

Colligo Console

Administrator Guide



Contents

About this guide.....	6
Audience.....	6
Requirements.....	6
Colligo Technical Support.....	6
Introduction.....	7
Colligo Console Overview.....	8
Colligo Console Home Page.....	9
Users.....	10
Users Page Actions.....	10
User Properties.....	12
Application behavior after a user is deactivated or deleted.....	13
Sites.....	15
Sites Page Actions.....	15
Site Properties.....	16
Groups.....	17
Groups Page Actions.....	17
Group Properties.....	18
Application behavior when a user is removed from a group or a group is deleted.....	19
Streams.....	21
Stream Actions.....	21
Stream Properties.....	22
Pinned Locations.....	23
Pinned Location Actions.....	23
Application behavior when a location is pinned.....	24
Pinned Location Properties.....	25
Policies.....	26
Policy Actions.....	26

Dashboards	27
Console Activity	27
Group Activity Dashboard	28
User Activity Dashboard	29
Email Manager Dashboard	30
Document Distribution Dashboard	32
Settings.....	33
Federation	33
Devices	34
User Profile and Help Menu	35
Federation.....	36
AD FS Federation.....	36
Create a Relying Party Trust in AD FS.....	36
Collect Settings Information.....	46
Configure AD FS in Colligo Console.....	49
Removing Access	51
Troubleshooting.....	51
Azure AD Federation.....	52
Configure Azure AD in Colligo Console.....	52
Viewing the Colligo Azure AD App in the Azure Management Portal.....	54
Removing Access	55
Troubleshooting.....	55
Binding AD Groups to Colligo Console Groups.....	56
Configuring Single Sign-On (SSO).....	57
Federate your organization in Colligo Console.....	57
Configure client browsers to support SSO	57
Configure AD FS to enable SSO for Edge and Chrome	57

Table of Figures

Figure 1: Colligo Console home page	9
Figure 2: Users Page.....	10
Figure 3: User Properties.....	12
Figure 4: User Properties: Groups	14
Figure 5: Sites Page	15
Figure 6: Site Properties	16
Figure 7: Groups Page.....	17
Figure 8: Group Properties.....	18
Figure 9: Group Properties: Users	19
Figure 10: Group Properties: Sites.....	20
Figure 11: Streams.....	21
Figure 12: Stream Properties.....	22
Figure 13: Stream Properties: Pinned Locations	23
Figure 14: Pinned Location Properties.....	25
Figure 15: Policies.....	26
Figure 16: Group Activity Dashboard	28
Figure 17: User Activity Dashboard	29
Figure 18: Email Management information.....	30
Figure 19: Email Management: Number of mails archived	31
Figure 20: Email Management: Number of Emails Archived by Location	31
Figure 21: Document Distribution information.....	32
Figure 22: Document Distribution: Search bar and Document List	32
Figure 23: Settings Page	33
Figure 24: Confirm de-authorization	34
Figure 25: User Profile.....	35
Figure 26: Help Menu	35
Figure 27: Adding a Federated Tenant: AD FS	50

Figure 28: Federated Tenants after configuring ADFS.....	51
Figure 29: Error message when the Token-signing Certificate has expired.....	51
Figure 30: Adding a Federated Tenant: Azure AD	53
Figure 33: Federated Tenants after Federating Azure AD.....	54
Figure 34: Azure Management Portal.....	54
Figure 35: Troubleshooting Granting Access in Azure AD when oauth is chosen.....	55
Figure 36: Troubleshooting Granting Access in Azure AD when wsfed is chosen.....	55

About this guide

This guide contains information on how to use, maintain, and configure Colligo Console for use in your organization.

Audience

This guide is intended for use by the person responsible for managing your organization's Colligo configuration. Federation and Single Sign-On should be performed by an IT administrator with network knowledge.

Requirements

Browser

Colligo Console requires the latest browser version.

Federation

Paid plans fully support federation with AD FS (3.0 and higher) and with Azure AD.

Authentication types supported by each protocol are listed below.

AD FS: supports **wsfed**

Azure AD: supports **oauth** and **wsfed**

Note: SAML is not supported.

Single Sign-On (SSO)

Colligo Console SSO is supported for organizations federated with Colligo Console using AD FS 3.0 and the **wsfed** authentication type on Windows Server 2010 R2 with the latest versions of Internet Explorer, Edge, or Chrome.

Colligo Technical Support

If you have a problem with your Colligo software, following are the available support options:

1. Colligo Knowledge Base: <http://www.colligo.com/support/knowledgebase>.
2. Colligo Support Community: <http://www.colligo.com/support/community>.
3. Colligo Online Support: <https://www.colligo.com/support/request>.

Submit a ticket online if you have current M&S or an active subscription.

Introduction

Colligo Console is a powerful management and analytics center, built on the Microsoft Azure cloud server. Colligo Console logs user activity for the different Colligo apps and makes the data available to IT administrators to facilitate decision making and to enforce compliance.

Colligo Console also serves as the central management center for configuring and managing Apps on any device. No company files are ever stored on the cloud service – your files remain on your systems, securely under your control.

Colligo Console is accessed at <https://www.colligoapp.com>.

Definitions

Group: A group is used within Colligo Console to push specific Streams, Pinned Locations, and Policies to a group of users.

Pinned Location: A pinned location is a specific location that is made up of a pre-configured site and a relative path. Pinning a location allows users to upload items directly to it. It also allows users to automatically synchronize the location for potential offline use.

Policy: A policy is used to specify allowed behavior at the level at which it is configured. A policy can be applied to a User, Site, Group, Stream, or Pinned Location.

Role: A role identifies which security privileges a user has within the system.

- **Admin:** This user is granted full setup, configuration, and reporting for an organization.
- **User:** This user can only access the home page (for downloading apps and requesting support) and the **Settings** page (for de-authorizing devices).

Site: A site in Colligo Console is the URL of a location you want made available to your Colligo app. Associating a site with a **Group** makes it available to the users in that group.

Stream: A stream is a collection of bookmarks that relate content for easy access. For example, grouping files and folders by project or legal matter or product or client.

Tenant: In the case of AD FS, 1 tenant is equivalent to 1 AD FS server. In the case of Azure AD, 1 tenant is equivalent to 1 Azure Active Directory.

Colligo Console Overview

Colligo Console Configuration

Colligo Console is where the Colligo Administrator configures and manages content to be made available to end users. It is recommended that Users and Sites are configured first.

A brief description of each configuration item is below. For details on how to perform the configuration activity, refer to the specific section.



The Groups page is where you define how content is available to users. All users in a group will have access to sites associated with the group and streams defined in the group.



Streams are defined in a group and contain Pinned Locations that are pushed to members of the group.



The Sites page is where you add a site and apply policies to a site.



The Users page is where you configure users and apply policies to a user. Colligo Console manages user licensing for Colligo apps, so a user must be defined to be able to use Colligo apps.



The Settings page is where you de-authorize devices and configure Tenant Bindings (if applicable to your plan).

Colligo Console Dashboards

Colligo Console is where you access centralized reporting dashboards for:

- Group Activity
- User Activity
- Email Management
- Document Distribution

Access all Dashboards from the left navigation column by clicking the  icon.

Colligo Console Home Page

To log in to Colligo Console, browse to <https://www.colligoapp.com>, enter your email address and click **Next**. Enter your password if prompted.

The home page for Colligo Console contains the following:

Navigation: access the configuration pages, the dashboards, or return to the home page.

Downloads: links for downloading Colligo apps.

Quick Start: get started quickly by adding a site from the home page. For additional options, use the **Sites** page.

Licensing and Plan Type: licensing and plan information are displayed here.

User Profile: links to the Terms of Service, the Privacy Policy, the logout option, and information regarding your organization.

Documentation and Support: links to the Quick Start Guide, the Administrator Guide, and the Colligo Support community forums, knowledge base, and help system.

Release Notes (not displayed in the figure below): This link is at the bottom right of the page.

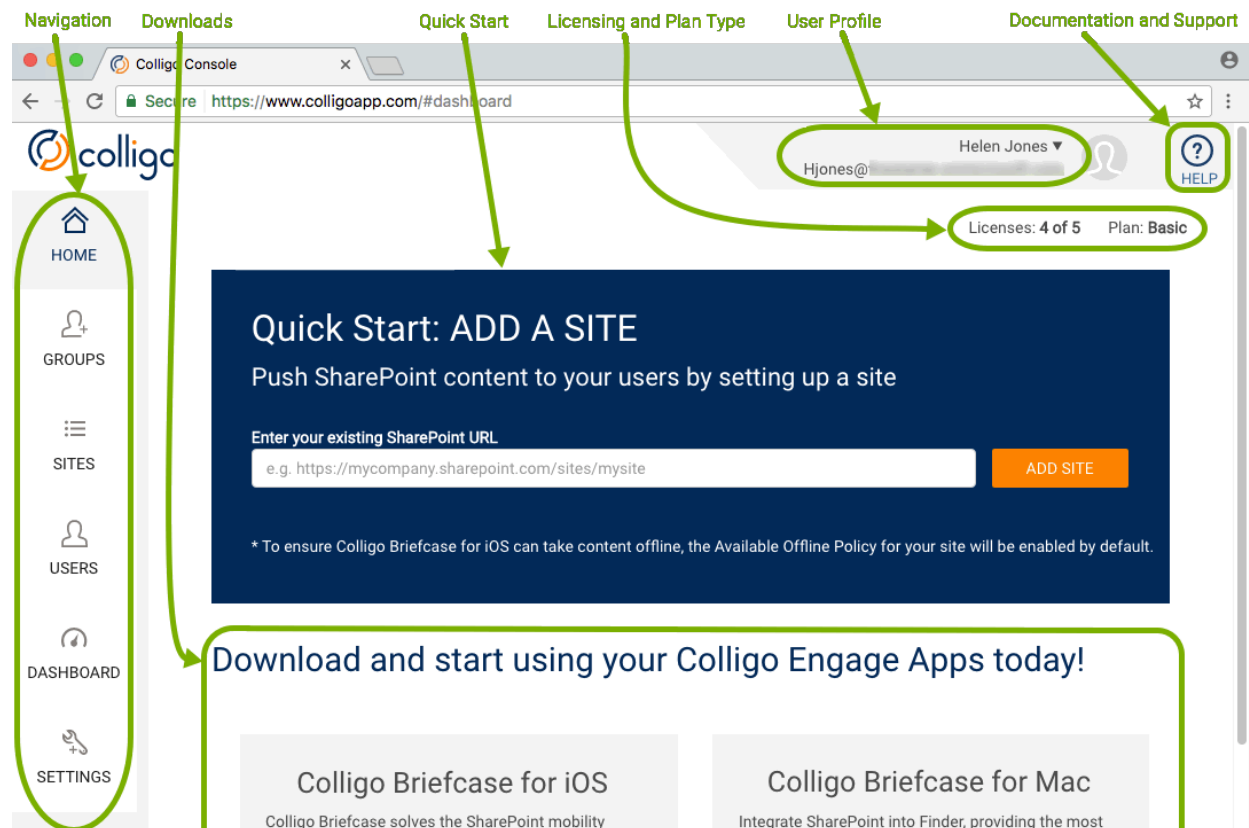



Figure 1: Colligo Console home page

Users

The Users page is where you configure users and apply policies to a user. Colligo Console manages user licensing for Colligo apps, so a user must be defined to be able to use Colligo apps.

The Users page is accessed by clicking the  icon in the left navigation column. Users are listed in a tabular view containing the following information:

Name: used to identify a user within Colligo Console

Email: a user's unique identifier within Colligo Console

Role(s): refers to the Colligo Console role(s) which are defined at the start of this guide

Control Group: indicates if the Control Group policy has been applied to the user

Status: a user's status within the system (Active or Not Active)

Send Invitation Email: a link to send an invitation email to the user

Users

- Users					
<input type="text" value="Search by name..."/>		Search	Sort	Add	Import
Name	Email	Role(s)	Control Group	Status	
Elizabeth Johnson	[REDACTED]	User	✗	Active	Send Invitation Email
Gordon Smith	[REDACTED]	User	✗	Active	Send Invitation Email
Helen Jones	[REDACTED]	Admin, User	✗	Active	Send Invitation Email

Figure 2: Users Page

Users Page Actions

Actions available from the Users page are:

Search for a specific user.

Sort users in alphabetical order ascending or descending.

Add a new user. Once a user has been added, you can modify the User Properties.

Import multiple users by importing a spreadsheet containing user information.

View/Modify User Properties. This is where you can delete or deactivate a user.

Send an Invitation Email to the user.

To **Add** an individual user:

1. Click **Add** on the Users table action bar.
2. On the **Add User** page, enter the requested information.

User Email is used for all password updates and for all login communication. As such, a user can have only one email address.

Phone Number and **Role/Position** are optional.

Send Invitation Email is checked by default. An invitation email will be sent to the new user when you click **Add User**. If you do not wish this to happen (because you first wish to configure policies), uncheck the setting.

3. Click **Add User** and the user will be added to the Users table.

To **Import** multiple users:

1. Click **Import** on the Users table action bar.
2. Follow the instructions on the **Import Users** page.

Send Invitation Email is checked by default. An invitation email will be sent to the new users when you click **Import Users**. If you do not wish this to happen (because you first wish to configure policies), uncheck the setting.

3. Click **Import Users** and the users will be added to the Users table.

Federation (not available in the Basic Plan) is discussed in the [Settings](#) section.

Send Invitation Email

When you click **Send Invitation Email**, the user will be sent an email invitation from Colligo Technical Services (donotreply@colligoapp.com). Basic Plan users will receive an email with a button for the user to confirm the email address and set a password. Federated users will receive an email with a link to sign in to Colligo Engage.

User Properties

The User Properties page is where you view/modify user information, assign roles, delete or deactivate the user, configure policies for the user, and see which groups the user is a member of.

The User Properties page is accessed by clicking the **Name** entry in the Users table:

Helen Jones

First Name
Helen

Last Name
Jones

Display Name
Helen Jones

Email
hjones@██

Phone
██

Role/Position

Locked Out?
No

[Edit User](#)
[Edit Roles](#)
[Deactivate](#)
[Delete User](#)

Policies

+ Policies
Sort Configure Policies

Groups

+ Groups

Search
Sort

Figure 3: User Properties

User information is listed at the top of the page with four action buttons:

Edit User: click this button to edit user information such as name and email.

Edit Roles: click this button to add or remove the Admin role.

(De)Activate: click this button to change the status of a user.

Delete User: click this button to delete the user.

Application behavior after a user is deactivated or deleted

Deactivated and deleted users are not able to log in to Colligo Console or into any Colligo apps. If a user is deactivated or deleted while logged in, behavior is as described below.

Briefcase for iOS and Briefcase for Mac: The user will be prompted to log-in during the next sync with Colligo Console.

Email Manager for Outlook (v8): The user will be prompted to log-in during the next sync with Colligo Console. If the user does not log in, the Add-in will change to a dormant state. Synchronizations will stop, and the user will not be able to upload emails. Unsynchronized changes will remain unsynchronized.

Email Manager for Outlook (v7) with Colligo Console: Synchronization will no longer occur. Offline items will still be available in the Colligo PST, current as of the date of the last synchronization. The user will be prompted to log-in during the next sync with Colligo Console. Dismissing the login screen will unload the add-in automatically, thus removing Colligo functionality. The PST file will remain behind.

Briefcase for Windows (v7) with Colligo Console: Synchronization will no longer occur. Files which were previously synchronized, including unsynchronized changes from the user's machine, will remain on the user's system. The Stand-alone interface will close, with subsequent restarts of the Stand-alone application prompting for credentials, then closing because the credentials are no longer valid.

Beneath User information is the Policies table for the user. Policies applied at the User level apply only to the specific user. For details on how to configure polices, refer to the [Policies](#) section.

Beneath the Policies table is the Groups table for the user:

Groups

- Groups

Search
Sort


Name	Control Group	Sites	Streams
All Users	✘	☰ sites >	☰ streams >
Marketing	✘	☰ sites >	☰ streams >

Figure 4: User Properties: Groups

All groups the user is a member of are listed in this table. For details on the group information displayed in the table, refer to the [Groups](#) section. Actions available from the Groups table are *Search*, *Sort*, and *View/Modify Group Properties*. For details on these actions, refer to the [Groups Page Actions](#) section.

Sites

The Sites page is where you add a site and apply policies to a site. A site in Colligo Console is the URL of a location you want made available to your Colligo app. Associating a site with a **Group** makes it available to the users in that group.

