egress

switch
secure data exchange

Egress Switch Secure Workspace 3.1

Administration Guide

April 2016

info@egress.com www.egress.com 0871 376 0014 @EgressSwitch

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

Introduction

Egress Switch 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 Switch's award-winning ease of use.

Switch 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 Switch Secure Workspace version 3.1, helping business administrators set up and manage their users and workspaces.

As an administrator you can:

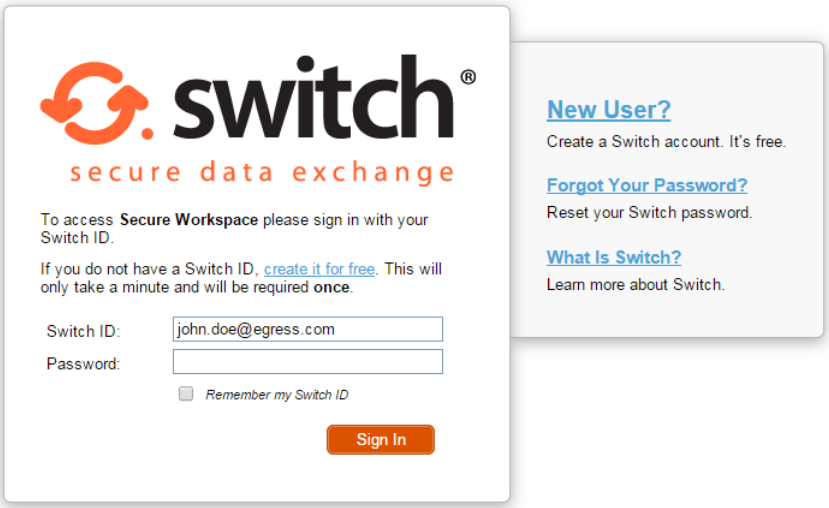
- Manage users, groups and roles
    - Invite users
    - Add users to groups
    - Change user roles
    - Disable user access to workspaces
- Manage workspaces
    - Create and delete workspaces
    - Share workspaces
    - Create and edit workspace templates
- View system audit events
    - View logs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

To understand the general-usage features of Switch Secure Workspace, please refer to *Egress Switch Secure Workspace 3.1 User Guide.*

Getting started

Signing in to Switch Secure Workspace

- Navigate to your Switch Secure Workspace web address. This should have been issued to you by your Egress Support representative.
- At the Egress Switch sign-in page, sign in with your Switch ID. Alternatively, Egress Switch 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 Switch Secure Workspace for the first time

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

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

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

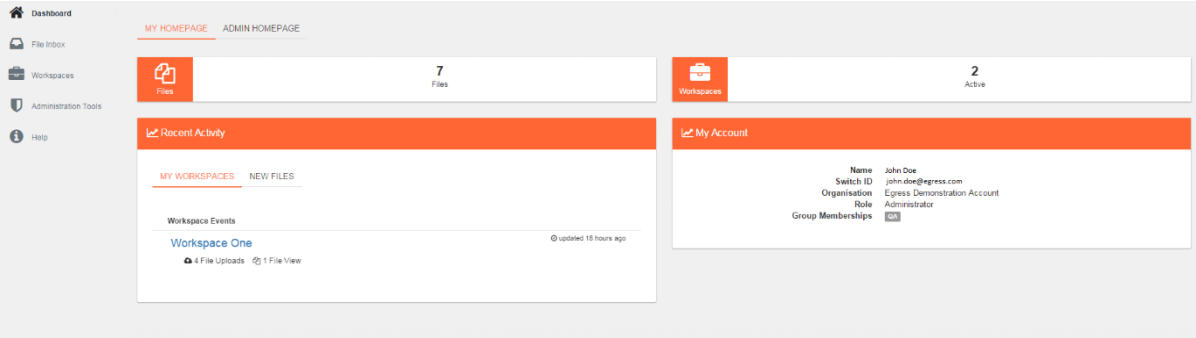
Once your workspace is created you may want to:

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

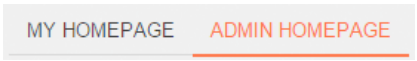
Using the dashboard

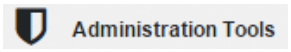
After signing in with your Switch ID you are presented with the Switch Secure Workspace dashboard. On the navigation sidebar you will find all of the tools you need to create and share workspaces and perform administrative functions. Also included is a help section and a file inbox. All users have their own dashboard and this user interface is customisable to suit your requirements. Please see Branding options for more details.

