Axcient

CloudFinder for Microsoft 365

NOTICE

Table of Contents

Chapter 1: Introduction

CloudFinder for Microsoft 365 provides peace-of-mind by ensuring that the data used in your organization's instance of Microsoft 365 is backed up, recoverable, and protected. CloudFinder backs up Microsoft 365 emails, contacts, calendars, and documents. When you deploy CloudFinder, your critical Microsoft 365 data is backed up to our encrypted, tamper-proof Axcient Cloud. The Axcient Cloud gives you absolute protection against accidental or malicious data loss. With multiple redundant Axcient Cloud storage and best-in-class encryption, you can rely on 99.999% durability and 99.999% availability.

After data is backed up, CloudFinder administrators can instantly search Microsoft 365 data with rich filtering and quickly select data to restore. In addition, detailed dashboards, reports, and monitoring of all backup activities visually indicate how CloudFinder is working to protect your Microsoft 365 data.

Supported Services

All Microsoft 365 Business Plans plans are supported by CloudFinder for Microsoft 365, including:

- Microsoft 365 Business Basic (formerly Microsoft 365 Business Essentials)
- Microsoft 365 Business Standard (formerly Microsoft 365 Business Premium)
- Microsoft 365 Business Premium (formerly Microsoft 365 Business)
- Microsoft 365 Apps (formerly Microsoft 365 Business and Microsoft 365 ProPlus)
- Enterprise E1, E3, E4, E5

CloudFinder for Microsoft 365 currently backs up these service connectors:

- Mail
- Contact
- Calendar
- OneDrive
- SharePoint (Document Libraries)

CloudFinder for Microsoft 365 does *not* currently support:

- Exchange Online Archiving (In-Place Archive)
- Environments connected to a physical environment

Supported Browsers

You can use the latest versions of the following browsers to access CloudFinder:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Safari

Security

Axcient holds our partners' data in highest regard. We maintain data integrity and protect partner data through methods that avoid compromise. Our data policies meet the requirements of GDPR (General Data Protection Regulation).

CloudFinder uses military-grade encryption when transporting data over Secure Sockets Layer (SSL) encrypted connections. From the SSL encrypted connections, it routes to an HTTPS stand-alone processes running behind a firewall. Our Server-Side Encryption (SSE) uses at minimum 128-bit SSL (128-bit) in transit and 256-bit Advanced Encryption Standard (256-bit AES) at rest. Stored data is only accessed by Microsoft 365 applications from behind a firewall.

CloudFinder is HIPAA Compliant. Please reference the **Axcient HIPAA Whitepaper** for details and requirements.

Terminology

Many key words used in this guide refer to industry terminology. For example:

Service:	A *service* refers to the SaaS platform supported by CloudFinder. For example: • MS Microsoft 365
Service Instance:	A *service instance* refers to a specific occurrence of a service. Each instance displays its own unique domain name. For example: • cloudfinder.onmicrosoft.com • cloudfinder.ems.com
Connector:	A *service connector* refers to the type of service. For example: • Microsoft 365 Mail

	- Microsoft 365 Contact - Microsoft 365 Calendar - Microsoft 365 SharePoint
Backup Objects:	A backup object refers to the content type that is backed up, including: - Document - Email - Event - Contact Please note that nested folders need to be restored individually. Metadata and permissions are backed up but not restored.

Partner Support

As a partner, you can access the service and product support you need to ensure you and their clients stay productive, safe, and up-and-running.

For response times and service levels, please check our **Support SLA** and our **Cloud Services SLA**.

For immediate assistance, **open a ticket** or search our **Knowledgebase**.

Chapter 2: Configuring CloudFinder

Configuring CloudFinder is a quick and streamlined process, allowing you to begin protecting client data after just a few simple steps.