The Sites page is accessed by clicking the  icon in the left navigation column. Sites are listed in a tabular view containing the following information:

Name: used to identify a site within Colligo Console

URL: the base URL address of the site

Sites

Name	URL	Provider
Marketing	https://[REDACTED]	SharePoint
Sales	https://[REDACTED]	SharePoint

Figure 5: Sites Page

Sites Page Actions

Actions available from the Sites page are:

Search for a specific site.

Sort sites in alphabetical order ascending or descending.

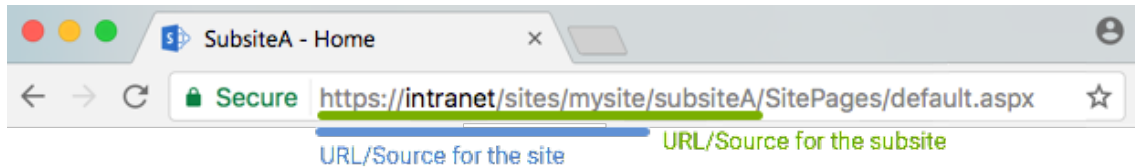
Add a new site. Once added, you can modify the Site Properties.

View/Modify Site Properties. This is where you can delete a site.

To **Add** a site:

1. Click **Add** on the Sites table action bar.
2. On the **Add Site** page, enter the requested information.

URL/Source is the base URL for the site, as shown in the example.



3. Click **Add Site** and the site will be added to the Sites table.

Site Properties

The Site Properties page is where you view/modify the site name or URL, delete the site, and configure policies for the site.

The Site Properties page is accessed by clicking the **Name** entry in the Sites table:

Sales

URL/Source
https://[redacted]

Provider
SharePoint

[Edit Site](#) [Delete Site](#)

Policies

Policies		
Policy Name	Enabled	Value(s)
Available Offline	Yes	true

Figure 6: Site Properties

Site information is listed at the top of the page with two action buttons:


Edit Site: click this button to edit the site Name and URL/Source information.

Delete Site: click this button to remove the site.

Beneath Site information is the Policies table for the site. Most policies applied at the Site level apply to the site, any of its sub-sites, and any pinned locations using this site as a base. Some Colligo applications require that the **Available Offline** policy be enabled at **both** the pinned location level and at the site level. For details on how to configure polices, refer to the [Policies](#) section.

Groups

The Groups page is where you define how content is available to users. All users in a group will have access to sites associated with the group and streams defined in the group.

The Groups page is accessed by clicking the  icon in the left navigation column. Groups are listed in a tabular view containing the following information:

Name: used to identify a group within Colligo Console

Control Group: indicates if the Control Group policy has been applied to the group

Sites ( **sites** >): a link to Sites associated with the group

Streams ( **streams** >): a link to Streams associated with the group

Groups





Name	Control Group	Sites	Streams
All Users	✘	 sites >	 streams >
Marketing	✘	 sites >	 streams >

Figure 7: Groups Page

The **All Users** group is automatically created and contains all users defined for your organization. This group cannot be deleted and its membership cannot be changed.

Groups Page Actions

Actions available from the Groups page are:

Search for a specific group.

Sort groups in alphabetical order ascending or descending.

Add a new group. Once added, you can modify the Group Properties.

View/Modify Group Properties. This is where you can delete the group.

The  **sites** > icon is a shortcut for viewing or modifying Sites associated with the group.

The  **streams** > icon is a shortcut for viewing or modifying Streams defined in the group.

To **Add** a group:

1. Click **Add** on the Groups table action bar.
2. On the **Add Group** page, enter a group name.
3. Click **Add Group** and the group will be added to the Groups table.

Group Properties

The Group Properties page is where you configure tenant bindings (if your plan permits them), rename the group, delete the group, configure users for the group, associates sites with the group, define and configure streams for the group, and configure policies for the group.

The Group Properties page is accessed by clicking the **Name** entry in the Groups table:

The screenshot shows the 'Group Properties' page for a group named 'Sales'. The page is organized into several sections, each with a title and a corresponding action bar:

- Name:** Sales
- Tenant Bindings:** Includes three buttons: 'Configure Tenant Bindings' (dark blue), 'Edit Group' (dark blue), and 'Delete Group' (orange).
- Users:** Includes a '+ Users' button, a search input field labeled 'Search by name...', and buttons for 'Search', 'Sort', 'Add', and 'Remove'.
- Sites:** Includes a '+ Sites' button, a search input field labeled 'Search by name...', and buttons for 'Search', 'Sort', 'Add', and 'Remove'.
- Streams:** Includes a '+ Streams' button, a search input field labeled 'Search by name...', and buttons for 'Search', 'Sort', and 'Add'.
- Policies:** Includes a '+ Policies' button, a 'Sort' button, and a 'Configure Policies' button.

Figure 8: Group Properties

Group information is listed at the top of the page with three action buttons:

Configure Tenant Bindings: if using Active Directory (AD) and your organization is federated with Colligo Console, click this button to add a Tenant-Group binding. For example, you might bind the Colligo Console group “Sales” with the AD group “Sales”. For details, refer to the [Binding AD Groups to Colligo Console Groups](#) section.

- This feature is not available in the Basic Plan.

Edit Group: click this button to rename the group.

Delete Group: click this button to delete the group.

Beneath Group Information is the Users table for the group:

Users

- Users					
Search by name...		Search	Sort	Add	Remove
Name	Email	Role(s)	Control Group	Status	
Helen Jones	[REDACTED]	Admin, User	✘	Active	Send Invitation Email
Gordon Smith	[REDACTED]	User	✘	Active	Send Invitation Email

Figure 9: Group Properties: Users

All users that are members of the group are listed in this table. For details on the user information displayed in this table, refer to the [Users](#) section.

To **Add** or **Remove** a user to/from the group:

1. Click **Add** or **Remove** on the Users table action bar.
2. Select the user(s) you wish to add or remove.
 - Select all users on a page by using the select all box.
 - Navigate between pages by using the navigation bar at the bottom.
3. Click **Add Users** or **Remove Users** and the Users table will be updated.

Application behavior when a user is removed from a group or a group is deleted

When a user is removed from a group, or a group is deleted, group configuration (Sites, Streams, and Policies) will no longer apply. Any previously pushed Stream, Folder or Favorite that is removed locally, will not be re-pushed. Within the app, behavior will differ, as described below.

Briefcase for Android and Briefcase for Mac: pushed locations become local sites.

Email Manager for Outlook (v8), Email Manager for Outlook (v7) with Colligo Console, and Briefcase for Windows (v7) with Colligo Console: group configuration is removed from the user's system.

Other actions available from the Users table are *Search*, *Sort*, *View/Modify User Properties*, and *Send Invitation Email*. For details on these actions, refer to the [Users Page Actions](#) section.

Beneath the Users table is the Sites table for the group:

Sites

- Sites			Search by name...	Search	Sort	Add	Remove
Name	URL	Provider					
Sales		SharePoint					

Figure 10: Group Properties: Sites

All sites associated with the group are listed in this table. For details on the site information displayed in this table, refer to the [Sites](#) section.

To **Add** (Associate) or **Remove** (Association of) a site:

1. Click **Add** or **Remove** on the Sites table action bar.
2. Select the site(s) you wish to add or remove.
 - Select all sites on a page by using the select all box.
 - Navigate between pages by using the navigation bar at the bottom.
3. Click **Add** or **Remove Sites** and the Sites table will be updated.

Note: Sites added using the Quick Start panel are automatically associated with the All Users group and will appear in the Sites table listed on the all Users Properties Page. All users will be able to access sites added from the Quick Start. Sites added from the Sites page are not available to users until they are associated with the group as described above.

Other actions available from the Sites table are *Search*, *Sort*, and *View/Modify Site Properties*. For details on these actions, refer to the [Sites Page Actions](#) section.

Beneath the Sites table is the Streams table for the group. All streams defined in the group are listed in this table. For details on how to define and configure streams, refer to the [Streams](#) section.

Beneath the Streams table is the Policies table for the group. Policies applied at the Group level apply all users in the group. For details on how to configure polices, refer to the [Policies](#) section.

Streams

A stream is defined in a group and contains Pinned Locations that are pushed to members of the group. A stream is a collection of bookmarks that relate content for easy access. For example, grouping files and folders by project or legal matter or product or client.

Streams are listed on the Group Properties page and can also be accessed from the Groups page by clicking the **streams >** icon for the group:

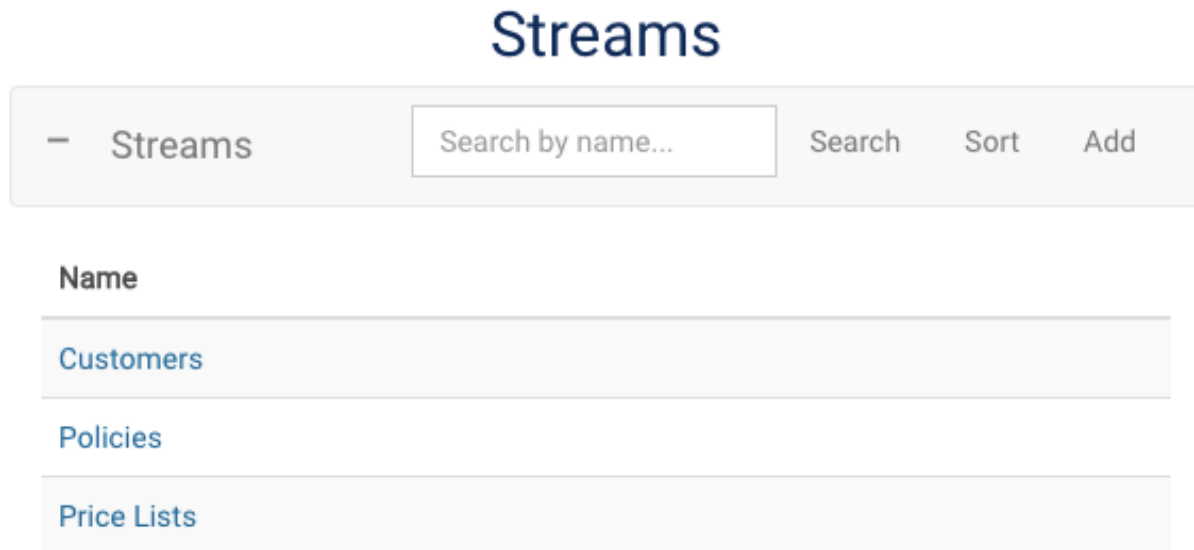


Figure 11: Streams

Stream Actions

Actions available for Streams are:

Search for a specific stream in the group.

Sort streams defined in the group in alphabetical order ascending or descending.

Add a stream to the group. Once added, you can modify the Stream Properties.

View/Modify Stream Properties. This is where you can delete the stream.

To **Add** a stream:

1. Click **Add** on the Streams table action bar.
2. On the **Add Stream** page, enter a stream name.
3. Click **Add Stream** and the stream will be added to the Streams table.

Stream Properties

The Stream Properties page is where you rename the stream, delete the stream, and configure pinned locations and policies for the stream.

The Stream Properties page is accessed by clicking the **Name** entry in the Streams table:

The screenshot displays the Stream Properties interface. At the top, the title "Price Lists" is centered. Below it, the "Name" field contains "Price Lists". Two action buttons are visible: "Edit Stream" (dark blue) and "Delete Stream" (orange). Below this is the "Pinned Locations" section, which includes a table header with a plus sign, the text "Pinned Locations", a search input field with the placeholder "Search by name...", and three action buttons: "Search", "Sort", and "Pin Location to Stream". Below the Pinned Locations section is the "Policies" section, which includes a table header with a plus sign, the text "Policies", and two action buttons: "Sort" and "Configure Policies".

Figure 12: Stream Properties

Stream information is listed at the top of the page with two action buttons:

Edit Stream: click this button to rename the stream.

Delete Stream: click this button to delete the stream.

Beneath Stream information is the Pinned Locations table for the stream. All locations pinned to this stream are listed in this table. For details on how to configure pinned locations, refer to the [Pinned Locations](#) section.

Beneath the Pinned Locations table is the Policies table for the stream. Policies applied at the Stream level apply to all Pinned Locations in the stream. For details on how to configure polices, refer to the [Policies](#) section.

Pinned Locations

A pinned location lives within a Stream and is a specific location made up of a pre-configured site and a relative path. Pinning a location allows users to upload items directly to it. It also allows users to automatically synchronize the location for potential offline use.

Pinned Locations are listed on the Properties page for the Stream in which it is pinned. Pinned Locations are listed in a tabular view containing the following information:

Display Name: used to identify the location within the stream

URL: the relative path to the location

Un-Pin: a link to remove the pinned location from the stream

Pinned Locations ⓘ

- Pinned Locations			
	<input type="text" value="Search by name..."/>	Search	Sort
			Pin Location to Stream
Display Name	Url		
2016 Price List	/		Un-Pin
2016 Promotions	/		Un-Pin
2016 Renewal Pricing	/		Un-Pin
2017 Price List	/		Un-Pin
2017 Promotions	/		Un-Pin
2017 Renewal Pricing	/		Un-Pin

Figure 13: Stream Properties: Pinned Locations

Pinned Location Actions

Actions available for Pinned Locations are:

Search for a specific pinned location in the stream.

Sort pinned locations in the stream in alphabetical order ascending or descending.

(Un-)Pin Location to Stream: add or remove a location to this stream.

Note: Pinning a very large site may lead to performance degradation within the application.

View/Modify Pinned Location Properties. This is where you configure policies for the location.

To **Un-Pin a Location** from a stream, click **Un-Pin**.

To **Pin a Location** to a stream:

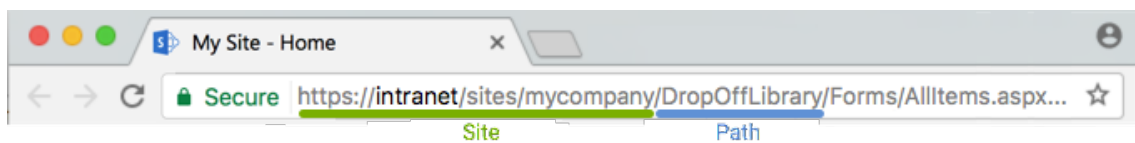
1. Click **Pin Location to Stream** on the Pinned Locations table action bar.
2. On the **Pin Location to Stream** page, enter the requested information.

Site is a pre-configured site chosen from the drop-down menu. For details on how to configure a site, refer to the [Sites](#) section.

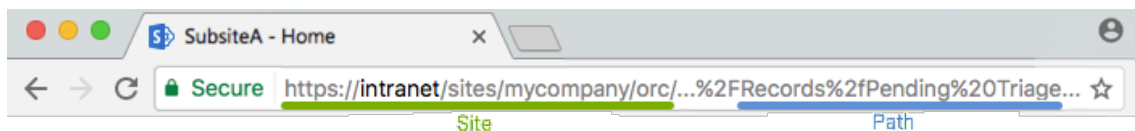
Path is the portion of the URL (as seen in the browser address bar) after what is configured for the **Site URL** and contains only the path to the location. Examples are shown below.

- Pinning a very large site (**Path** is left blank) may lead to performance degradation within the application.
- For some applications, pinning a subfolder of a list or library will result in the application adding the list or library that contains the subfolder.

Example of a Document Library in a site:



Example of a folder (Pending Triage) in a Document Library (Records) in a subsite:



The **Path** in the example above can also be entered as `Records/Pending%20Triage`.

Name is used to identify the location within Colligo Console and can be any relevant text.

Description is only used within Colligo Console.

3. Click **Pin to Stream** and the location will be added to the Pinned Locations table.

Application behavior when a location is pinned

When a location is pinned, application behavior is as described below.

Briefcase for iOS and Briefcase for Mac: the location will be pushed to connected Colligo apps during the next Colligo Console sync. On a Mac, force a sync by clicking the Colligo logo and choosing **Synchronize**. In iOS, force a sync by pressing the **Sync** icon within the application.

Email Manager for Outlook (v8), Email Manager for Outlook (v7) with Colligo Console, and Briefcase for Windows (v7) with Colligo Console: the location will be received during the next start of the application.

Pinned Location Properties

The Pinned Location Properties page is where you view/modify the pinned location configuration.

The Pinned Location Properties page is accessed by clicking the **Display Name** entry in the Pinned Location table.

Edit Pinned Location

Site

Sales ⌵

Name

2017 Price List

Path

[https://firestarter.sharepoint.com/sl/ PriceLists/2017](https://firestarter.sharepoint.com/sl/PriceLists/2017)

Description

Pinned Location for 2017 Price Lists ⌵

Save Changes
Cancel

Policies

+ Policies	Sort	Configure Policies
------------	------	--------------------

Figure 14: Pinned Location Properties

Pinned Location information is listed at the top of the page. Modify information as required and click **Save Changes** to return to the Stream Properties page.