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



If you are listed as an administrator, you will have access to the administration tools in addition to your personal homepage:

- the **Admin Homepage** tab 

- the **Administration Tools** link on the sidebar 

Administration Tools

- Select the **Administration Tools** link on the sidebar to access various tools for managing users and workspaces. There are five different types of administration tools:
    - **Users and Groups Management**
    - **Roles and Capabilities**
    - **Manage Workspaces**
    - **Web Page Management**
    - **System Audit**
    - **Server Settings**

Adding new users

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

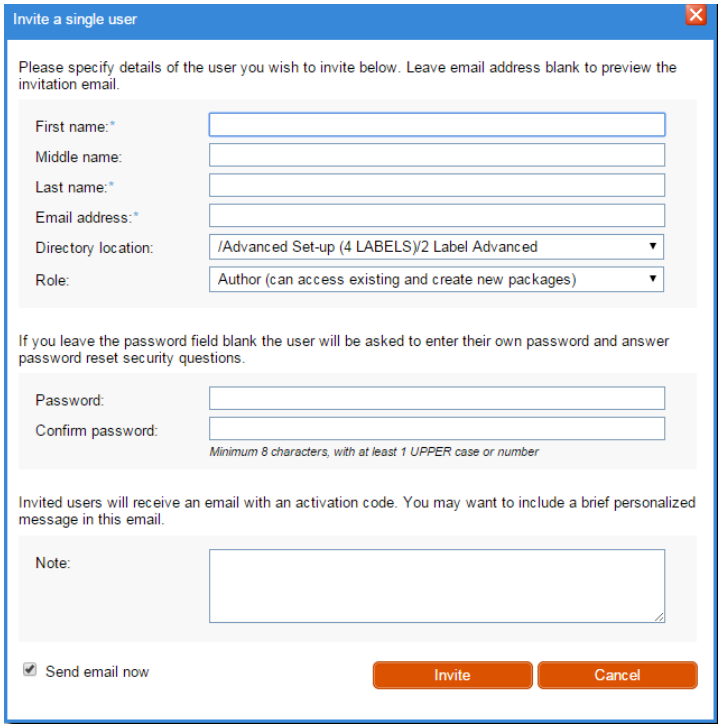
The Switch Secure Workspace auto-enrolment policy means that external users you share workspaces with are automatically granted access and so do not require you to create an account for them. If you want to add multiple third-party users in bulk without first sharing workspaces with them, you can do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

Internal users are automatically enrolled in Switch Secure Workspace via the Egress Switch 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.

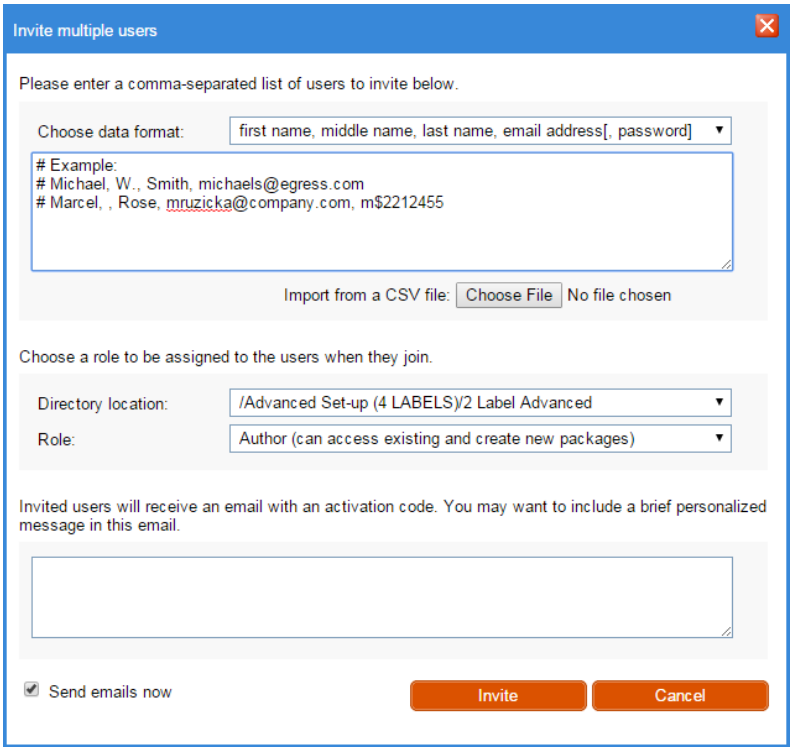
Adding internal users

1. Go to switch.egress.com (or local address) and sign in with your Switch ID. This opens the Switch 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 Switch Business Account.



