role can also be customised, and new roles can be created.

To change a user's system role:

1. Go to the Administration Tools page and select **Manage Enrolled User and Group permissions.**
2. Navigate to the user whose role you which to change.
3. Use the drop-down menu next to the user's name and under the **Role** heading to choose the new role. The change in role will take place the next time the user signs in. To see a description of each role, go to the **Egress Knowledge Base** here.



To change a user's zone role:

1. Go to the zone
2. On the right side of the zone is a shared user list, organised by zone role. Select the user whose role you wish to change.
3. Choose the new role you wish to assign the user, or revoke their access. Press **Save** to confirm.

Create a new role

It is easy to create a new role and the method is the same for both system and zone roles.

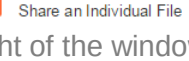
1. Select the Roles tab and **Manage System Roles** or **Manage Zone Roles** on the Administration Tools page.
2. Select + button in the top right.
3. Name the new role and press **Create Role.**
4. The new role will appear in the list of roles. Select it and choose the capabilities you wish to give to users assigned to this role.

Changing role features

You may want to change the specific permissions that a certain role provides. The ability to perform a certain action is known as a capability. To modify a specific role's capabilities:

1. Go to **Manage System Roles** or **Manage Zone Roles** on the Administration Tools page. Here you can see each role, the number of users assigned to each role and the number of capabilities a role contains.
2. Select a role to open the **Edit System Role** window.
3. Change the permission capabilities for the role by checking and unchecking individual capabilities.
4. Press **Save Changes** in the top-right of the screen to finalise the role feature change.

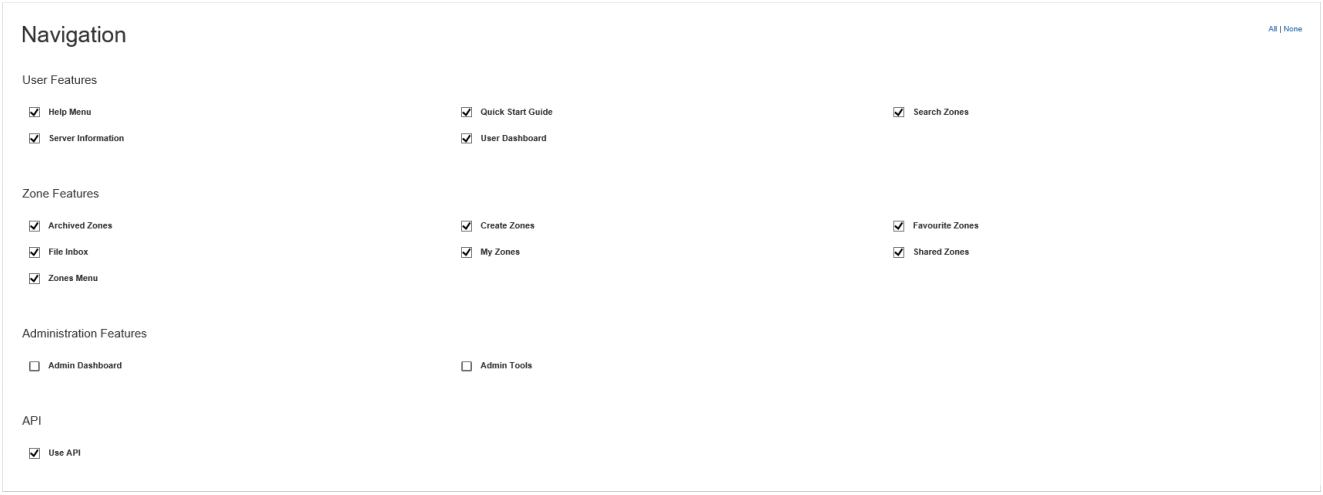
As an example, to give **Guest Users** the permission to share an individual file in a zone:

1. Navigate to the **Administration Tools - Roles** tab, then to **Manage Zone Roles.**
2. Select **Guest User.**
3. Scroll down the capabilities list to the **Sharing** section.
4. Check the box next to **Share an** 

Individual File.
5. Press the **Save Changes** button at the top-right of the window.