As part of this setup process, you will complete the following steps:

- Sign up for a CloudFinder reseller account.
- Log in to your CloudFinder reseller account.
- Create a new CloudFinder client account.
- Create an administrator user for each CloudFinder client account.
- Add one or more service instances to a client account.
- Define end user data to be backed up.
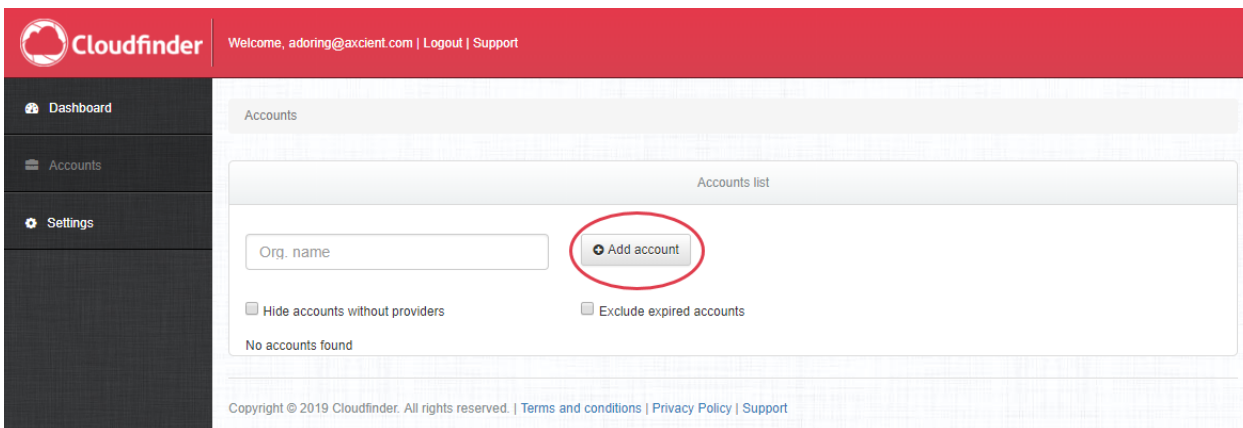
Signing Up for a CloudFinder Reseller Account

As a first step, you need to create a CloudFinder reseller account. For example, you can sign up for a CloudFinder trial account, which will trigger the CloudFinder reseller account creation process.

Note: Trial accounts are valid for 30 days. You must upgrade a trial account before the 30 day trial period ends to ensure your services are not interrupted. Please contact your Partner Enablement Specialist or Partner Success Manager for help.

To sign up for a CloudFinder trial:

STEP 1: Navigate to the CloudFinder Site

From your preferred browser, navigate to the **CloudFinder web site** and click the **Sign Up** button. The Axcient *Contact Us* form displays.

STEP 2: Sign Up for a CloudFinder Account

In the *Contact Us* form, enter your contact information and click the **Submit** button. An Axcient representative will contact you and provide you with a username and password to access CloudFinder.

Please note that trial accounts are valid for 30 days. You must upgrade a trial account before the 30 day trial period ends to ensure your services are not interrupted. Please contact your Partner Enablement Specialist or Partner Success Manager for help.

Logging In To Your CloudFinder Reseller Account

When you have a CloudFinder reseller account, you can log in and create new client accounts.

To log in to your CloudFinder reseller account:

STEP 1: Navigate to Your CloudFinder Reseller Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter your CloudFinder reseller account credentials and click the **Login** button.
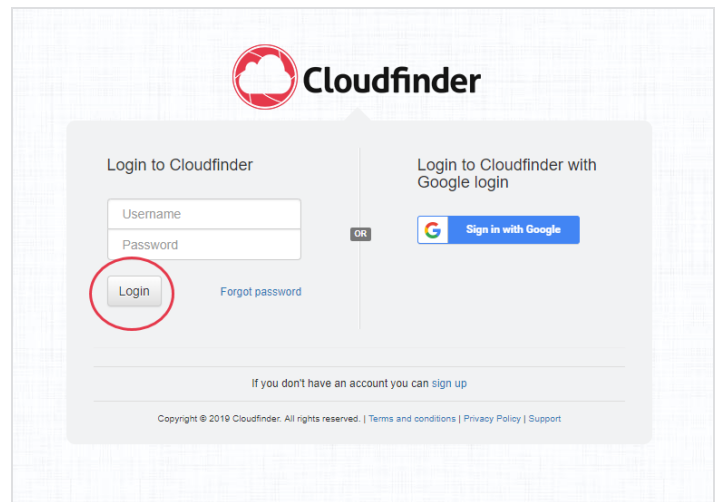
STEP 2: Manage Settings