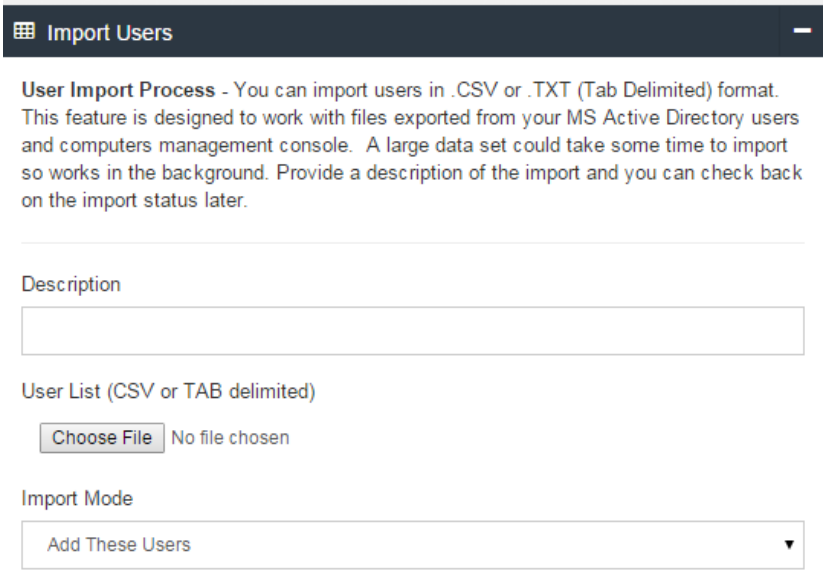
4. If you select **Invite Multiple Users**, you can either type in the user details into the text box in the window, or import the user details from a CSV file. You can choose the format the user data comes in but make sure when importing a CSV file that the data is arranged according to your chosen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



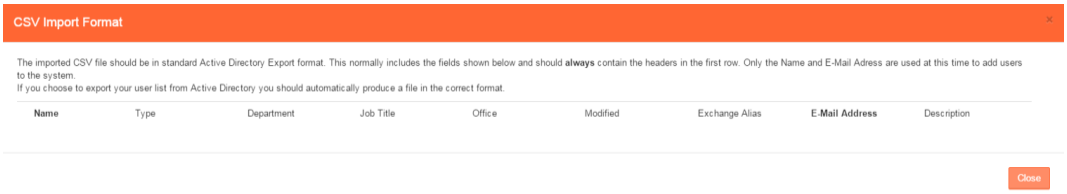
5. After typing in or importing the user details, choose a directory location and role for the imported users.
6. Optionally include a personalised message for the email these invited users will receive. Press **Invite**.

Adding external users

1. On the Administration Tools page in Switch Secure Workspace, go to **Bulk User Import (From CSV).**
2. 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.



3. 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. Switch Secure Workspace only uses the **Name** and **Email Address** fields to add users to the system.



4. Press **Save** to import your user list.

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

Creating auto-enrolment policies

You may wish to auto-enrol users from specific groups or Organisational Units in your Active Directory into a similar group in Switch 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.**
2. Press **Create 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 Switch 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 Switch 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 workspaces

Creating a workspace for another user

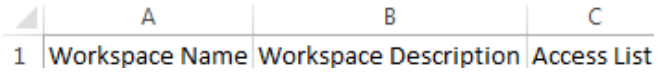
As a system administrator, you can create workspaces for other users and assign them as the workspace administrator. You can assign someone as a workspace administrator even if they do not exist on the system, simply enter their email address and they will be invited to create and activate their Switch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

To create a workspace for another user:

1. Select **Create a Workspace for other users** on the Administration Tools page.
2. Fill in the boxes in the **Workspace Create** page to give the new workspace a name, description, owner and template. The owner you specify will be given the workspace administrator role.
3. Choose whether to send an invitation email and whether to make the owner a **Power User**.
4. Click **Create**.