- Back at the **Roles** screen, you can also disable or delete roles using the ⊗ or 🗑 icons respectively.

Note: capability changes take effect when the user next signs in. It is also possible to roll back any changes to role permissions by using the 'Restore Previous Versions' menu.



- Please see the Role appendix for a breakdown of the default system and zone role capabilities.

Disabling user access

You may want to prevent a user from accessing any zones at all, for example if an external customer no longer requires access.

1. Go to the Administration Tools page, and select **Manage Enrolled User and Group permissions.**
2. Use the arrows to locate the user account you wish to disable, or search for the user with the search bar.
3. Upon finding the user, press the icon to disable their account.
4. Conversely, if a user's account has already been disabled, press the icon to enable their account.

Viewing security audit logs

Administrators can view security audit logs for all of the users and zones under their administrative control. This provides in-depth access to information about user actions in Secure Workspace. For example, you can find out who has been viewing a certain document or what time users have been signing in.

- To see an audit log for all the zones you administrate, go to the Administration Tools page and select the Audit Events tab, **System Security Events.** This lists:
    - Every action
    - The date and time each action occurred
    - The zone where it occurred
    - The zone's owner
    - The IP address of the action's source

You can search the log using the search bar, or download it as a CSV file. It can also be accessed through the main Secure Workspace dashboard by selecting **Admin Homepage** and then **Recent User Events.** From there, select the link to **View System Security Events**.

Viewing a user's audit log

Rather than viewing every user's audit log together, you may want to investigate a specific user's actions.

1. Go to **Administration Tools** and select **Manage Enrolled User and Group permissions.**
2. Navigate to the user you wish to audit by using the arrow key icons or the search box.
3. Select on the user's name to open the **User Properties** dialog box. This displays the user's Egress ID, display name and group membership details.
4. Select the **Recent Activity** tab.
5. Press the **View full audit** button to see a complete audit. As before, you can search through it and download it as a CSV file.

Viewing the user summary

In addition, see a quick user summary by going to the **Admin Homepage** and selecting the **User Summary** tab in the **User Statistics** section. This shows:

- Account status (number of active and inactive accounts).
- User profiles (number of organisation users and number of external guest users).
- A list of the most active users. Investigate these users' events logs by clicking on the magnifying glass icon on their entry 

.
- A list of the external domains associated with your zones, with a user count for each domain.
- You can search the events log using the search toolbar and also download it as a CSV file.

Changing server settings

The **Administration Tools** menu contains a section called **Server Settings**, where Administrators can modify ESI, multi-factor authentication settings and document editor settings.