Beneath the Pinned Location information is the Policies table for the Pinned Location. Policies applied at the Pinned Location level apply only to the specific pinned location. For details on how to configure polices, refer to the [Policies](#) section.

Policies

A policy is used to specify allowed behavior at the level at which it is configured. A policy can be configured for a User, Site, Group, Stream, or Pinned Location.

Policies are listed on the Properties page for the item for which it is configured. Policies are listed in a tabular view containing the following information:

Policy Name: used to identify the policy

Enabled: indicates if the policy has been enabled

Value(s): value(s) associated with the policy

Policies		
Policy Name	Enabled	Value(s)
Allow Offline Content	Yes	true

Figure 15: Policies

Policy Actions

Actions available for Policies are:

Sort enabled policies in alphabetical order ascending or descending.

Configure Policies at the current level (User, Site, Group, Stream, or Pinned Location).

To configure a policy:

1. Click **Configure Policies** on the Policies table action bar.
2. The **Configure Policies** page will list policies available at the current level.

To **disable** a policy, toggle the Yes / No switch to **No**.

To **enable** a policy, toggle the Yes / No switch to **Yes** and select (or specify) a value for the policy.

3. Click **Save Policies** and the Policies table will be updated.

Dashboards

Colligo Console displays a rich set of activity data in formats including interactive graphs, bar charts, and raw data. Centralized reporting dashboards are available for:

Group Activity: Colligo application ratings are displayed with an interactive graph containing up to a year of group activity. Up to 30 days of group activity can be downloaded.

User Activity: Colligo application ratings are displayed with an interactive graph containing up to a of user activity. Up to 30 days of user activity can be downloaded.

Email Management: Data specific to email management is displayed with an interactive graph containing up to 30 days of email activity and a bar chart of emails archived by location. Up to 30 days of email activity can be downloaded.


Document Distribution: Data specific to document distribution is displayed with a searchable list of the last 90 days of download activity.

Console Activity

Console activities included in the interactive graphs are as described below:

Drop-down	Included activities
Edit	<p>Add: An item is added or copied from the local file system or from SharePoint.</p> <p>CheckIn, CheckOut, DiscardCheckOut: Any check in, check out, or discard check out.</p> <p>Delete: An item is deleted from the local file system or from SharePoint.</p> <p>Edit: The metadata on an item is edited either at add time, or on an existing item.</p> <p>SyncEngine:Upload: An upload that happen as a result of sync activity. May be logged as a direct result of some of the other user actions (e.g. An Add can cause an upload).</p>
Read	<p>Read: A document has been opened.</p>
Share	<p>AttachInEmail and LinkInEmail: A file is shared in an email as an attachment or link using Colligo applications.</p>
Sync	<p>SyncEngine:StartListSync: The start of a list/library sync.</p> <p>SyncEngine:Download: A download that happens as a result of sync activity. May be logged as a direct result of some of the other user actions (e.g. A Read can cause a download).</p>
All	<p>All the above, as well as:</p> <p>AccountAdd: A new account is added either by a user within an application or via getting an account pushed from Colligo Console.</p>

Group Activity Dashboard

The Group Activity dashboard is accessed by clicking the  icon in the left navigation column. Colligo application ratings are displayed at the top of the dashboard followed by an interactive graph containing up to a year of group activity:

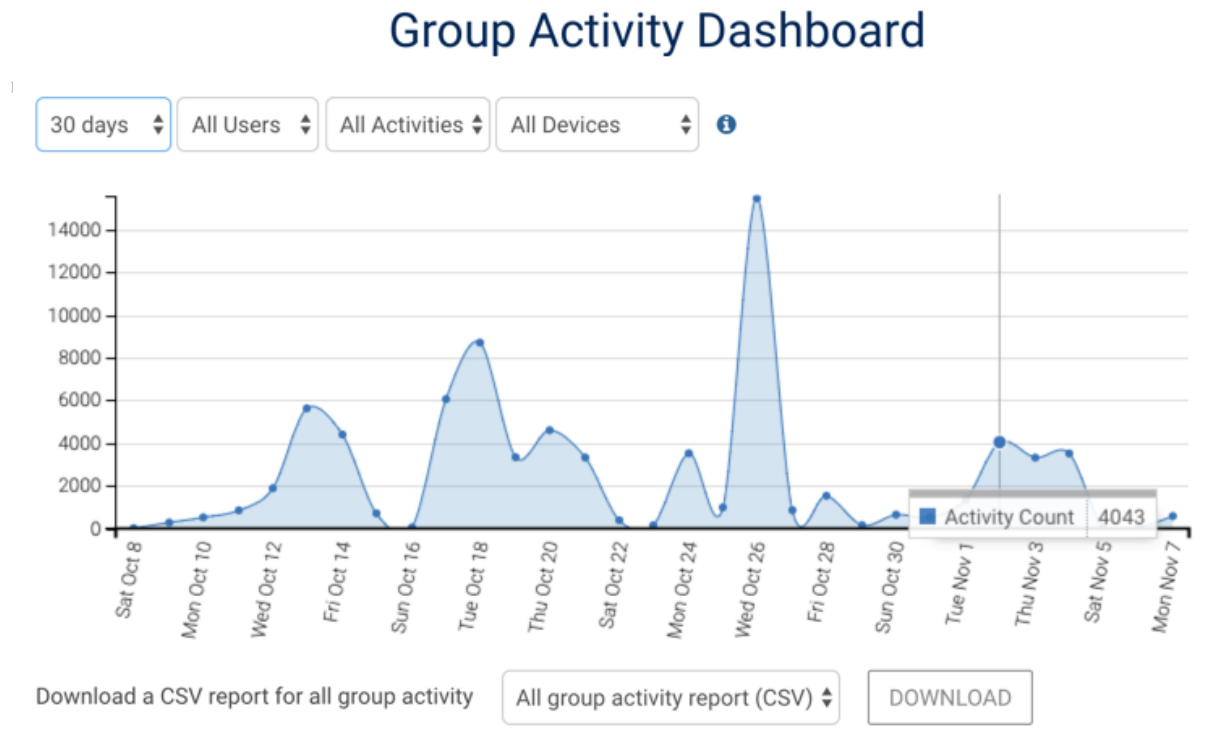



Figure 16: Group Activity Dashboard

Hover over a specific point in the graph and the value at that time will be displayed. Drop-down controls allow you to change the:

- **duration** (1 day, 7 days, 30 days, 6 months, 1 year)
- **group name**
- **activity** (All Activities, Edit, Read, Share, Sync), as defined in the [Console Activity](#) section
- **device** on which activity is taking place

Beneath the graph is a button for downloading 1, 7, or 30 days of all Group Activity.

User Activity Dashboard

The User Activity dashboard is accessed by clicking the  icon in the left navigation column and then clicking the words **User Activity**. Colligo application ratings are displayed at the top of the dashboard followed by an interactive graph containing up to a year of user activity:

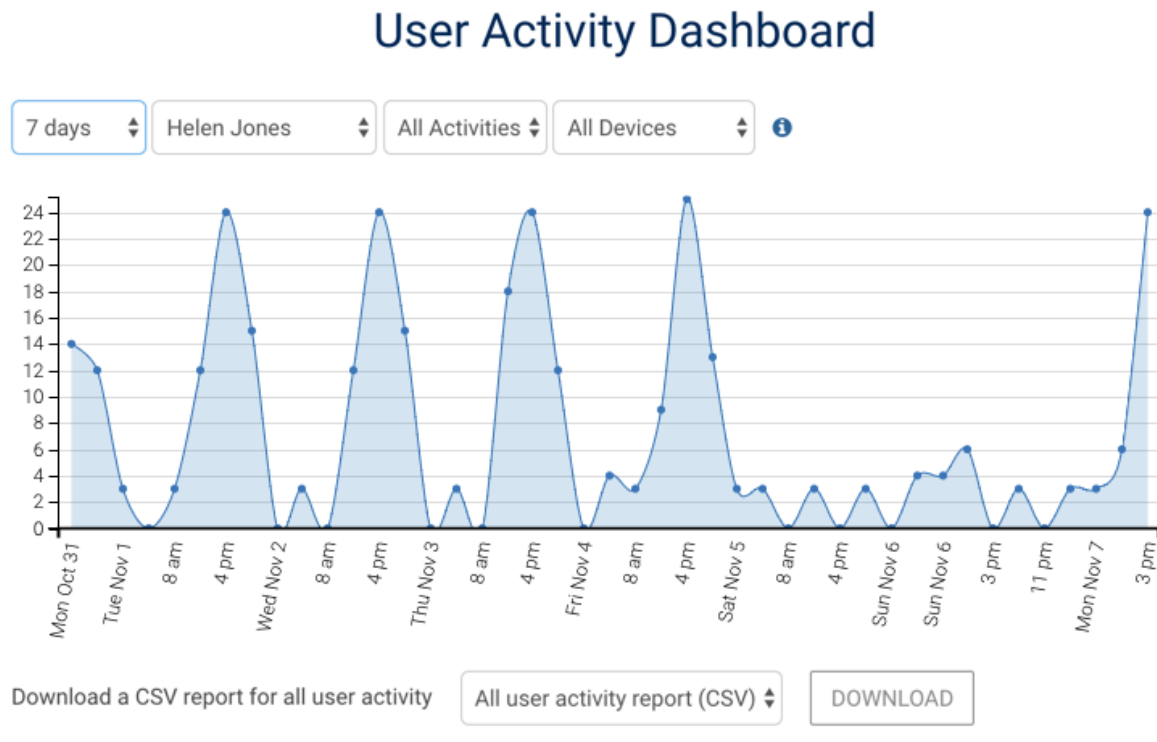



Figure 17: User Activity Dashboard

Hover over a specific point in the graph and the value at that time will be displayed. Drop-down controls above the graph allow you to change the:

- **duration** (1 day, 7 days, 30 days, 6 months, 1 year)
- **user name**
- **activity** (All Activities, Edit, Read, Share, Sync), as defined in the [Console Activity](#) section
- **device** on which activity is taking place

Beneath the graph is a button for downloading 1, 7, or 30 days of all User Activity.

Email Manager Dashboard

The Email Manager dashboard is accessed by clicking the  icon in the left navigation column and then clicking the words **Email Manager**. Data specific to email management is displayed at the top of the dashboard with data for:

Devices Deployed: Number of unique devices deployed in Colligo Console, excluding browsers.

Active Users: Number of users that have posted activities in the past 15 minutes.

Emails Uploaded: Total number of emails uploaded today.

Number of Emails: Total number of emails uploaded to date.

Emails Uploaded (Avg.): Average number of emails uploaded to date by users who have logged in at least once.

Users Uploading Emails: Percentage of users (logged in at least once) who have uploaded emails to date.

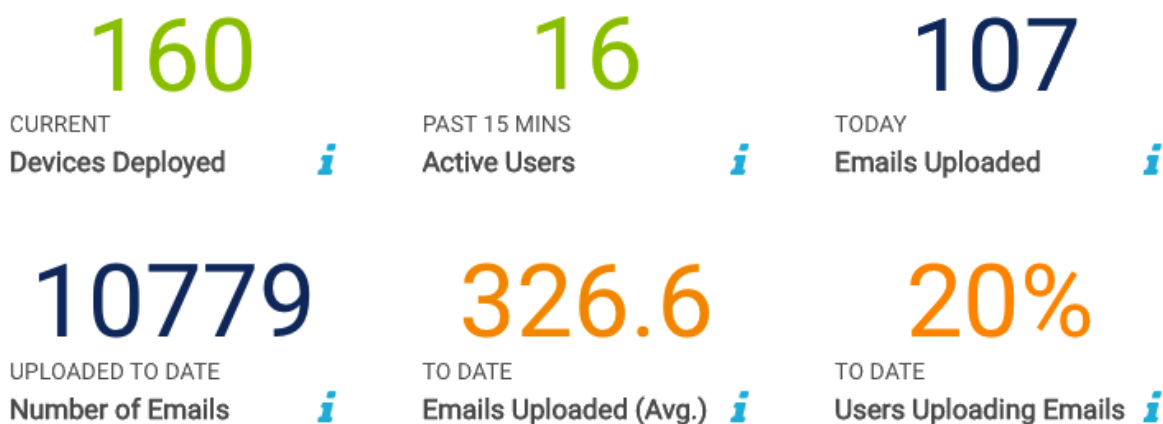


Figure 18: Email Management information

Beneath these boxes an interactive graph displays the number of emails archived over time. Hover over a specific point in the graph and the value at that time will be displayed.

Drop-down controls above the graph allow you to change the:

- **duration** (1 day, 7 days, 30 days)
- **platform** (All Platforms, Desktop, Mobile)
- **device** on which activity is taking place
- **group** for which the activity is being reported

Email Manager Dashboard

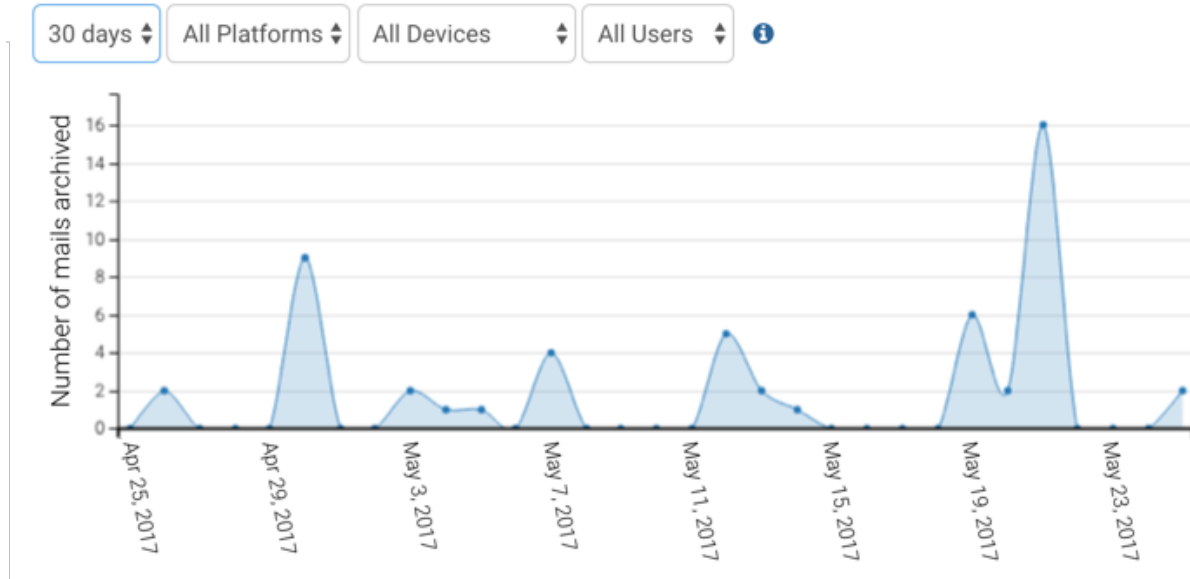


Figure 19: Email Management: Number of mails archived

Under this graph is a bar chart of the number of emails archived by location.