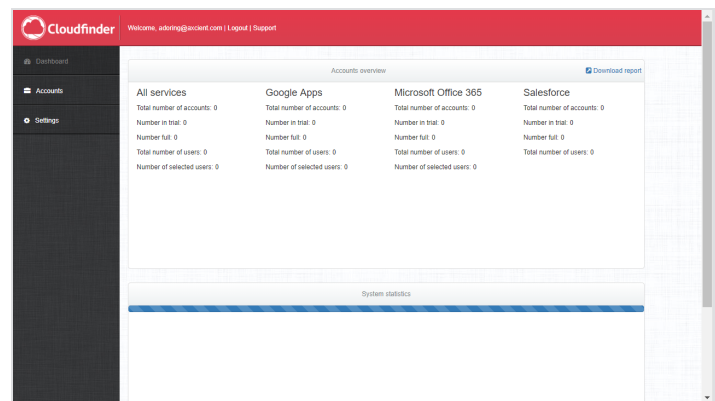In the *CloudFinder Dashboard* page, you can begin to create new client accounts.

Creating New Client Accounts

When you have access to your CloudFinder reseller account, you can begin to create a new client account for each client that you support.

To create new client accounts:

STEP 1: Navigate to the Accounts Tab

From your CloudFinder reseller account, click the **Accounts** tab in the left-hand navigation menu. The *Accounts* page displays, showing all active client accounts.
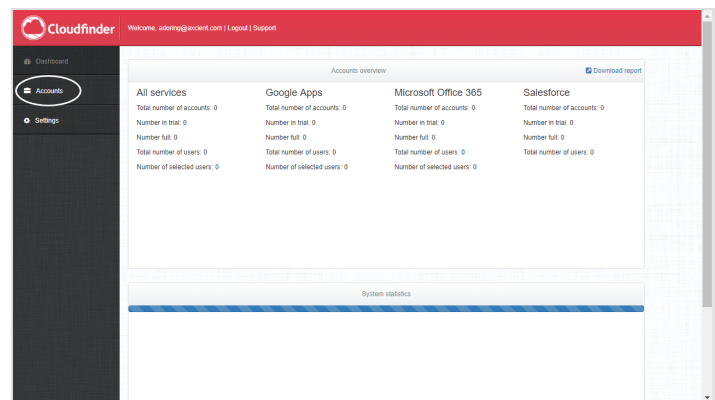
STEP 2: Add an Account

In the *Accounts* page, click the **Add Account** button. The *Create New Account* pop-up window displays.
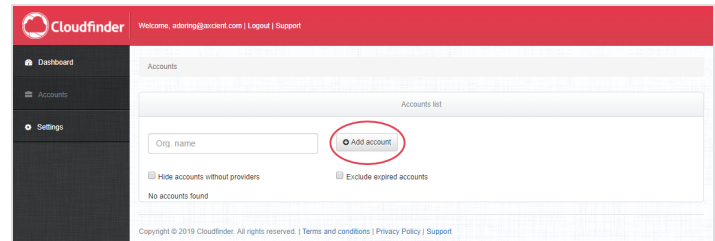
STEP 3: Define Settings

In the *Create New Account* pop-up window, enter account details:

- In the *Account Name* field, enter the **name** of the new client account.
- In the *Employees* drop-down field, select the **employee count range** for the new client account. This information *does not* affect how many users you can

select for backups.

- Optionally, click the **Is this an NFR account** checkbox if you plan to use this account for NFR purposes. If you set this account as an NFR account, it will be limited to 25 users.

Click the **Continue** button to save your changes.

Creating New Administrator Users

After you create a CloudFinder client account, you can create one or more administrator users that will log in and manage the CloudFinder client account. CloudFinder administrators perform critical administrative tasks for the client account, including selecting users for backup, running reports, restoring data when necessary, and more.