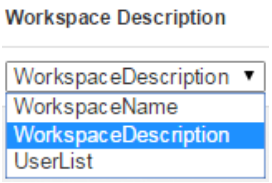
Creating workspaces in bulk

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



	A	B	C
1	Workspace Name	Workspace Description	Access List

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



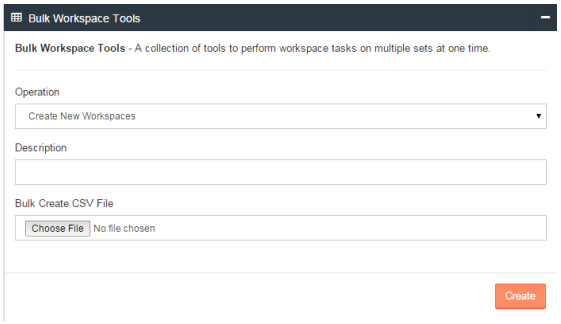
4. Choose the workspace role to give the members in your workspace access lists. Workspace roles are fully customisable, see the Changing role features section for details.
5. Choose who owns the new workspaces. This can be you, or the first name in the access list.
6. Select **Create** to create the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

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

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

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

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



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

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

Viewing and managing workspaces

You can view a list of all the workspaces under your administrative control. This is useful if you want to view workspace information such as the number of files a workspace contains, the owner's name or the date it was last modified.

- Go to the Administration Tools page and select **Manage All Workspaces.** You can click on a workspace name to go to that workspace if you have access.

Editing workspace templates

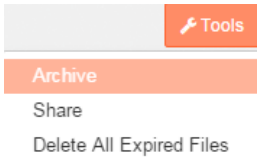
When you create a workspace, you start by choosing a workspace template. As an administrator you can view and edit the workspace templates available to your organisation. You may want to do this to allow or disallow certain file types being used, for example.

1. Select **View/Edit Workspace 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.

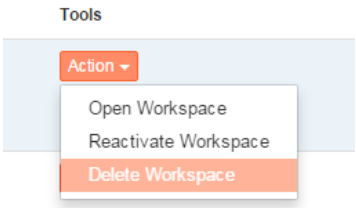
Deleting a workspace

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

1. Navigate to the workspace you wish to delete and select the **Tools** tab and then **Archive**. You can also archive a workspace from the **My Workspace** menu by selecting the **Action** drop-down menu.



2. Go to the archive by selecting **Workspaces** in the sidebar, and then select **Archive**. Locate the workspace to delete, and select **Action – Delete Workspace**.



Managing users and groups

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

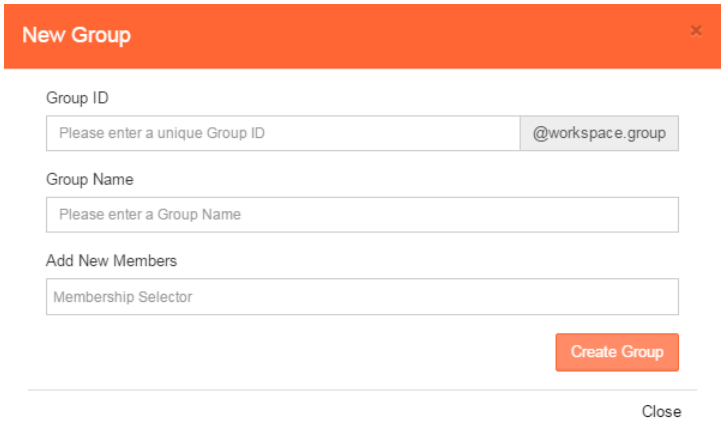
Use the ESI when managing internal users of your business account. The user details in the ESI are taken from your Active Directory. Any changes you make to internal users in Switch Secure Workspace will not affect their entry in the directory, so will only have an effect until they next sign in to their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

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

Creating a user group

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

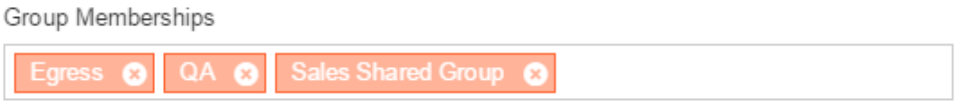
1. On the **Administration Tools** page, select **Manage Enrolled User and Group permissions**
2. Press the **Add New Group** button on the top right of the screen to open the **New Group** dialog box.
3. Choose a group ID and group name.
4. Press the drop down menu under **Add New Members** to choose 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.
2. Find the user whose group membership 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 user's name or the **View Account** button to open their **User Properties** window.
4. To add the user to a group, click inside the Group Membership text box. A drop-down menu appears, listing the current existing groups.