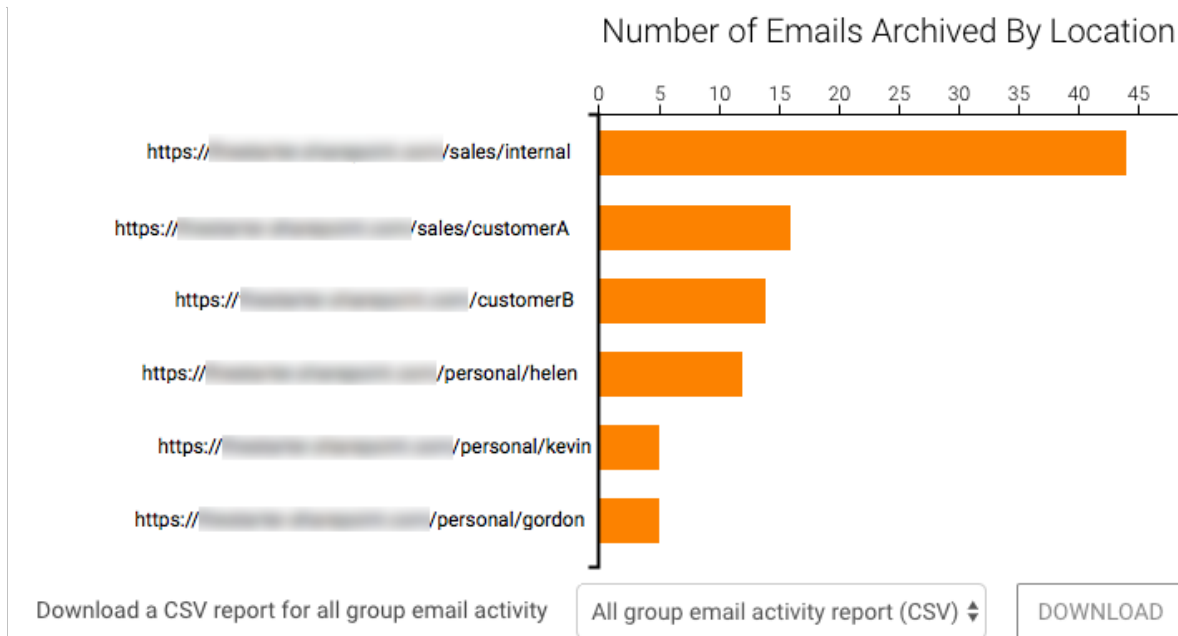



Figure 20: Email Management: Number of Emails Archived by Location

Beneath this bar chart is a button for downloading 1, 7, or 30 days of all Group Email Activity.

Document Distribution Dashboard

The Document Distribution dashboard is accessed by clicking the  icon in the left navigation column and then clicking the words **Document Distribution**. Data specific to document distribution is displayed at the top of the dashboard with data for:

- Documents downloaded today.
- Devices synced today.
- Users downloading documents today.



Figure 21: Document Distribution information

Beneath these boxes is a list of the last 90 days of download activity. Actions available are:

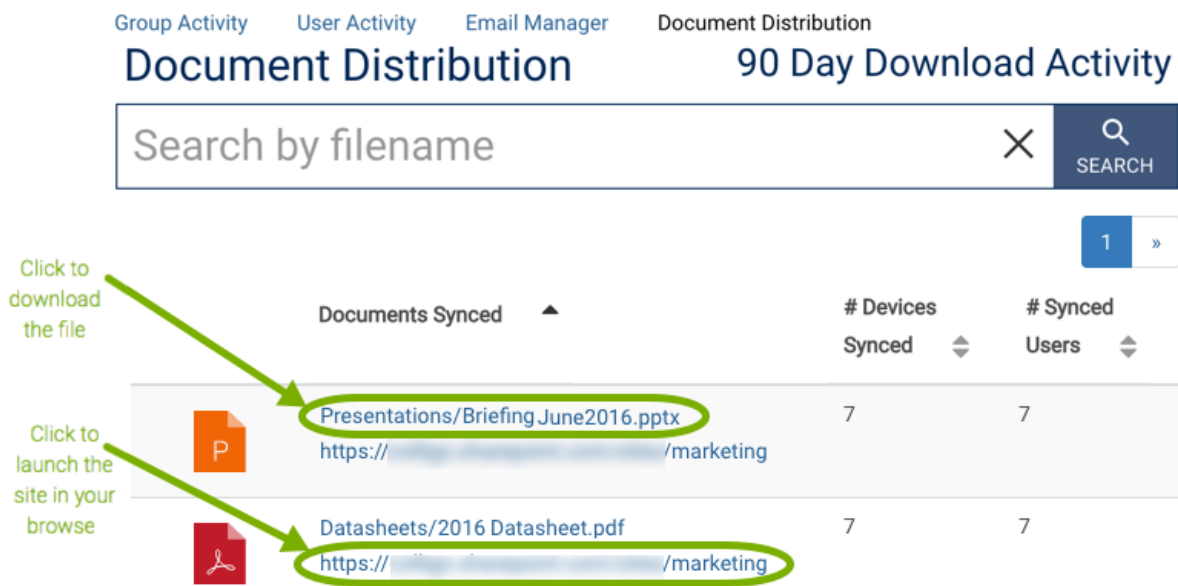
Search for a file using the search bar.

Sort columns by clicking on the direction arrow next to the column title.

Download the file by clicking on the file name (top link in the file list).

Launch the site in your browser by clicking the site URL (bottom link in the file list).

Note: Data beyond 90 days is not retained.



The screenshot shows the 'Document Distribution' dashboard with the '90 Day Download Activity' section. A search bar is at the top with the text 'Search by filename'. Below it is a table with columns: 'Documents Synced', '# Devices Synced', and '# Synced Users'. Two rows of data are visible:

Documents Synced	# Devices Synced	# Synced Users
Presentations/Briefing June2016.pptx https://.../marketing	7	7
Datashheets/2016 Datasheet.pdf https://.../marketing	7	7

Annotations in the image include:

- A green arrow pointing to the search bar with the text 'Click to download the file'.
- A green arrow pointing to the file name 'Presentations/Briefing June2016.pptx' with the text 'Click to launch the site in your browse'.
- Green circles highlighting the file names and URLs in the table.

Figure 22: Document Distribution: Search bar and Document List

Settings

The Settings page is where you view a list of signed in devices, de-authorize devices, and modify authentication and federation settings (if applicable to your plan).

The Settings page is accessed by clicking the  icon in the left navigation column.

[Click here](#) to modify authentication & federation settings. (preview!)

Devices

Warning: When deauthorizing devices, it may take up to 15 minutes to log out all devices.

- Device Sign Ins		Deauthorize All Devices	
Product/Device	Name	IP Address / Unique ID	Last Login
Browser	Chrome	[REDACTED]	05/25/2017 15:57 PM (UTC)
Outlook	OutlookApp	[REDACTED]	04/24/2017 17:28 PM (UTC)
Android	Engage Xamarin Android	[REDACTED]	03/23/2017 14:25 PM (UTC)
Mac OS X	Colligo Engage	[REDACTED]	05/12/2017 20:03 PM (UTC)

Figure 23: Settings Page

A link to **modify authentication & federation settings** is displayed at the top of the page followed by a list of all devices and browsers used to log in to Colligo applications.

Federation

Paid plans fully support federation with AD FS and with Azure AD. AD serves as the identity provider for authentication as well as for tenant-group bindings.

Supported protocol versions and the authentication types supported by each protocol are listed at the start of this document in the [Requirements](#) section.

For details on how to federate your organization in Colligo Console, refer to the [Federation](#) section.

Note: Federation is not available in the Basic Plan. Clicking the link to modify authentication and federation settings will display a message to this effect.

Devices

All devices and browsers used to log in to Colligo applications are listed in a tabular view containing the following information:

Product/Device and Name: This combination shows how/where the login to Colligo occurs, be it Colligo Console, or one of the Colligo Apps.

IP Address / Unique ID: The identifier for the log in.

Last Login: Date when the log in occurred.

De-authorizing Devices

Click **Deauthorize All Devices** on the Device Sign Ins table action bar. A popup will appear:

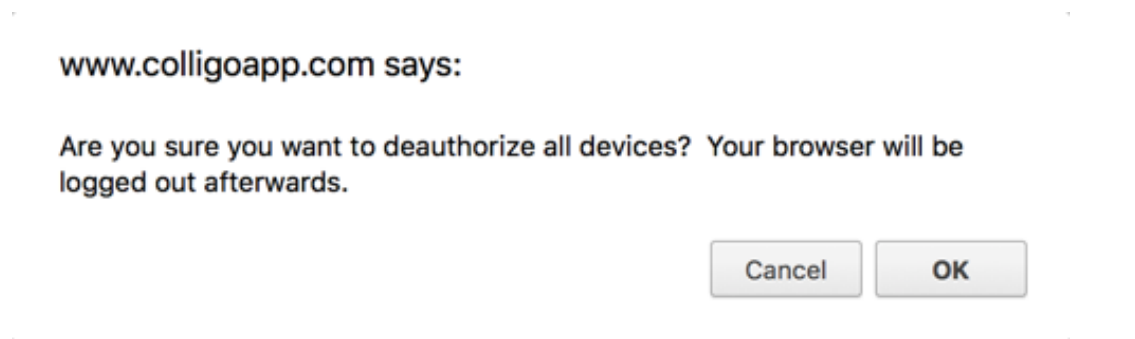


Figure 24: Confirm de-authorization

Click **OK** to continue. It is recommended that you close your browsers after clicking **OK**. It may take up to 15 minutes to log out all devices.

User Profile and Help Menu

The User Profile is where you can access information for your organization, the Terms of Service, the Privacy Policy, and the option to Logout of Colligo Console.

The Help menu contains links to documentation and the Colligo Support Center.

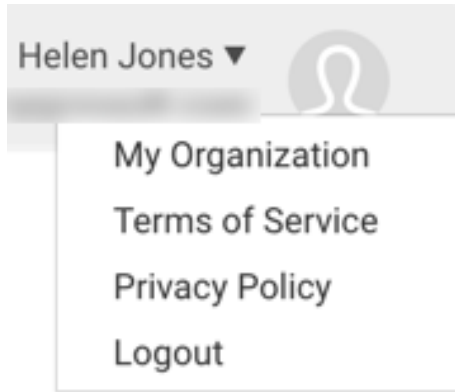


Figure 25: User Profile

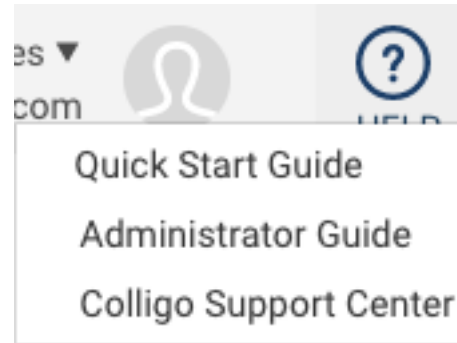


Figure 26: Help Menu

My Organization will list information for your organization followed by the information found on the Users, Groups, and Sites pages. Underneath the Organization Information is the button **Edit Organization Details**. Click here to change the name of the Organization.

Federation

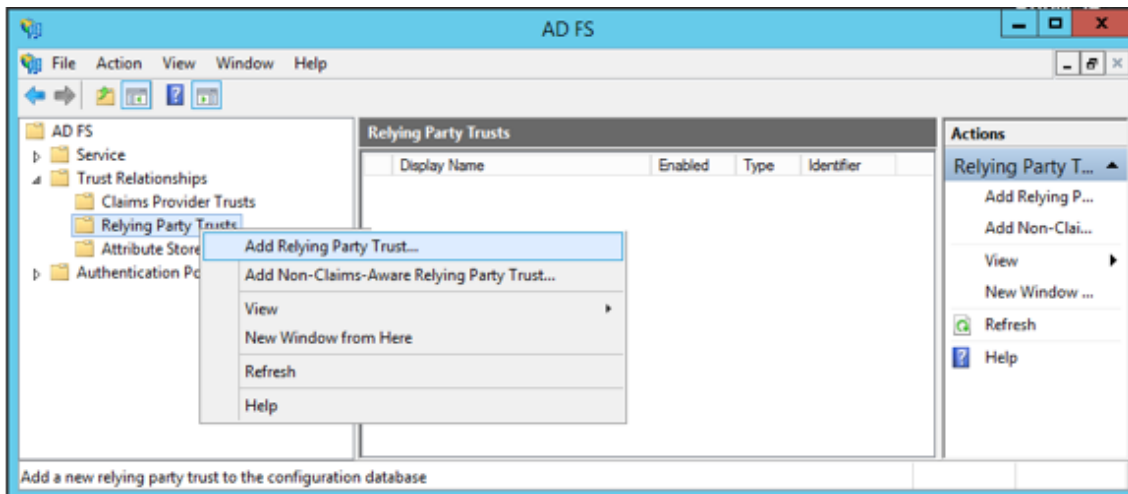
AD FS Federation

To set up AD FS Federation in Colligo Console you need the **entityID**, the thumbprint and expiry of the Primary Token signing certificate, and the Authorization Endpoint from the Relying Party Trust for Colligo Engage.

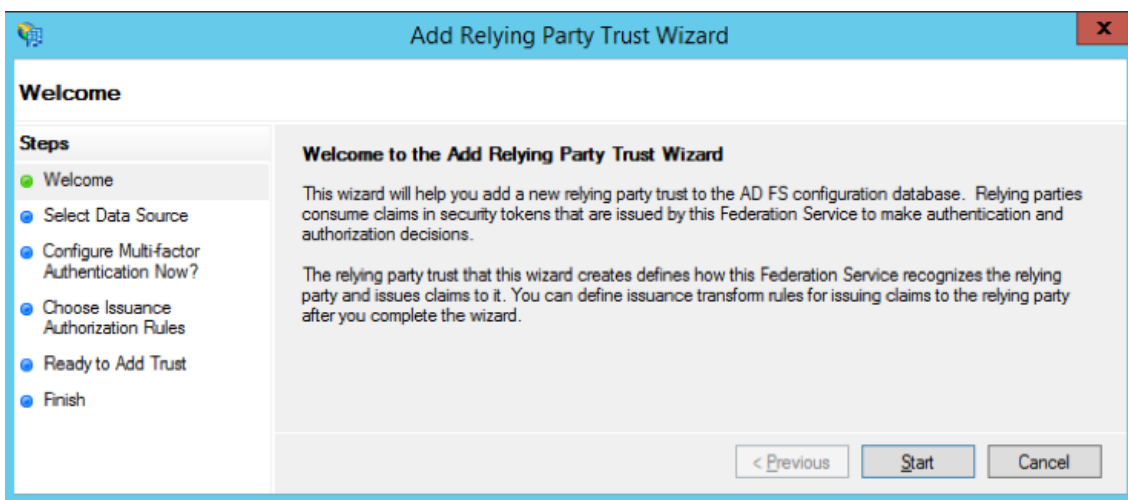
Create a Relying Party Trust in AD FS

To create a Relying Party Trust:

1. In the AD FS Management tool, navigate to Trust Relationships \ Relying Party Trusts.
2. Right-click Relying Party Trusts and select Add Relying Party Trust...



3. In the Add Relying Party Trust Wizard Welcome screen, click Start.



4. For Select Data Source, select Enter data about the relying party manually and click Next.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Select Data Source' step. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options:

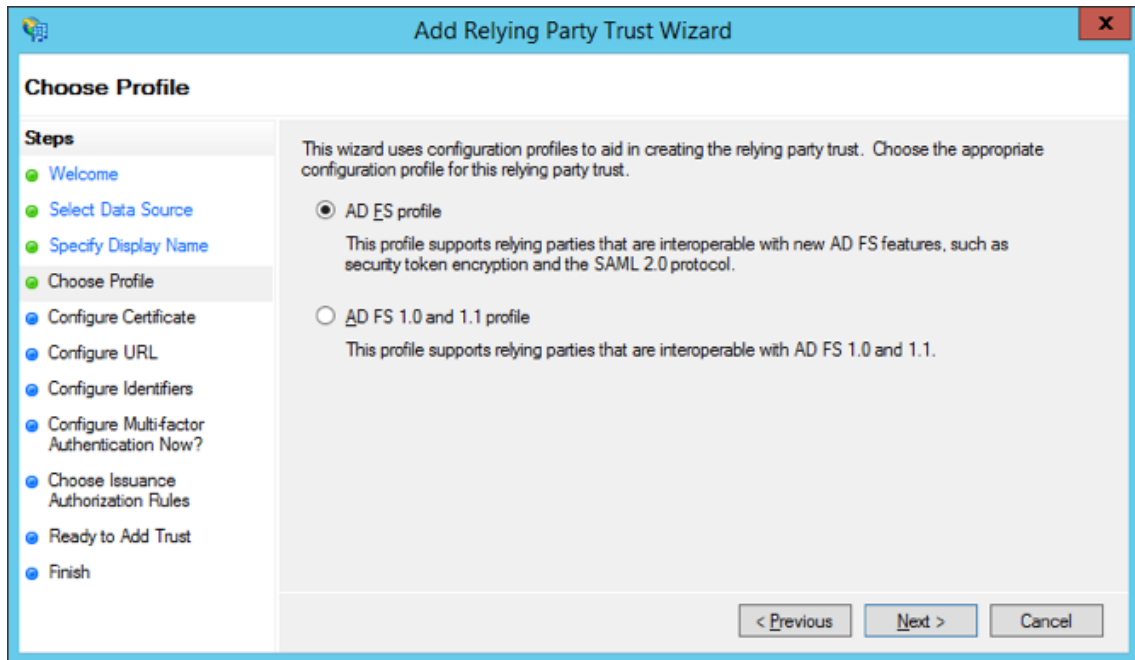
- Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Below this is a text box labeled 'Federation metadata address (host name or URL):' with an example: 'Example: fs.contoso.com or https://www.contoso.com/app'.
- Import data about the relying party from a file. Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Below this is a text box labeled 'Federation metadata file location:' and a 'Browse...' button.
- Enter data about the relying party manually. Use this option to manually input the necessary data about this relying party organization.