To create new administrator users for a client account:

STEP 1: Navigate to the Accounts Tab

From your CloudFinder reseller account, click the **Accounts** tab in the left-hand navigation menu. The *Accounts* page displays, showing all active client accounts.
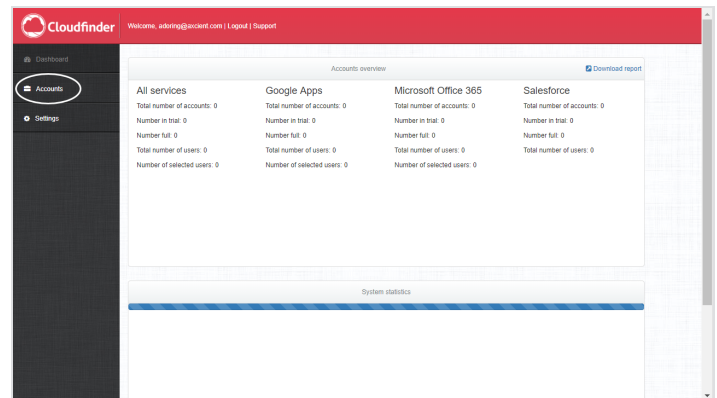
STEP 2: Find the Client Account

In the *Accounts* page, find the appropriate client account and click the **organization** name. The *Client Accounts* page displays.
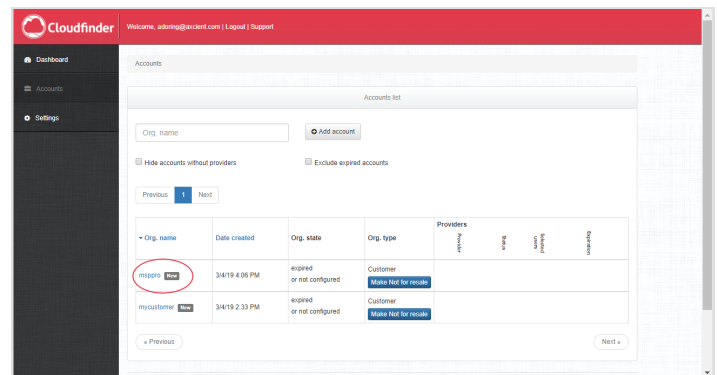
STEP 3: Define Settings

In the *Create New User* pop-up window, enter account details:

- In the *Email* field, enter the **email address** of the new administrator user.
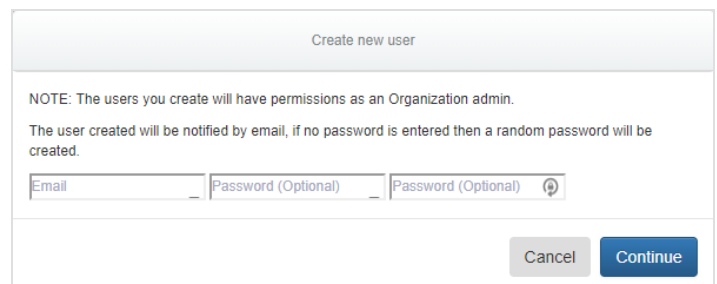
- Optionally, in the *Password* field, enter a **password** for the new administrator user. If you do not enter a password, then a random password will be assigned. If you do set a specific password, you must also re-enter your password to confirm.

Click the **Continue** button to save your changes. The new user will be notified by email with his or her user information.

Adding Services to Client Accounts

When you have created a client account, you can add one or more service instances to this account. For example, you can connect a Microsoft 365 service. CloudFinder can support multiple service instances for each client account.

Note: You can also add services from your CloudFinder client account. For instructions, please reference the **Enabling Service Connectors and Configuring Service Settings** section of this guide.

To add one or more service instances to client accounts:

STEP 1: Navigate to the Accounts Tab

From your CloudFinder reseller account, click the **Accounts** tab in the left-hand navigation menu. The *Accounts* page displays, showing all active client accounts.
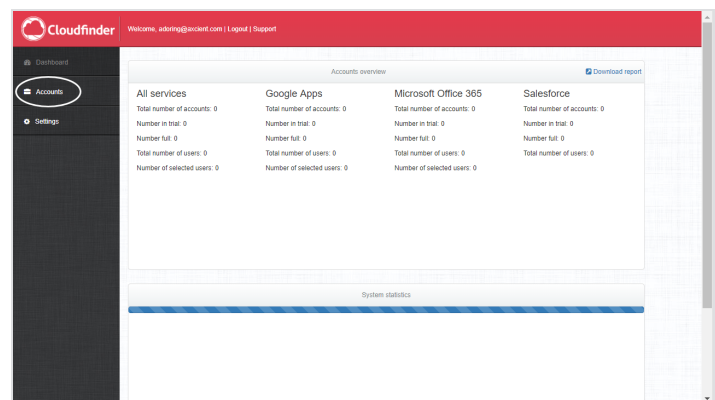

STEP 2: Find the Client Account

In the *Accounts* page, find the appropriate client account and click the **organization** name. The *Client Accounts* page displays.