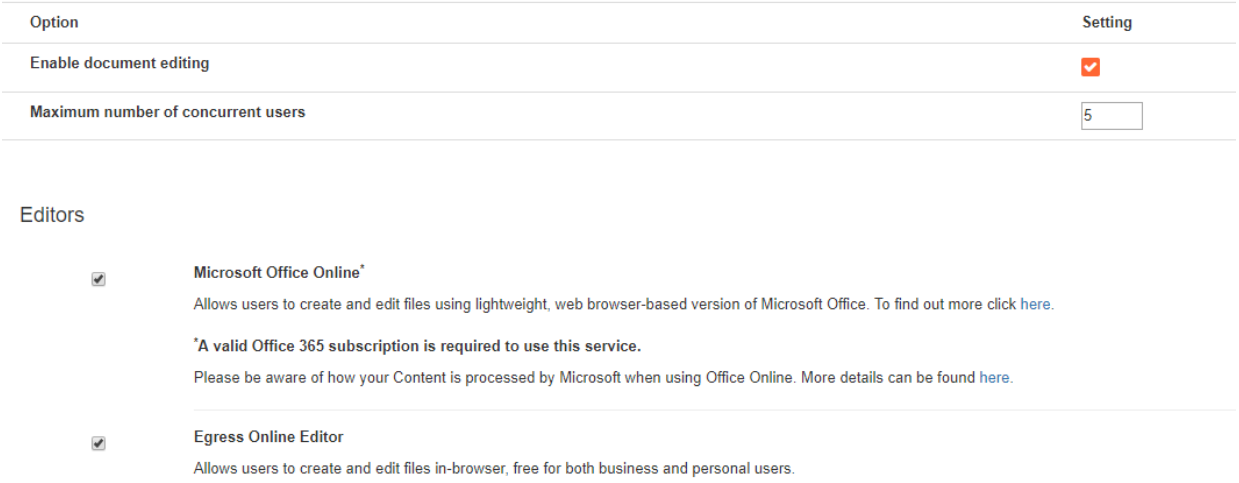
ESI authentication settings

Secure Workspace contains functionality to view and edit your Egress Server Infrastructure (ESI) authentication settings. For help managing your account's ESI, please contact your dedicated Egress technical account manager.

Document editor settings

While the permissions regarding which users are able to access the document editor can be modified easily, administrators can also turn off document editing functionality for all users and choose which editors are available for users.

1. In Secure Workspace, go to **Administration Tools**.
2. Under **Server Settings**, select **Document Editor Settings**. The following options are displayed:



3. To prevent any users from opening the document editor, untick the box next to **Allow Document Editing.**
4. Press **Save Changes**.

- The second option in the **Document Editor Settings** window is **Maximum Number of Concurrent Editors Per User**. This field specifies the number of document editors that a user can have open at any time. Type a new value into the field and then press **Save Changes** to update (default is 5).

Changing default editors

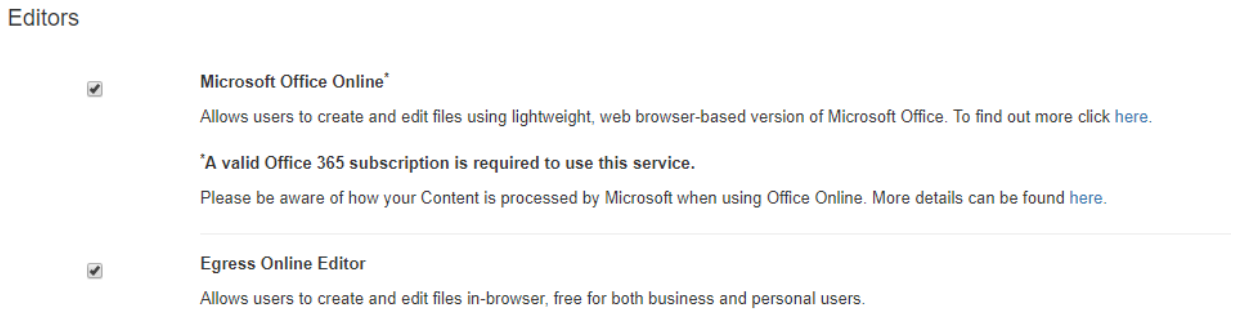
Administrators can specify which editors are available to users. There are two editors available for use:

Egress Online Editor – The feature-rich document editor included with all Secure Workspace subscriptions

Microsoft Office Online –browser-based versions of the Microsoft Office apps: Word, Excel and PowerPoint. A valid Office 365 for Business subscription is required to use Office Online

Administrators can set whether users have the option to choose their preferred editor, or they can pre-define which editor users will have access to.