 At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

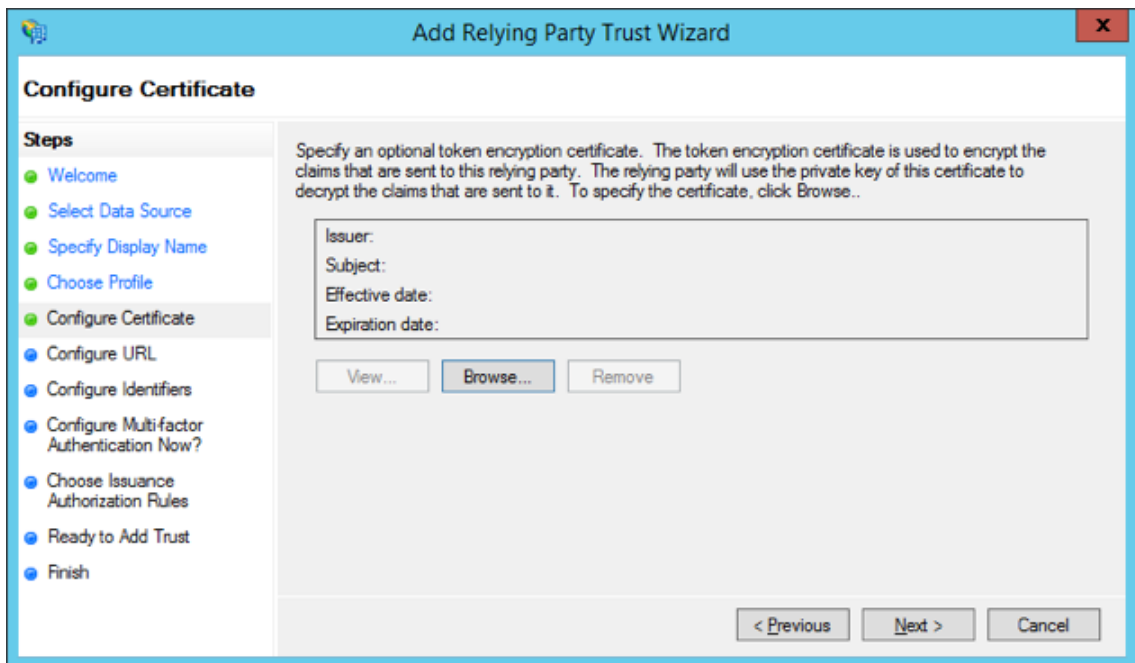
5. For Specify Display name, enter a name for the Trust (Colligo Engage is suggested) and click Next.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Specify Display Name' step. The title bar reads 'Add Relying Party Trust Wizard'. On the left, the 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction: 'Enter the display name and any optional notes for this relying party.'. There is a text box labeled 'Display name:' containing the text 'Colligo Engage'. Below it is a text area labeled 'Notes:'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

- For Choose Profile, select AD FS profile and click Next.



- For Configure Certificate, leave as is and click Next.



- For Configure URL, check Enable support for the WS-Federation Passive protocol, enter the URL: <https://colligoapp.onmicrosoft.com/colligoengage> and click Next.

Note: SAML is not supported.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure URL' step. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL (highlighted), Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.' There are two checkboxes: 'Enable support for the WS-Federation Passive protocol' (checked) and 'Enable support for the SAML 2.0 WebSSO protocol' (unchecked). Below the first checkbox, it says 'The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.' and provides a text input field for 'Relying party WS-Federation Passive protocol URL:' with the value 'https://colligoapp.onmicrosoft.com/colligoengage' and an example 'https://fs.contoso.com/adfs/ls/'. Below the second checkbox, it says 'The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.' and provides a text input field for 'Relying party SAML 2.0 SSO service URL:' which is empty, with an example 'https://www.contoso.com/adfs/ls/'. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

- For Configure Identifiers, leave as is and click Next.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure Identifiers' step. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers (highlighted), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.' There is a text input field for 'Relying party trust identifier:' which is empty, with an 'Add' button to its right. Below this, it provides an example: 'https://fs.contoso.com/adfs/services/trust'. There is a larger text area for 'Relying party trust identifiers:' containing the value 'https://colligoapp.onmicrosoft.com/colligoengage', with a 'Remove' button to its right. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

10. For Configure Multi-factor Authentication Now?, leave as is and click Next.

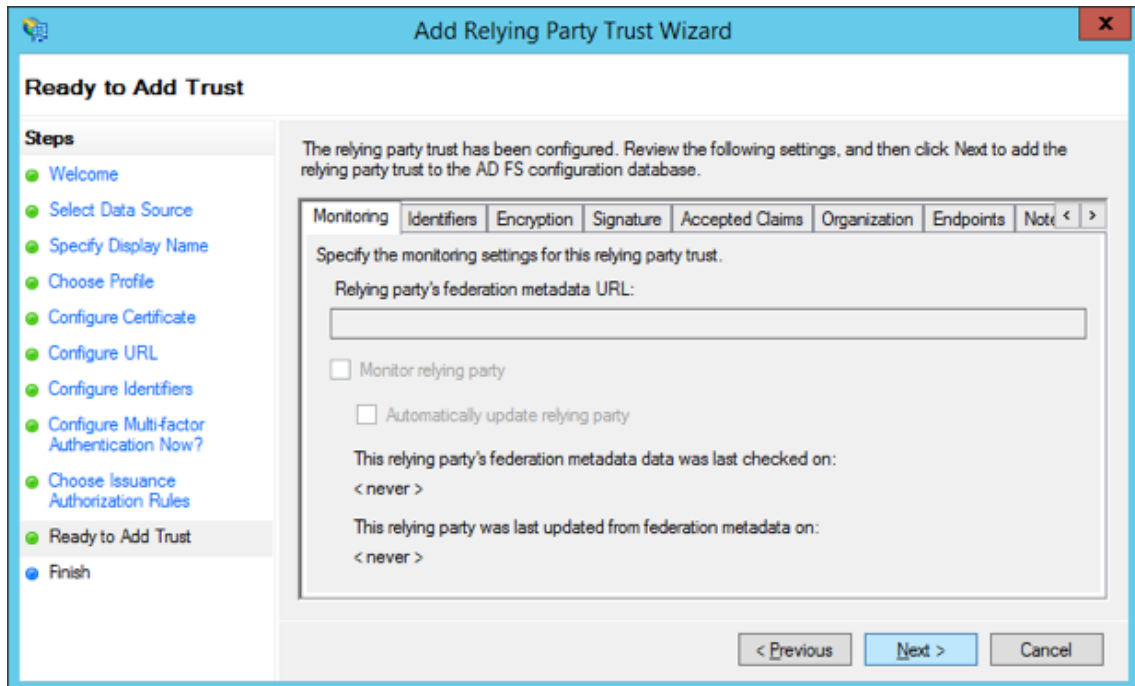
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, **Configure Multi-factor Authentication Now?** (highlighted), Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the following text: 'Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.' Below this is a table with two columns: 'Multi-factor Authentication' and 'Global Settings'. The table contains three rows: 'Requirements' with 'Users/Groups' and 'Not configured', 'Device' with 'Not configured', and 'Location' with 'Not configured'. Below the table are two radio button options: the first is selected and reads 'I do not want to configure multi-factor authentication settings for this relying party trust at this time.', and the second is unselected and reads 'Configure multi-factor authentication settings for this relying party trust.' At the bottom, there is explanatory text: 'You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).' and three buttons: '< Previous', 'Next >', and 'Cancel'.

Multi-factor Authentication	Global Settings
Requirements	Users/Groups
	Not configured
	Device
	Not configured
	Location
	Not configured

11. For Choose Issuance Authorization Rules, select the Permit option and click Next.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, **Choose Issuance Authorization Rules** (highlighted), Ready to Add Trust, and Finish. The main area contains the following text: 'Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.' Below this are two radio button options: the first is selected and reads 'Permit all users to access this relying party', with a sub-text: 'The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.'; the second is unselected and reads 'Deny all users access to this relying party', with a sub-text: 'The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.' At the bottom, there is explanatory text: 'You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.' and three buttons: '< Previous', 'Next >', and 'Cancel'.

12. For Ready to Add Trust, leave as is and click Next.



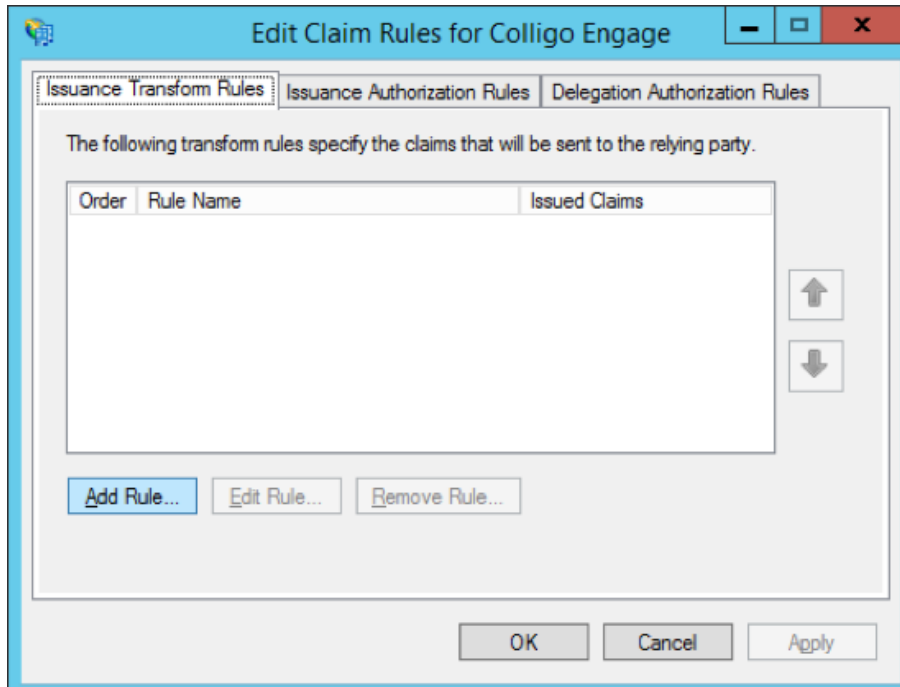
13. On the final step, check Open the Edit Claim Rules dialog... and click Close.



Add a Claim Rule

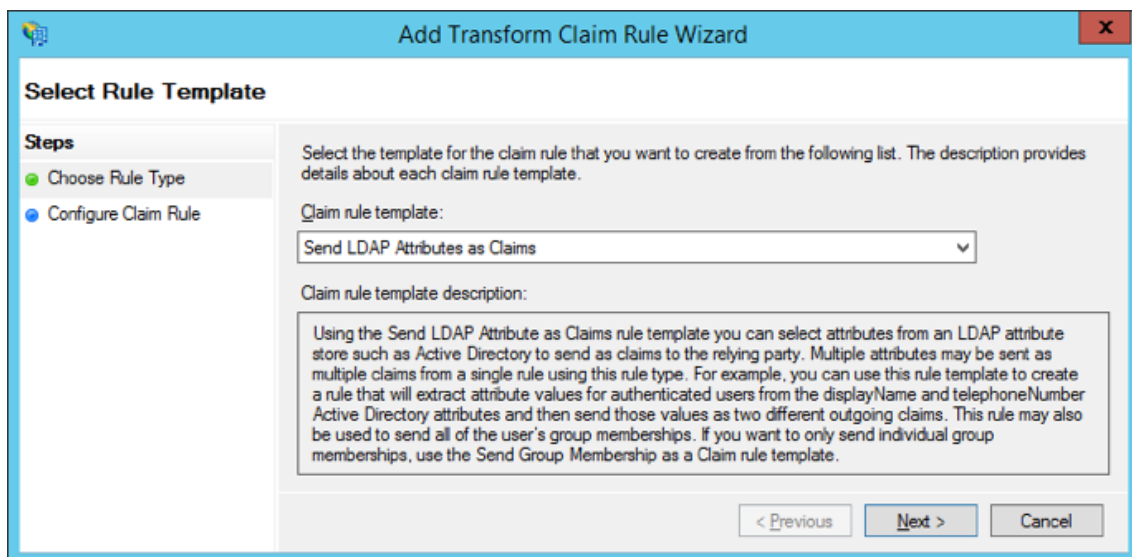
To support binding AD groups to Colligo Console Groups a claim rule is needed to have AD FS send users' group memberships via the users' claims. To add a claim rule:

1. In the Edit Claim Rules dialog for your relying party trust click **Add Rule...**



If this dialog is not open, open it by right-clicking on the configured Relying Party Trust and selecting **Edit Claim Rules...**

2. For **Choose Rule Type**, select **Send LDAP Attributes as Claims** from the Claim rule template drop-down and click **Next**.



- For **Configure Claim Rule**, select **Active Directory** from the **Attribute store** drop-down, configure the Claim as displayed in the image below, and click **Finish**.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: LDAP Claim Colligo Engage

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

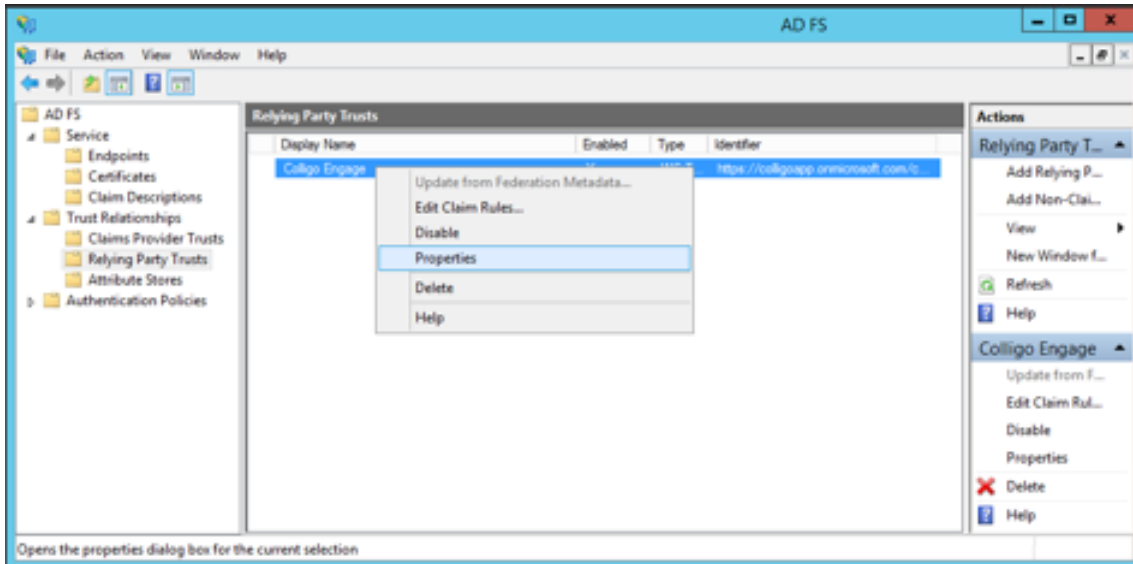
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	Name
	Given-Name	Given Name
	Surname	Surname
▶	Token-Groups - Unqualified Names	Group
*		

< Previous Finish Cancel

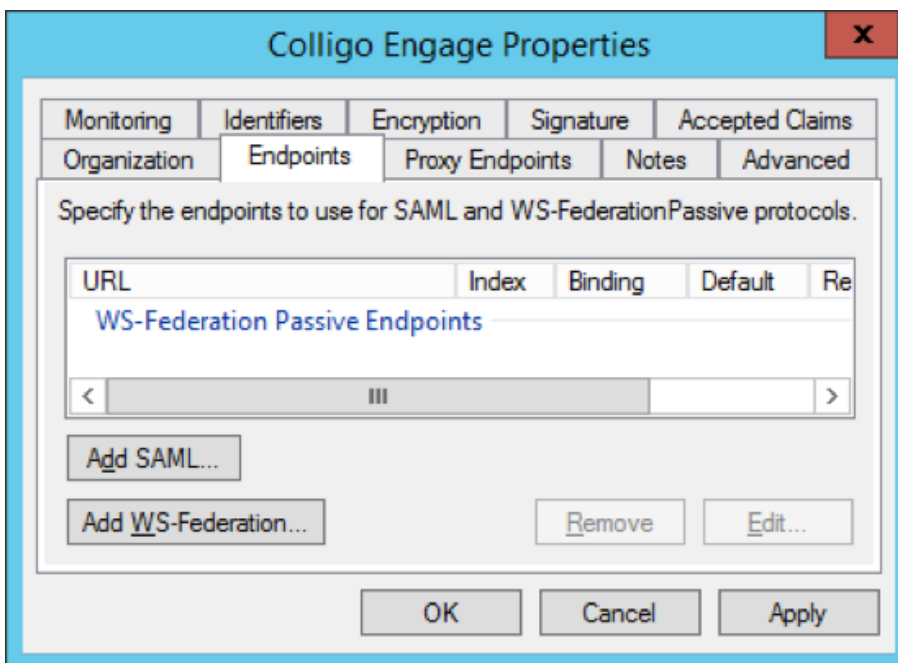
Add an Endpoint

An additional endpoint needs to be added to the Relying Party Trust that was setup for Colligo Engage. To do this:

1. Navigate to AD FS \ Trust Relationships \ Relying Party Trusts.
2. Right-click on the Colligo Engage entry and select Properties.