STEP 3: Add a Provider

In the *Client Accounts* page, click the **Add Provider** button. The *Get Started With CloudFinder* pop-up window displays, prompting you to enter details about the client's service.
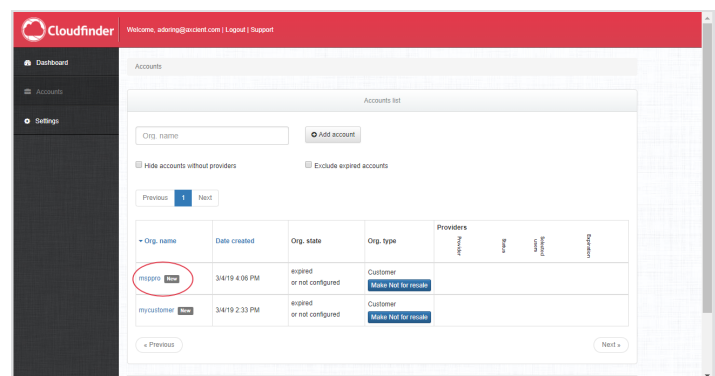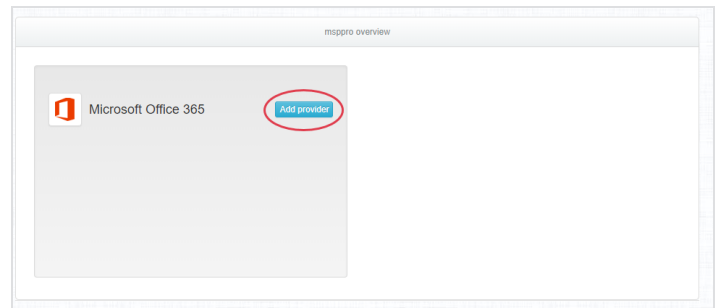

STEP 4: Define Settings
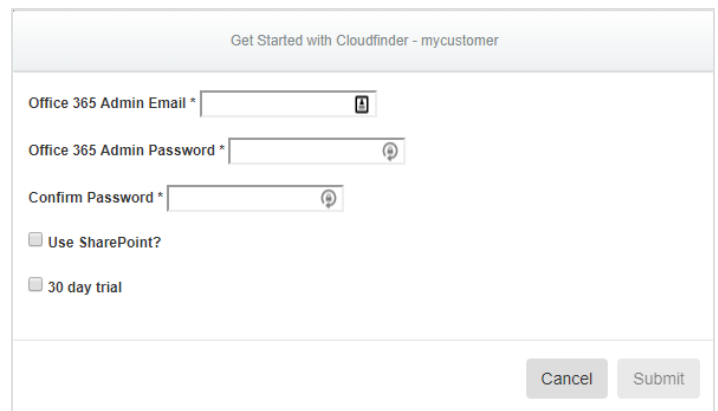
In the *Get Started with CloudFinder* pop-up window, enter details:

- In the *Microsoft 365 Admin Email* field, enter the **email address** of the Microsoft 365 administrator.

- In the *Microsoft 365 Admin Password* field, select the **password**. You will also be prompted to confirm your password.

  As a best practice, we recommend configuring a non-expiring password for this Microsoft 365 administrator.

- Optionally, click the **Use SharePoint** checkbox if you want to back up SharePoint data. If you select this checkbox, you will also be prompted to enter the URL of the SharePoint site.

- Optionally, click the **30 day trial** checkbox if you want to configure a trial.

  Note: This is a trial that you will manage between you and your client. You must remember to upgrade the trial to a full account, or end the trial, after the 30 day time period ends.

Click the **Submit** button to save your changes. You can repeat these steps for each client service instance.