1. Use the check boxes to choose which editors users can access.



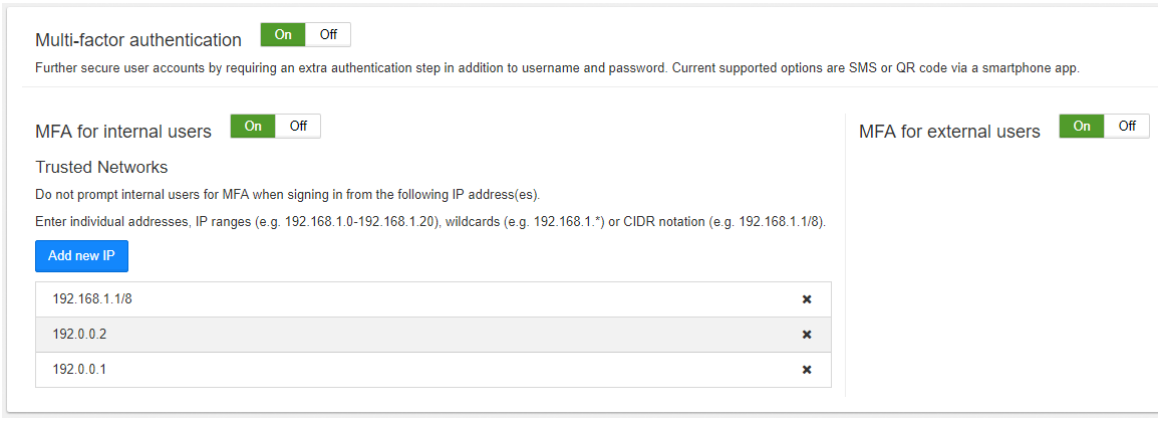
2. Press Save Changes.

Leaving both editors checked means that when a user opens a document for editing they will have a choice of editor and be able to set their own default editor. Giving users only one editor option means they will be taken straight to that editing environment when they open a document for editing.

Note: Using Office Online Editor involves data being sent to Microsoft Office Online server environments, so data residency requirements cannot be guaranteed.

MFA settings

Secure Workspace supports multi-factor authentication (currently limited to two-factor authentication only) using either SMS or QR code as the additional authentication step. Administrators can configure MFA through Administration Tools > Server Settings > MFA Settings.



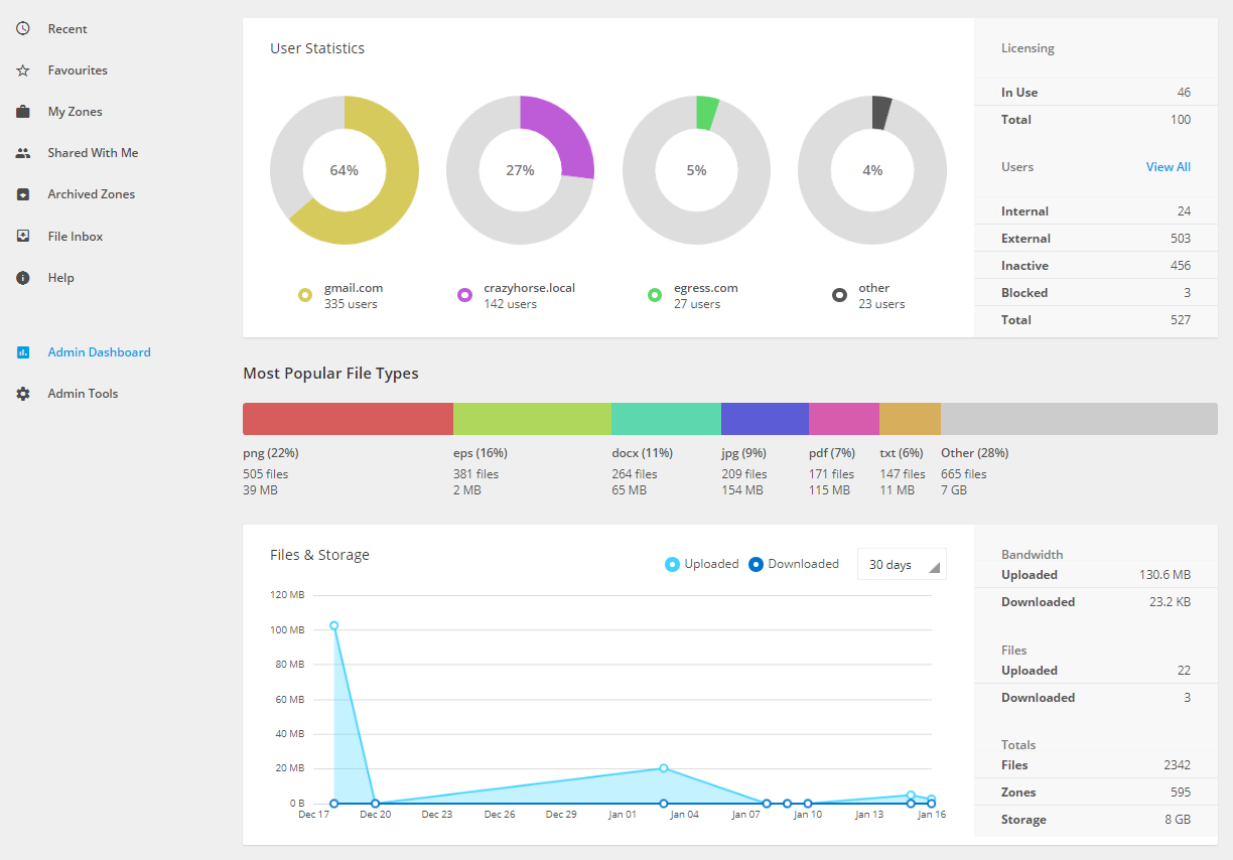
MFA can be configured for the following scenarios:

1. All users
2. External users only
3. Internal users only
4. External users and internal users from non-approved networks
5. Internal users from non-approved networks only

Viewing statistics

You may want to get an overview of the activity across all your zones. This can be useful if you want to investigate the source of significant bandwidth usage or make sure you have sufficient storage space available.

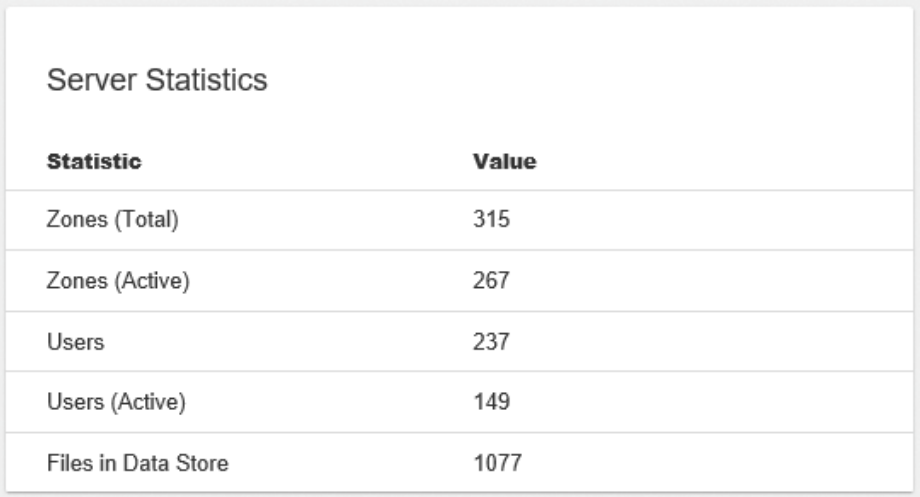
Select the **Admin Dashboard** option on the left-hand menu to see a breakdown of storage statistics and user information.



Server statistics

Found on the **Admin Tools** page, this window gives you a quick way of viewing statistics:

- Zones (Total)
- Zones (Active)
- Users
- Users (Active)
- Files in Data Store

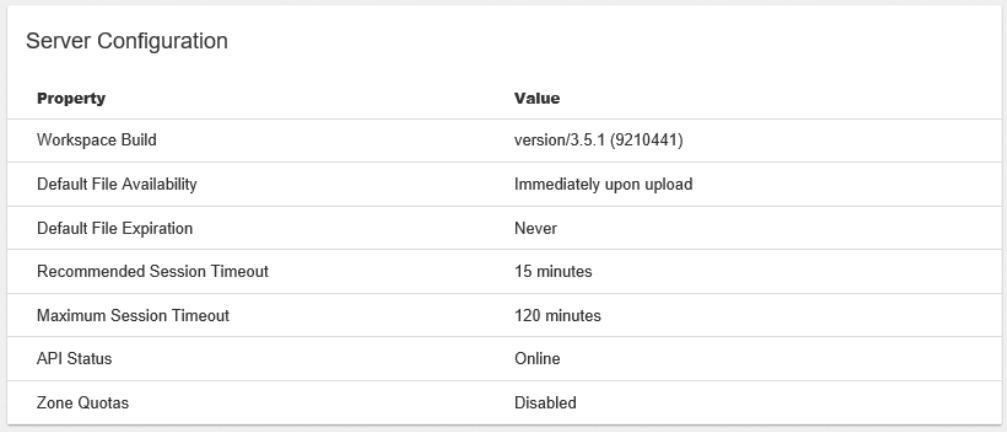


Server Statistics

Statistic	Value
Zones (Total)	315
Zones (Active)	267
Users	237
Users (Active)	149
Files in Data Store	1077