3. In the Properties dialog, select the Endpoints tab and then click Add WS-Federation...



- In the Edit Endpoint popup, enter <https://www.colligoapp.com/v1/session/external/wsfed> in the Trusted URL box and click OK.

Edit Endpoint

Endpoint type:
 WS-Federation

Set the trusted URL as default

Trusted URL:

Example: <https://sts.contoso.com/adfs/ls>

OK Cancel

- In the Properties dialog, click Apply and then OK.

Colligo Engage Properties

Monitoring Identifiers Encryption Signature Accepted Claims
 Organization Endpoints Proxy Endpoints Notes Advanced

Specify the endpoints to use for SAML and WS-Federation Passive protocols.

URL	Index	Binding	Default	Re
WS-Federation Passive Endpoints				
https://www.colligoapp.com/...		POST	No	

< ||| >

Add SAML... Add WS-Federation... Remove Edit...

OK Cancel Apply

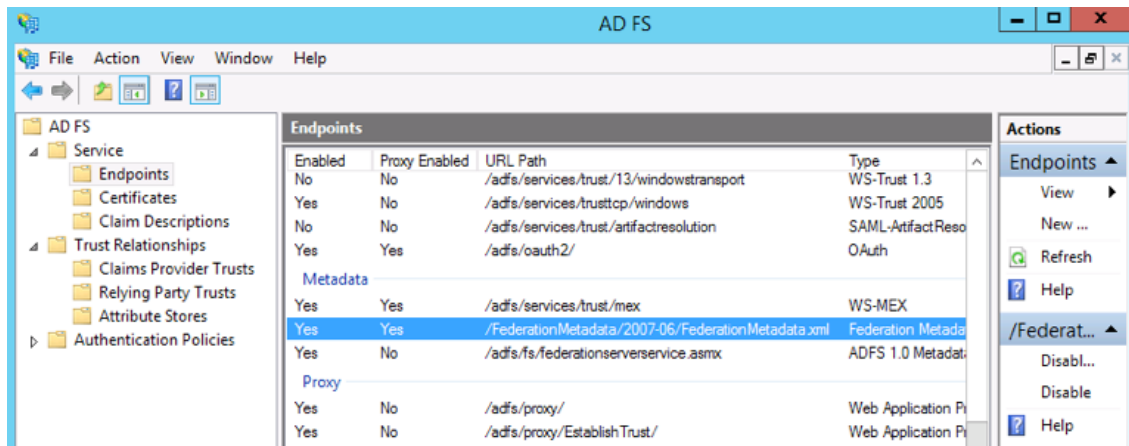
Collect Settings Information

entityID

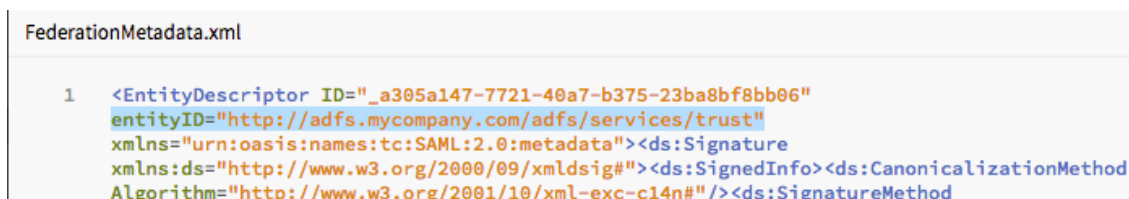
To retrieve the entityID:

1. In the AD FS Management tool, navigate to Service \ Endpoints.
2. In the **Metadata** section, locate the **Federation Metadata** type and make note of the URL Path. In the screenshot below, the URL Path is:

</FederationMetadata/2007-06/FederationMetadata.xml>



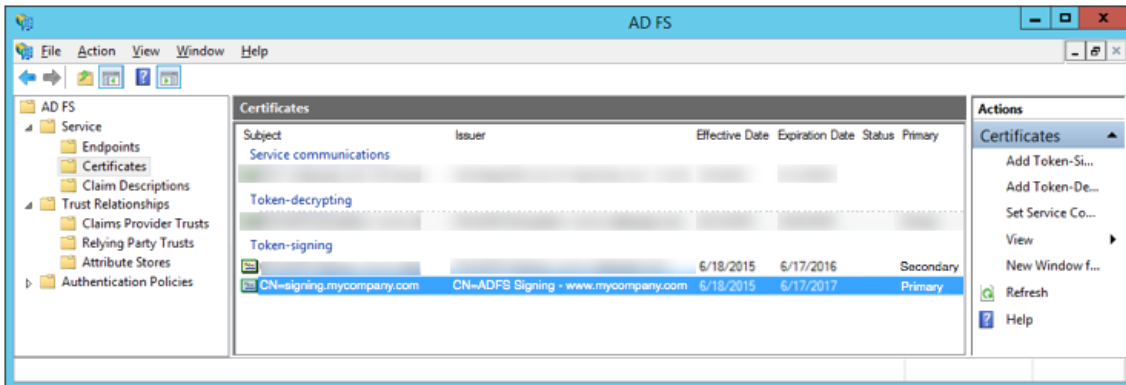
3. In your browser, load the URL https://<your_adfs_server>/<URL_path_from_above>. For example, the URL might be: <https://ads.mycompany.com/FederationMetadata/2007-06/FederationMetadata.xml>.
4. Open the XML file and locate the **entityID** entry at the start of the file and make note of the URL. In the screenshot below, the URL is: <http://ads.mycompany.com/ads/services/trust/>.



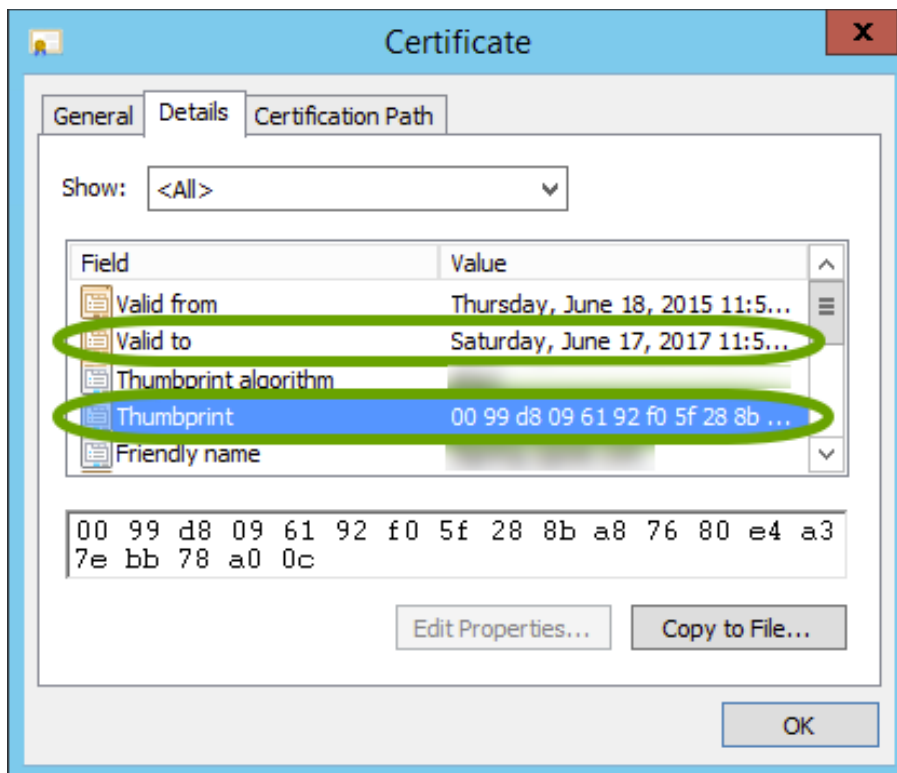
Primary Token signing certificate information

To retrieve the required Primary Token signing certificate information:

1. In the AD FS Management tool, navigate to **Service \ Certificates**.
2. In the **Token Issuance** section, open the **Primary Token** signing certificate by double-clicking the entry or by right-clicking the entry and choosing **View Certificate**.



3. In the **Certificate** popup, select **Details** tab and make note of the **Valid to** date and the **Thumbprint**, as highlighted in the image below.

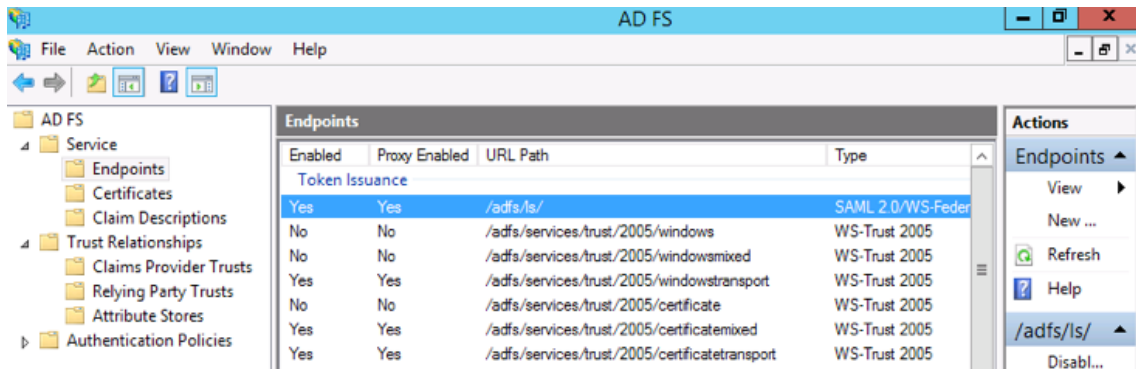


Note: When entering the **Thumbprint** in Colligo Console, it must be entered without spaces and with capitalized letters. For example, the thumbprint value for the certificate shown above is: **0099D8096192F05F288BA87680E4A37EBB78A00C**.

Authorization Endpoint

To retrieve the Authorization Endpoint:

1. In the AD FS Management tool, navigate to **Service \ Endpoints**.
2. In the **Token Issuance** section, locate the **SAML 2.0/WS-Federation** type and make note of the **URL Path**. In the screenshot below, the URL Path is [/adfs/ls/](#).



3. Create the **Authorization Endpoint** by appending this **URL Path** with the URL for your AD FS server. For example, the URL might be: <https://adfs.mycompany.com/adfs/ls/>.

Configure AD FS in Colligo Console

Add a non-domain Administrator

If AD FS is configured incorrectly, **all users**, including administrators will be unable to log in.

Prior to configuring AD FS in Colligo Console it is recommended that you add an administrator with an email address that does not belong to the domain(s) you will be specifying on the **Configure ADFS** tab (step 6). For example, if you are configuring the domain **mycompany.com**, you could add an administrator with the email myname@personalemail.com. For details on how to add this user, refer to the [Users](#) section.

If information is accidentally entered incorrectly on the **Configure ADFS** tab (step 6), this non-domain administrator will still be able to log in to Colligo Console.

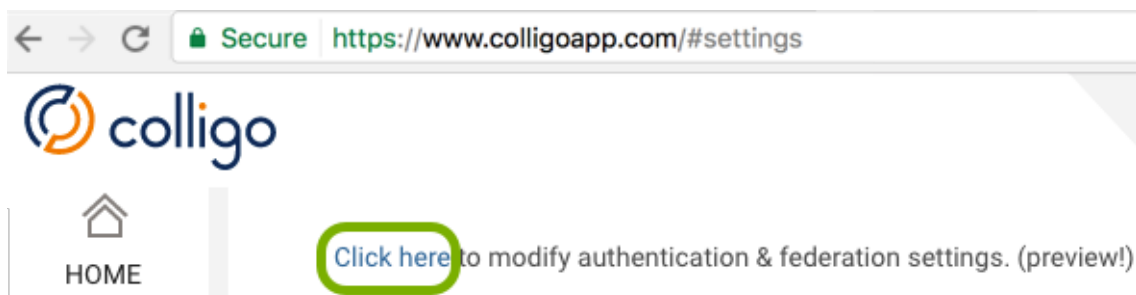
Configure AD FS in Colligo Console

To configure AD FS in Colligo Console:

1. Log in to Colligo Console using an **Organization Administrator** account.
2. In the left navigation column, click **Settings**.



3. At the top of the page, click the link to modify authentication & federation settings.



- On the Federated Tenants page, click Add.

Federated Tenants

- Tenants

Search
Sort
Add

Name	Email Domain(s)	Tenant ID	Custom Auth Url/Endpoint (if applicable)
------	-----------------	-----------	--

- In the Add Federated Tenant page, select the Configure ADFS tab.
- Enter values as suggested in the screenshot, then click Configure ADFS.

Azure AD
Configure ADFS

Used to identify the tenant within Colligo Console. Can be any relevant text.

Tenant Name
My Organization

Auth type
wsfed

Note: After you click the **Configure ADFS** button, the URL will be appended with **/idpinitiatedsignon**.

Authorization Endpoint
https://adfs.mycompany.com/adfs/ls

Entity ID
https://adfs.mycompany.com/adfs/services/trust

Token-signing Certificate Thumbprint (no spaces)
561593C0DC2C74C85B5BA4B16625531B5CE42A56

Token-signing Certificate Expiry Date
04/20/2016

The domain of your organization. **Note:** mycompany.com is listed for users with email addresses such as first.last@mycompany.com

Email Address Domains (one per line)
mycompany.com

Configure ADFS

Figure 27: Adding a Federated Tenant: AD FS

Federation is now complete and you will be taken back to the list of Federated Tenants. Users should now be able to log into Colligo apps using their email address and domain password.

Federated Tenants

Name	Email Domain(s)	Tenant ID	Custom Auth Uri/Endpoint (if applicable)
MyOrg	mycompany.com	http://adfs.mycompany.com/adfs/services/trust	http://adfs.mycompany.com/adfs/ls/idpinitiatedsignon

Figure 28: Federated Tenants after configuring ADFS

Removing Access

If you ever wish to completely disallow access to your active directory, delete the tenant in Colligo Console and remove the Colligo Engage Relying Party Trust from your AD FS Management Tool.

To delete the tenant in Colligo Console:

1. Log in to Colligo Console using an **Organization Administrator** account.
2. In the left navigation column, click **Settings**.
3. At the top of the page, click the link to modify authentication & federation settings.
4. On the **Federated Tenants** page (see Figure 28), click the entry for your tenant.
5. On the **Edit Federated Tenant** page, click **Delete Tenant**.

To remove the Colligo Engage Relying Party Trust:

1. Navigate to **AD FS \ Trust Relationships \ Relying Party Trusts**.
2. Right-click on the **Colligo Engage** entry and select **Delete**.

Troubleshooting

In step 6 of the [Configure AD FS in Colligo Console](#) section you are asked to provide the expiry date for the Token-signing Certificate. If users see the error message below when logging in, it is likely that the certificate has expired and you will need to contact Colligo Support for assistance.

We could not validate your supplied credentials. Please contact your Organization Administrator. WIF10201: No valid key mapping found for securityToken: 'System.IdentityModel.Tokens.SamlSecurityToken' and issuer: 'http://[redacted]/adfs/services/trust'.

Figure 29: Error message when the Token-signing Certificate has expired

Azure AD Federation

Configure Azure AD in Colligo Console

Add a non-domain Administrator

If Azure AD is configured incorrectly, **all users**, including administrators will be unable to log in.