5. Choose the group(s) you wish to add the user to and then press **Save.**

- To remove the user from a group, simply go to their user properties window and press the **X** symbol by the group name, then press **Save.**

Changing a user's role

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

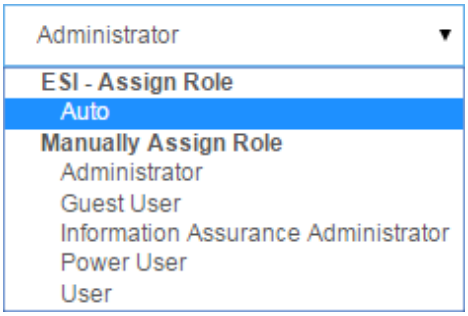
For example, a user may be a **Guest User** in the overall system, but an **Administrator** role in a particular workspace. They would not be able to create workspaces or perform other administrative or auditing functions, but would have full control over the functionality of the specific workspace they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

You can change internal users' system roles by going to the administration panel at switch.egress.com and selecting **User Management**. A quick way to reach this panel is to click on the user icon in Switch Secure Workspace, and select **Manage Switch Account**.

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 workspace role:

1. Go to the workspace
2. On the side of the workspace is a shared user list, organised by workspace 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 workspace roles.

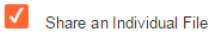
1. Select **Manage System Roles** or **Manage Workspace Roles** on the Administration Tools page.
2. Select the **Create New Role** button.
3. Name the new role and press **Create Role.**
4. The new role will appear in the list of roles. Select it and choose the capabilities you wish to give to users 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:

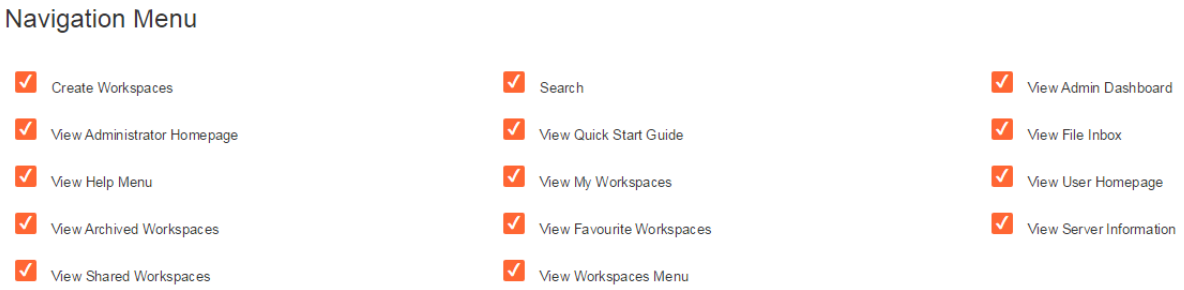
1. Go to **Manage System Roles** or **Manage Workspace Roles** on the Administration Tools page. Here you can see each role, the number of users assigned to each role and the number of capabilities a role contains.
2. Select a role to open the **Edit System Role** window.
3. Change the permission capabilities 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 workspace:

1. Navigate to the **Administration Tools** page, then to **Manage Workspace 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 workspace role capabilities.

Disabling user access

You may want to prevent a user from accessing any workspaces 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 workspaces under their administrative control. This provides in-depth access to information about user actions in Switch 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 of the workspaces you administrate, go to the Administration Tools page and select **System Security Events.** This lists:
    - Every action
    - The date each action occurred
    - The workspace where it occurred
    - The workspace'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 workspace dashboard by selecting **Admin Homepage** and then **Recent User Events.** From here, select the link to **View Audit Events**.

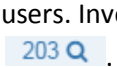
Viewing a user's audit log

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 Switch 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 workspaces, 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 authentication settings and document editor settings.

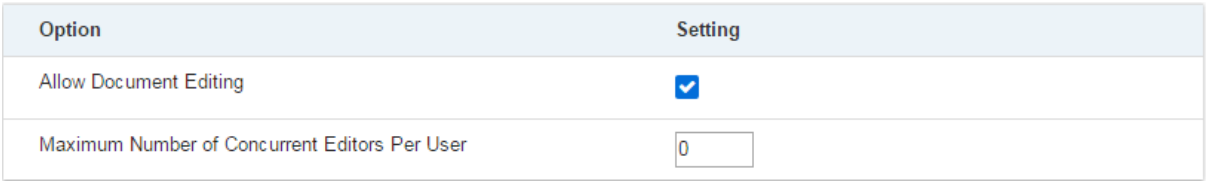
ESI authentication settings

Switch 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.