Server configuration

Also on the **Administration Tools** page is a window displaying details of the server configuration. This includes the user expiry dates for internal and external users after a period of inactivity, and the default settings for file expiration.



Server Configuration

Property	Value
Workspace Build	version/3.5.1 (9210441)
Default File Availability	Immediately upon upload
Default File Expiration	Never
Recommended Session Timeout	15 minutes
Maximum Session Timeout	120 minutes
API Status	Online
Zone Quotas	Disabled

Web page management

As an administrator you can create and edit HTML documents that are used throughout Secure Workspace. On the Administration Tools page of the workspace dashboard there is a section called **Miscellaneous**. From here, select **View/Edit HTML documents** to create and edit HTML documents such as welcome emails and notifications.

Branding options

The Secure Workspace user interface can be branded to your requirements. Amongst other options, you can customise the colour scheme, the use of company logos and the dashboard features. Please contact your Egress account manager for further details.

Role appendix

Roles define the actions that users can perform in Secure Workspace. There are **System Roles** and **Zone Roles**. System roles define the core system permissions the user has, such as whether they have access to administration and auditing tools. Zone roles define the capabilities a user has on a per-zone basis. By default, Secure Workspace is provisioned with three system roles – Administrator, User and Guest User. There are also three default zone roles of the same types.

The permissions that these roles allow are detailed below:

Manage System Roles

	Administrator	User	Guest User
User Features – Ability to view and use the help and user data features of Secure Workspace			
Help Menu	✓	✓	✓
Quick Start Guide	✓	✓	✓
Search Zones	✓	✓	
Server Information	✓	✓	✓
User Dashboard	✓	✓	
Zone Features – Ability to use tools to create and access Zones and use the File Inbox			
Archived Zones	✓	✓	
Create Zones	✓	✓	
Favourite Zones	✓	✓	
File Inbox	✓	✓	
My Zones	✓	✓	
Shared Zones	✓	✓	✓
Zones Menu	✓	✓	✓
Administration Features – Ability to view and use the workspace administration features			
Admin Dashboard	✓		
Admin Tools	✓	✓	
API – Ability to upload and download files			
Use API	✓		
Session Management			
View Session Timeout Settings	✓	✓	
Edit Session Timeout Settings	✓	✓	
Server Upgrades – Ability to be notified when new Server Upgrades are available			
Notify of Server Upgrades	✓		
Users and Groups – Ability to manage users and groups			
View Users and Groups	✓		
Edit Users and Groups	✓		
Create Groups	✓		
Delete Groups	✓		
Add Users to Groups	✓		

Remove Users from Groups	✓		
Assign System Roles to Users	✓		
User Import (From CSV)	✓		
Export users to CSV	✓		
Auto-Enrolment Policies – Ability to manage policies when auto-enrolling users			
View Auto-Enrolment Policies	✓		
Edit Auto-Enrolment Policies	✓		
Create Auto-Enrolment Policies	✓		
Delete Auto-Enrolment Policies	✓		
Zone Management – Ability to create and manage zones			
Create a Zone on behalf of another user	✓		
Bulk Create Zones (From CSV)	✓		
Manage All Zones	✓		
Zone Templates – Ability to manage zone templates			
View Zone Templates	✓		
Edit Zone Templates	✓		
HTML Documents – Ability to manage the HTML documents used in Secure Workspace			
View HTML Documents	✓		
Create HTML Documents	✓		
Edit HTML Documents	✓		
System Audit – Ability to view system audit events e.g. user sign ins, file uploads, sent invitations			
View System Events	✓		
Export System Events	✓		
Roles and Capabilities – Ability to manage system and zone roles (inc. create, edit, delete)			
View System Roles	✓		
Edit System Roles	✓		
Create System Roles	✓		
Delete System Roles	✓		
View Zone Roles	✓		
Edit Zone Roles	✓		
Create Zone Roles	✓		
Delete Zone Roles	✓		
Create File/Folder Roles	✓		
View File/Folder Roles	✓		
Edit File/Folder Roles	✓		
Delete File/Folder Roles	✓		
Server Settings – Ability to change authentication and document editor settings			
View Authentication Settings	✓		
Edit Authentication Settings	✓		
View Document Editor Settings	✓		
Edit Document Editor Settings	✓		
View Automatic Update Settings	✓		
Edit Automatic Update Settings	✓		