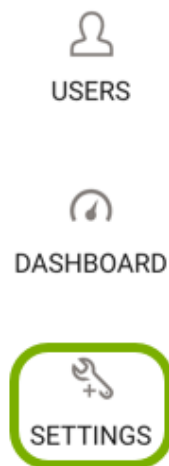
Prior to configuring Azure AD in Colligo Console it is recommended that you add an administrator with an email address that does not belong to the domain(s) you will be specifying on the **Azure AD** tab (step 6). For example, if you are configuring the domain **mycompany.com**, you could add an administrator with the email myname@personalemail.com. For details on how to add this user, refer to the [Users](#) section.

If information is accidentally entered incorrectly on the **Azure AD** tab (step 6), this non-domain administrator will still be able to log in to Colligo Console.

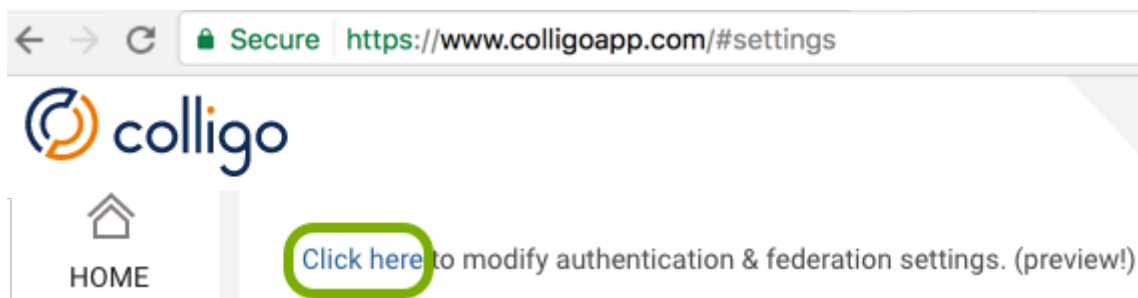
Federate Azure AD with Colligo

To federate Azure AD with Colligo Console:

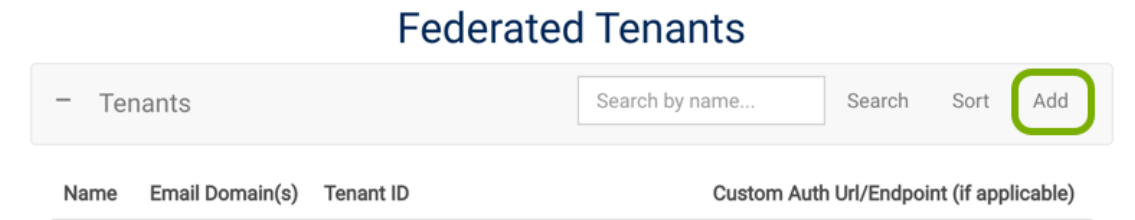
1. Log in to Colligo Console using an **Organization Administrator** account.
2. In the left navigation column, click **Settings**.



3. At the top of the page, click the link to modify authentication & federation settings.



- On the Federated Tenants page, click Add.



- In the Add Federated Tenant page, select the Azure AD tab.
- Enter values as suggested in the screenshot, then click Federate Azure AD with Colligo.

Figure 30: Adding a Federated Tenant: Azure AD

- You will be directed to Microsoft Azure to grant access to your active directory. You may be prompted to authenticate if you haven't already.
Note: To grant access to your active directory, your Azure user must have administrator rights in your active directory.
- In the prompt to grant access to your active directory, click the appropriate option (**Accept** [oauth] or **grant access** [wsfed]). The prompt you see will depend on the authentication type chosen in step 6.

Federation is now complete and you will be taken back to the list of Federated Tenants. Users should now be able to log into Colligo apps using their email address and domain password.

Federated Tenants

Name	Email Domain(s)	Tenant ID	Custom Auth Url/Endpoint (if applicable)
MyOrg	myorg.com	6949ca7f-4642-3a7f-b78f-cbdfef6cbd3a7	

Figure 31: Federated Tenants after Federating Azure AD

Viewing the Colligo Azure AD App in the Azure Management Portal

The Colligo Engage Azure AD App should now be present in your Applications list in your Active Directory within the management portal, as shown below.

The screenshot shows the Azure Management Portal interface. The top navigation bar includes 'Microsoft Azure', 'Check out the new portal', 'Subscriptions', and a user profile icon. The left sidebar shows the 'Colligo' application icon. The main content area displays the 'colligo' application details, with tabs for 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. The 'APPLICATIONS' tab is active, showing a list of applications. The 'Colligo Engage' application is highlighted with a green oval, indicating it is the selected item. The application details show the name 'Colligo Engage', publisher 'Colligo Engage', type 'Web application', and app URL 'https://www.colligoapp.com'. The 'MANAGE ACCESS' button at the bottom is also highlighted with a green oval.

NAME	PUBLISHER	TYPE	APP URL
Colligo Engage	Colligo Engage	Web application	https://www.colligoapp.com
Microsoft Azure Subscription Management		Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/

Figure 32: Azure Management Portal

If you view the **details** of the newly added Colligo Engage app, you will see an option in the **Configure** tab entitled **User Assignment Required to Access App**. If you wish to restrict user access to any Colligo product, including Colligo Console in the browser, simply select **Yes** and choose only users you would like to utilize Colligo products.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is enabled in the Azure Management Portal by the Azure administrator for the organization. Once enabled, users secure their account by configuring one of the provided MFA options. MFA will take place the next time the user logs in to Colligo Console.

Removing Access

If you ever wish to completely disallow access to your active directory, click the **Manage Access** button at the bottom of the page (see previous figure), and click **Remove Access**. Once this has been done, Colligo will no longer have access. You should also delete the tenant in Colligo Console.

To delete the tenant in Colligo Console:

1. Log in to Colligo Console using an **Organization Administrator** account.
2. In the left navigation column, click **Settings**.
3. At the top of the page, click the link to modify authentication & federation settings.
4. On the **Federated Tenants** page (see Figure 33), click the entry for your tenant.
5. On the **Edit Federated Tenant** page, click **Delete Tenant**.

Troubleshooting

If you federate with an Azure ID that does not have administrator rights in your active directory, you will receive a failure message. The message you see will depend on the authentication type chosen.

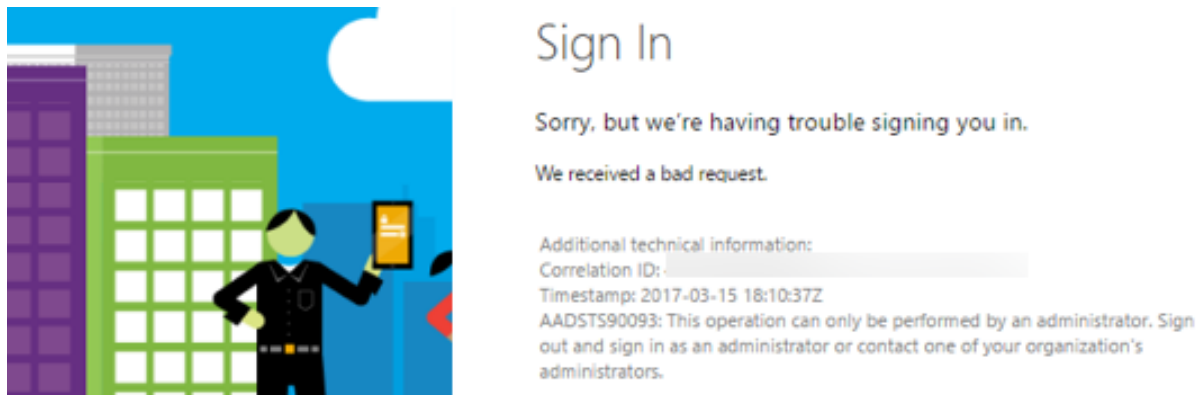


Figure 33: Troubleshooting Granting Access in Azure AD when oauth is chosen

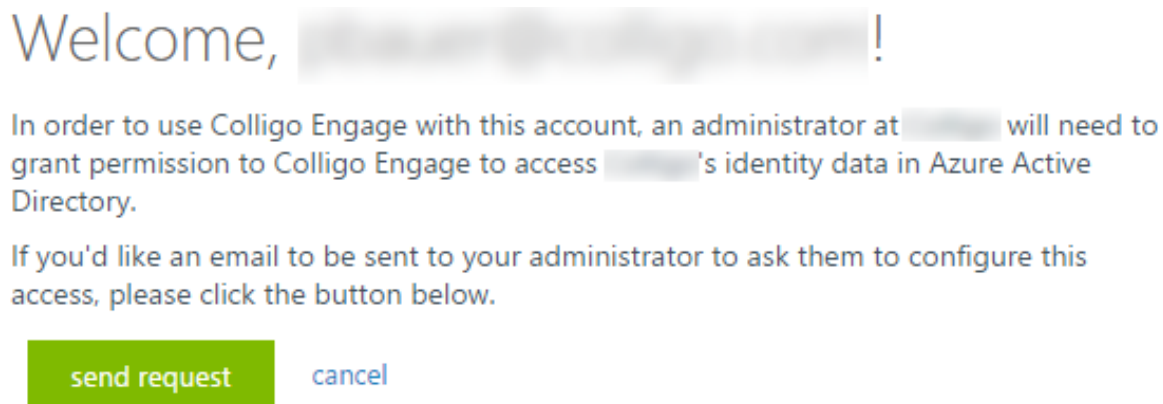


Figure 34: Troubleshooting Granting Access in Azure AD when wsfed is chosen

Binding AD Groups to Colligo Console Groups

A Tenant-Group binding is required to bind an Active Directory Group to a Colligo Console group. For example, you might bind the Colligo Console group “Sales” with the AD group “Sales”. To create a Tenant-Group binding:

1. Open the Group Properties page of the Colligo Console group and click **Configure Tenant Bindings** to display a list of **Tenant-Group Bindings**.

Tenant-Group Bindings

External Ref Id

Tenant Name

2. Click **Add Tenant-Group Binding** and provide the **External Reference ID**.
 - For AD FS, this is the name of the AD group.
 - For Azure AD, this is the object ID of the group. It is obtained from the Azure Management Portal by navigating to **Active Directory \ <Directory> \ Groups \ <Group>**.

3. Select your **Tenant** from the drop-down menu and then click **Add**.

The Tenant-Group binding will now appear in the tabular view.

Note: If you are using AD FS, these instructions assume you are sending users' group memberships via the users claims, as configured in the section [Add a claim rule](#).

Configuring Single Sign-On (SSO)

To configure SSO for Colligo Console:

1. Federate your organization in Colligo Console.
2. Configure client browsers to support SSO.

Note: An additional step is required to use browsers such as Edge or Chrome, as the default behavior when AD FS 3.0 is deployed is that only Internet Explorer works for SSO.

Federate your organization in Colligo Console

To ensure your organization can be federated in Colligo Console, refer to the [Requirements](#) section.

For details on how to federate your organization in Colligo Console, refer to the [Federation](#) section.

When complete, clear the browser cache and validate the federation by:

1. Navigating to www.colligoapp.com.
2. Entering your email address.
3. Entering your password at the SSO prompt.

Federation has been successfully configured if you end up on the Colligo Console home page as depicted in Figure 1 (page 9).

Configure client browsers to support SSO

To enable single sign-on on a Windows computer, the tasks listed below must be performed on each client computer. Note that some of these settings may already be set as described.

- Add your access URL to the list of approved sites for single sign-on.
- Enable active scripting (JavaScript) and automatic logon.
- Enable integrated authentication.

For details on performing these tasks, refer to the section [How to Configure Client Browsers to Support SSO](#).

When complete, clear the browser cache and validate the SSO configuration by navigating to www.colligoapp.com and entering your email address.

SSO has been successfully configured if you next see the Colligo Console home page as depicted in Figure 1 (page 9) without having ever entered your password into the browser.

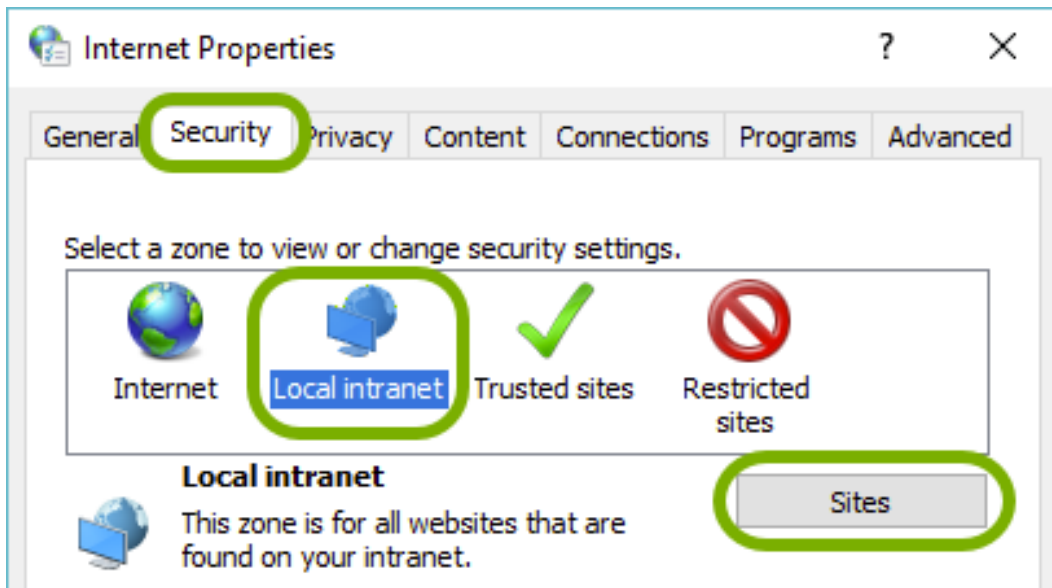
Configure AD FS to enable SSO for Edge and Chrome

For details on enabling additional browsers, refer to the section [How to configure AD FS to enable SSO for Edge and Chrome](#).

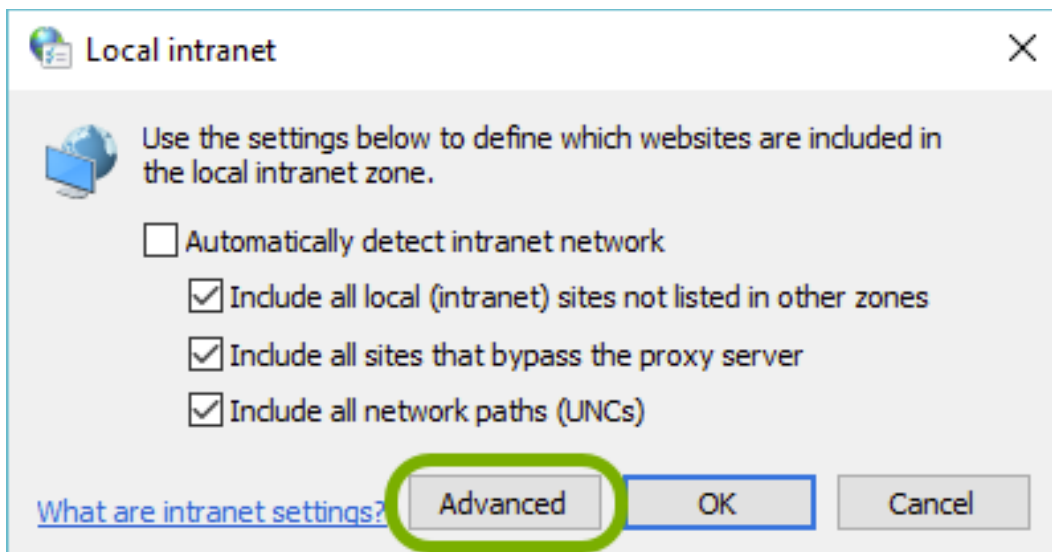
How to Configure Client Browsers to Support SSO

To enable single sign-on on a Windows computer, perform the steps below on each client computer. Note that some of these settings may already be set correctly.