1. In Switch 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).

Viewing statistics

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

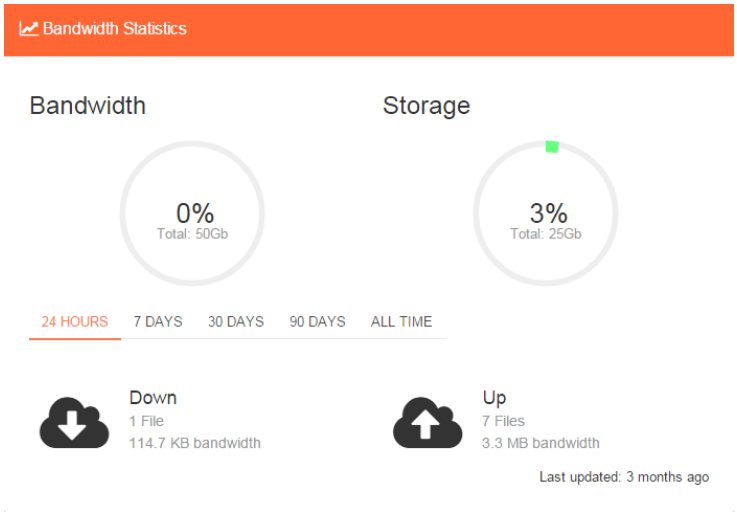
- Select the **Admin Homepage** tab on the main dashboard to access statistics and user information.

The top ribbon displays the total number of files in the workspaces you administrate, disk space these files use. It also displays the number of active and archived workspaces and the number of licenses in use. There are three windows on the admin homepage: **Bandwidth Statistics**, **File Statistics**, and **User Statistics**.

Bandwidth Statistics

The bandwidth statistics window displays:

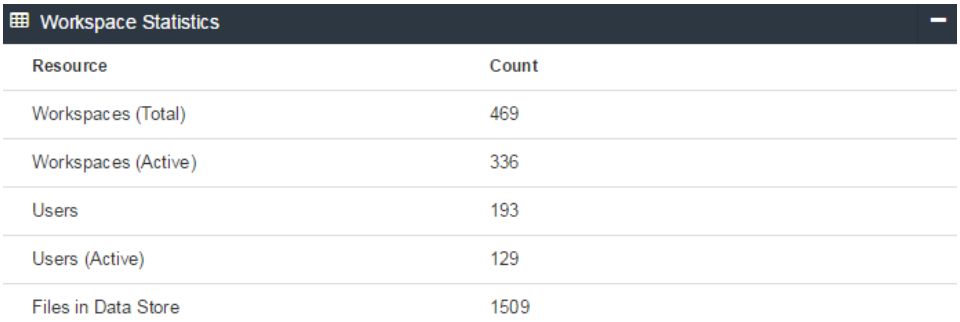
- **Bandwidth usage** as a percentage of total available bandwidth.
- **Storage space usage** as a percentage of total available storage space.
- **Up/down bandwidth data**: the number of files and amount of data uploaded and downloaded in different time frames (last 24 hours, all time, 7 days, 30 days and 90 days).



Workspace statistics

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

- Workspaces (total)
- Workspaces (active)
- Users
- Users (active)
- Files in Data Store

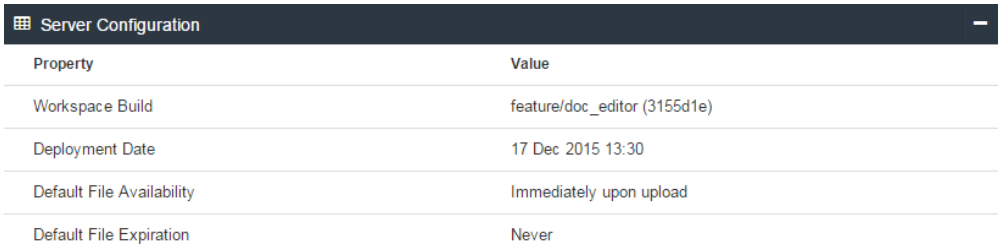


Workspace Statistics

Resource	Count
Workspaces (Total)	469
Workspaces (Active)	336
Users	193
Users (Active)	129
Files in Data Store	1509

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	feature/doc_editor (3155d1e)
Deployment Date	17 Dec 2015 13:30
Default File Availability	Immediately upon upload
Default File Expiration	Never

Server updates

The **Administration Tools** page contains a **Server Updates** section, which lets administrators allow or prevent automatic server updates. If the box is checked, whenever new updates to Switch Secure Workspace are released they are automatically made available, allowing users to start using new functionality immediately.