Zone Templates – Ability to access the different styles of zone templates			
File Sharing	✓	✓	✓
Document Sharing	✓	✓	
Project Management	✓		
Marketing Projects	✓		
Court Bundles	✓		
Disclaimer Message – Ability to present a disclaimer before signing in to Secure Workspace			
No Disclaimer			
Notification Email Text	✓		
Welcome Email Text	✓		
Access Level Number – Ability to determine the System Access Roles a user can grant to other users			
Access Level Number Selection	✓		

Manage Zone Roles

	Administrator	**User**	**Guest User**
Zone Preferences – Ability to view a specific zone			
View Zone	✓	✓	✓
View Zone Information	✓	✓	✓
Administration – Ability to perform various administrative actions (e.g. deleting or archiving)			
Edit Zone Information	✓	✓	
Archive Zone	✓		
Delete Zone	✓		
View Zone Audit	✓	✓	
Discussion – Ability to use messaging features in a specific zone			
Add/Remove Discussion Messages	✓	✓	
View Zone Discussion	✓	✓	
E-mail Preferences – Ability to use the Direct Email feature in a zone			
Manage Direct Email to Zone Preferences	✓		
Send Direct Emails to Zone	✓	✓	
Sharing – Ability to share files and manage zone membership			
Edit Zone Members	✓		
View Zone Members	✓	✓	
Files/Folders Access Role – Ability to perform various actions on the files and folders in a zone			
Administer File Locks	✓		
Create Folders	✓	✓	
Delete Files/Folders	✓	✓	
Download Files	✓	✓	✓
Lock Files	✓	✓	
Move Files	✓	✓	
Rename Files	✓	✓	

View File History	✓	✓	
View File Properties	✓	✓	
Edit File Properties	✓	✓	
Add/Edit Files	✓	✓	
File Restrictions (Availability Dates)	✓		
Allow Exclusive Editing of Documents	✓		
View File/Folder Permissions	✓		
Edit File/Folder Permissions	✓		
Share an Individual File	✓		
Notification E-mail Events – Email notifications sent in the event of a specified zone action.			
Zones			
Zone Created	✓	✓	✓
Zone Created in Bulk	✓	✓	✓
Zone Modified			
Zone Renamed			
Zone Classification Modified	✓	✓	
Zone Archived/Reactivated			
Zone Added/Removed from Favourites			
Permission Changes	✓		
Access Requests Approved			
Access Requests Received			
Access Requests Denied			
Users Removed			
Files			
Files Added	✓	✓	✓
Files Deleted			
Files Downloaded			
Files Viewed			
Files Renamed			
Files Moved			
Files Locked/Unlocked			
File Descriptions Modified			
Folders Added			
Folders Renamed			
File Properties Viewed			
File Classifications Modified			
Folders Deleted			
Files Rejected			
File Type Violations			
Messages			
Messages Added	✓	✓	
Messages Edited			

Access Level Number – Ability to determine the Zone Access Roles a user can grant to other users			
Access Level Number Selection	✓		

Roles are fully customisable and as a business account administrator you have full control over the roles that users receive. They can also be assigned automatically to invited users. The specific permissions for each role can also be customised, and new roles can be created. See Changing a user's role and Changing role features for details.

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