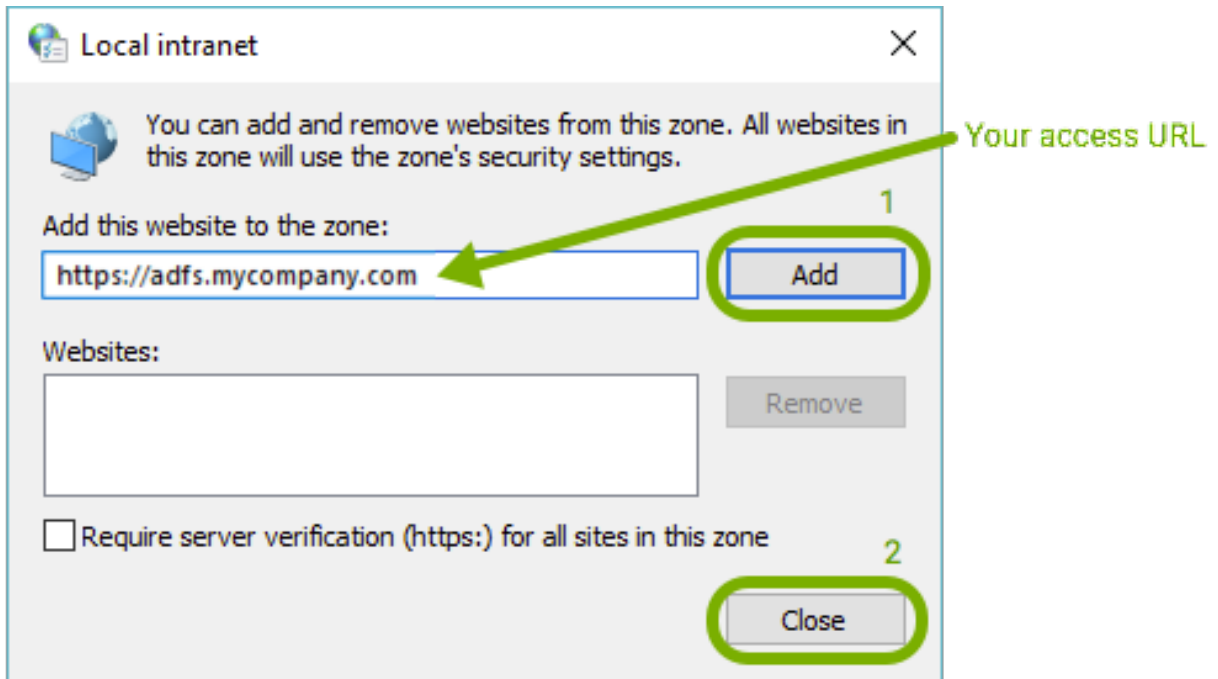
1. Open the **Internet Properties** dialog box. One way to do this is to search for **Internet Options**.
2. Select the **Security** tab.
3. Select **Local intranet** and choose **Sites**.



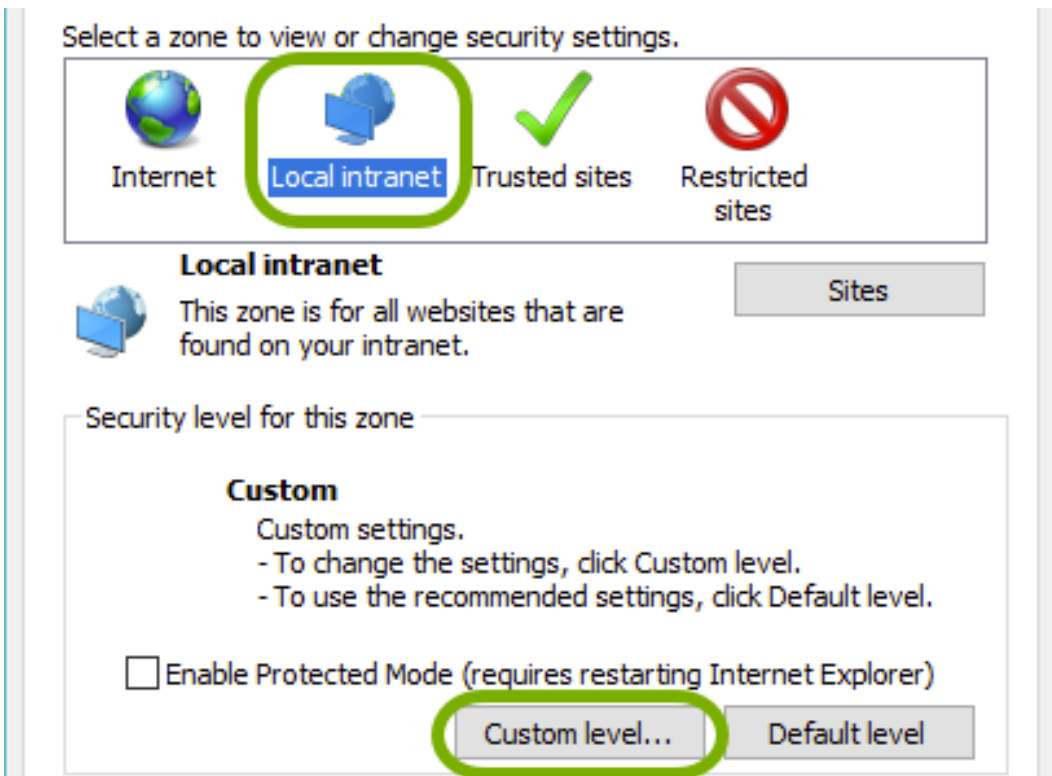
4. In the **Local intranet** dialog box, choose **Advanced**.



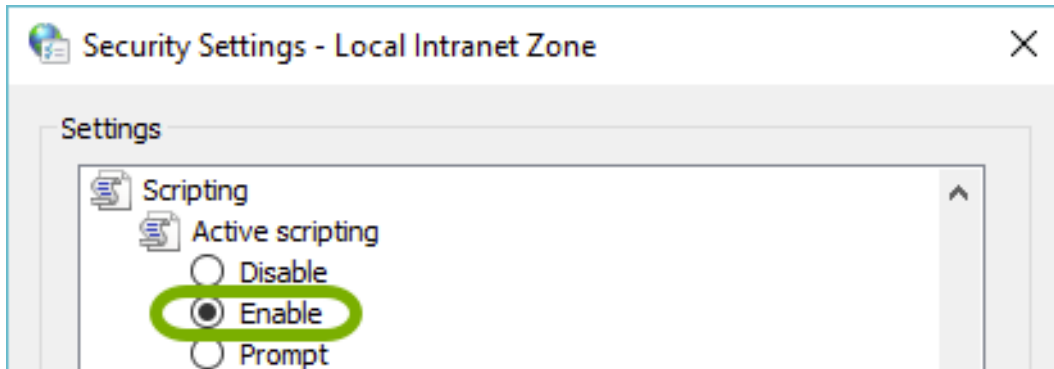
5. Add your access URL to the list of websites and choose Close.



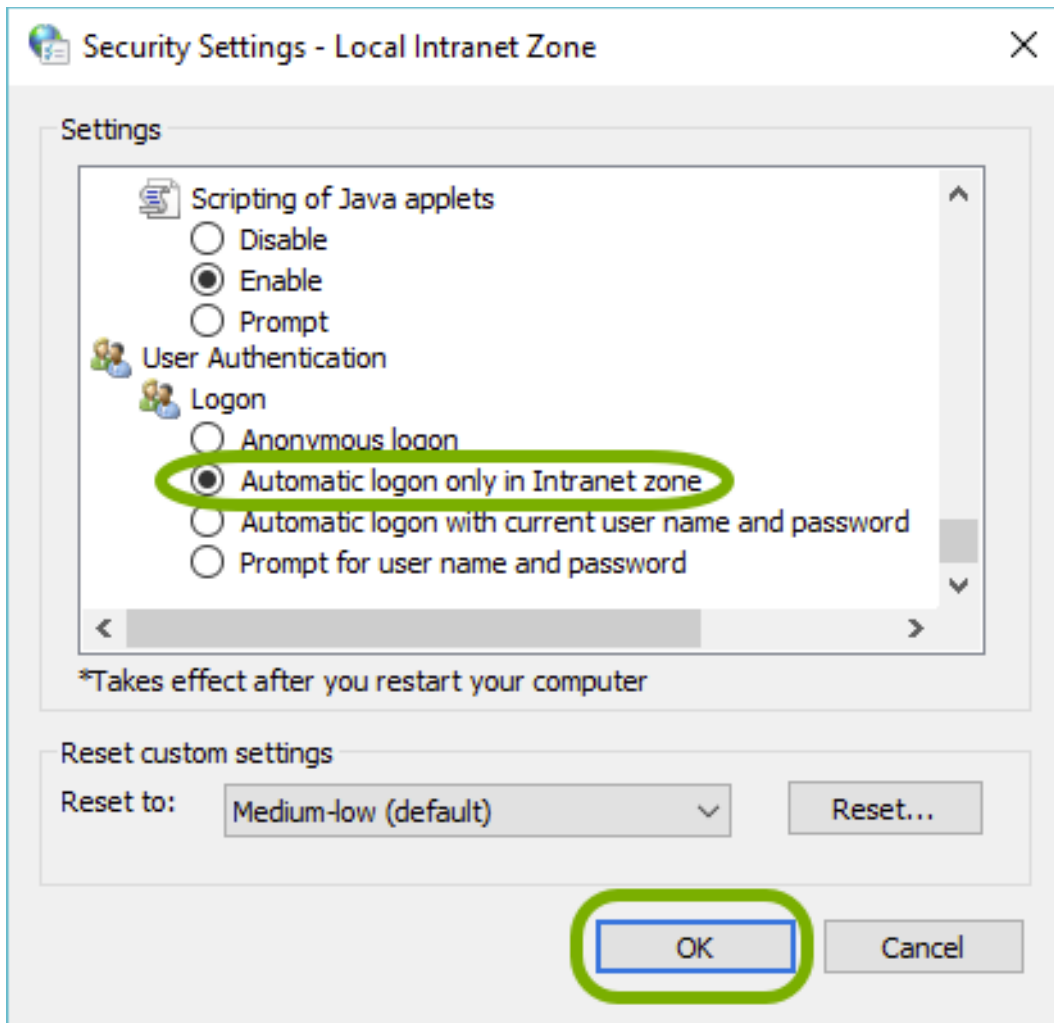
6. In the Local intranet dialog box (pictured in step 4), choose OK.
7. In the section Security level for this zone choose Custom level...



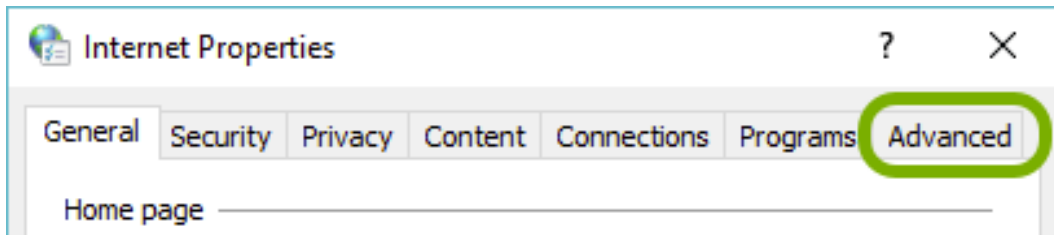
- In the Security Settings - Local Intranet Zone dialog box, scroll down to Scripting and select Enable under Active scripting.



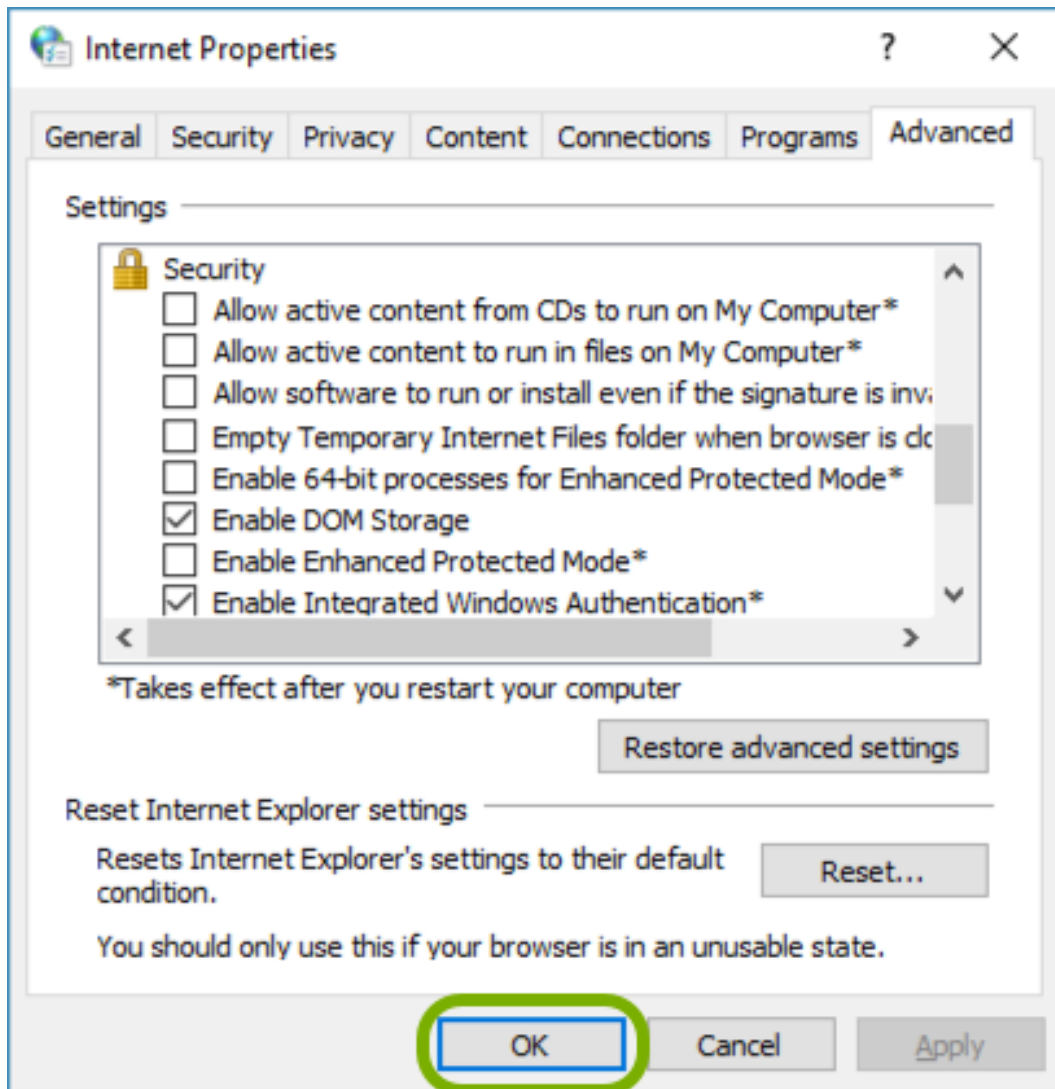
- In the Security Settings - Local Intranet Zone dialog box, scroll down to User Authentication and select Automatic logon only in Intranet zone under Logon. Next click OK.



10. Select the Advanced tab.



11. Scroll down to Security and select Enable Integrated Windows Authentication. Next click OK.



12. Close any open browsers to have these changes take effect.

Note: The above can also be done by using Group Policies. Refer to this article for details:
http://docs.aws.amazon.com/directoryservice/latest/admin-guide/ie_sso.html

How to configure AD FS to enable SSO for Edge and Chrome

When AD FS 3.0 is deployed, the default behavior is that only Internet Explorer works for SSO. The steps below will add Chrome and Edge to the AD FS configuration.

1. Stop the **Active Directory Federated Services** service on all AD FS servers. An easy way to do this is to open an elevated PowerShell window and run the command:

```
net stop adfssrv
```

2. Confirm that the browser headers are not present with the command:

```
Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents
```

This command will display a list of all supported browser user agents.

```
PS C:\Windows\system32> Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents
MSAuthHost/1.0/In-Domain
MSIE 6.0
MSIE 7.0
MSIE 8.0
MSIE 9.0
MSIE 10.0
Trident/7.0
MSIPC
Windows Rights Management Client
```

In this example, Edge and Mozilla 5.0 are not present.

3. Issue the following command to add the Edge and Mozilla 5.0 (Chrome) user agents:

```
Set-AdfsProperties -WIASupportedUserAgents @("MSAuthHost/1.0/In-Domain", "MSIE 6.0", "MSIE 7.0", "MSIE 8.0", "MSIE 9.0", "MSIE 10.0", "Trident/7.0", "MSIPC", "Windows Rights Management Client", "Mozilla/5.0", "Edge/12")
```

Note: this command requires all user agents (existing and new) to be passed in.

4. Confirm the new ones were added by running the **Get-ADFSProperties** command again:

```
PS C:\Windows\system32> Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents
MSAuthHost/1.0/In-Domain
MSIE 6.0
MSIE 7.0
MSIE 8.0
MSIE 9.0
MSIE 10.0
Trident/7.0
MSIPC
Windows Rights Management Client
Edge/12
Mozilla/5.0
```

5. Start up the AD FS Services on all AD FS servers:

```
net start adfssrv
```