Web page management

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

Branding options

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

The permissions that these roles allow are detailed below:

System roles

	Administrator	User	Guest User
User Features – Ability to view and use the help and user data features of Switch Secure Workspace			
Help Menu	✓	✓	✓
Quick Start Guide	✓	✓	✓
Search Workspaces	✓	✓	
Server Information	✓	✓	✓
User Dashboard	✓	✓	
Workspace Features – Ability to use tools to create and access workspaces and use the File Inbox			
Archived Workspaces	✓	✓	
Create Workspaces	✓	✓	
Favourite Workspaces	✓	✓	
File Inbox	✓	✓	
My Workspaces	✓	✓	
Shared Workspaces	✓	✓	✓
Workspaces Menu	✓	✓	✓
Administration Features – Ability to view and use the workspace administration features			
Admin Dashboard	✓		
Admin Tools	✓		
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)	✓		
Roles and Capabilities – Ability to manage policies when auto-enroling users			
View Auto-Enrolment Policies	✓		
Edit Auto-Enrolment Policies	✓		
Create Auto-Enrolment Policies	✓		
Delete Auto-Enrolment Policies	✓		
Workspace Management – Ability to create and manage workspaces			

Create a Workspace on behalf of another user	✓		
Bulk Create Workspaces (From CSV)	✓		
Manage All Workspaces	✓		
Workspace Templates – Ability to manage workspace templates			
View Workspace Templates	✓		
Edit Workspace Templates	✓		
CMS Documents – Ability to manage the HTML documents used in Switch Secure Workspace			
View CMS Documents	✓		
Create CMS Documents	✓		
Edit CMS 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 workspace roles (inc. create, edit, delete)			
View System Roles	✓		
Edit System Roles	✓		
Create System Roles	✓		
Delete System Roles	✓		
View Workspace Roles	✓		
Edit Workspace Roles	✓		
Create Workspace Roles	✓		
Delete Workspace 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	✓		
Workspace Templates – Ability to access the different styles of workspace templates			
File Sharing	✓	✓	✓
SWOT Analysis	✓	✓	✓

Workspace roles

	Administrator	**User**	**Guest User**
Workspace Preferences –Ability to view a specific workspace			
View Workspace	✓	✓	✓
View Workspace Information	✓	✓	✓
Administration –Ability to perform various administrative actions (e.g. deleting or archiving)			
Edit Workspace Information	✓	✓	
Archive Workspace	✓		
Delete Workspace	✓		
View Workspace Audit	✓	✓	
Discussion –Ability to use messaging features in a specific workspace			
Add/Remove Discussion Messages	✓	✓	

View Workspace Discussion	✓	✓	
E-mail Preferences –Ability to use the Direct Email feature in a workspace			
Manage Direct Email to Workspace Preferences	✓		
Send Direct Emails to Workspace	✓	✓	
Files and Folders –Ability to perform various actions on the files and folders in a workspace			
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)	✓		
Sharing – Ability to share files and manage workspace membership			
Share an Individual File	✓	✓	
Edit Workspace Members	✓		
View Workspace Members	✓	✓	
Document Editing – Ability to edit documents inline			
Allow Exclusive Editing of Documents	✓		
Notification E-mail Events – Email notifications sent in the event of a specified workspace action. **Workspaces**			
Workspace Created	✓	✓	✓
Workspace Created in Bulk	✓	✓	✓
Workspace Modified			
Workspace Renamed			
Workspace Classification Modified	✓	✓	
Workspace Archived/Reactivated			
Workspace 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			

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.

Switch support centre

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

Useful contact information:

Egress Europe:	+44-844-8000-172
Egress North America	1-888-505-8318
Egress Australia	1-800-768-043
Egress Singapore	800-130-2208
Egress Website Address:	http://www.egress.com
Egress Sales:	sales@egress.com
Account Services:	accountservices@egress.com
Support:	support@egress.com
Follow Egress Online:	Twitter
	Facebook
	LinkedIn
	Egress Blog