Configuring Basic Client Account Settings
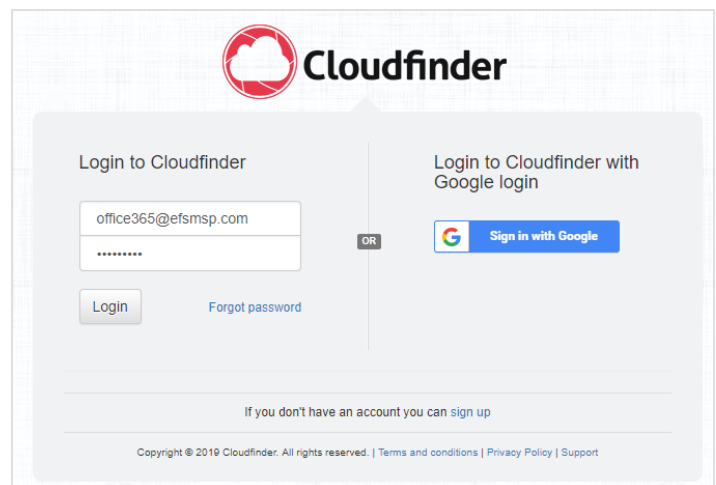
After you configure service information for a client account, you can log in to CloudFinder with administrator account credentials and configure settings for your client. For example, you can:

- Add users,
- Manage warnings and notifications,
- Turn on Backup Digest emails, and
- Turn on or off content visibility settings for documents.

To configure basic client account settings:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Navigate to the Settings Page

In the left-hand navigation menu, click the **Settings** tab. The *Settings* page displays, showing all settings for the client account.

STEP 3: Update Basic Settings

In the *Settings* page, update key settings for the client account. For example, you can update the following:

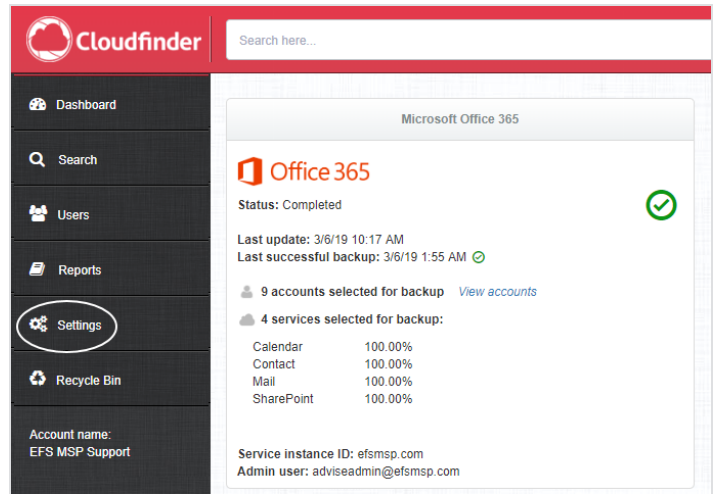- In the *Users* section, add, remove, or update administrator accounts for the client.

- In the *Warnings & Notifications* section, configure email notifications for system warnings. For example, a notification will be sent when a password expires or if Microsoft 365 is experiencing service health issues.

- In the *Backups Digest* section, configure backup digest emails.

- In the *General Settings* section, turn on or off content visibility settings for documents. By default, the **Document Summary** checkbox is selected, allowing you to view the details of backed up documents.
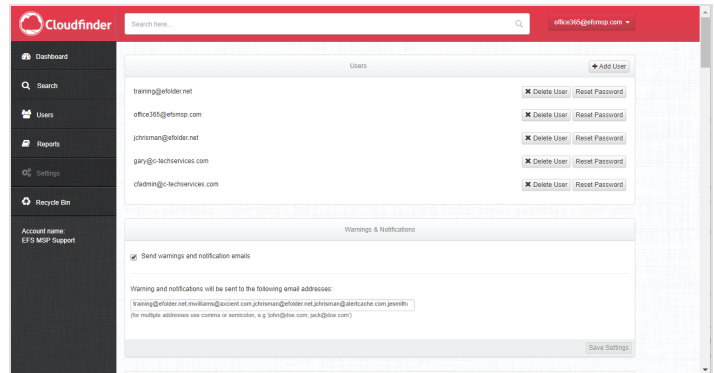
Enabling Service Connectors and Configuring Service Settings

In addition to configuring basic settings for your client account, you also need to enable service connectors and configure service settings. These settings control how CloudFinder backs up your Microsoft 365 data.

In the *Settings* page of the client account, you can:

- Configure user filter settings,
- Select your preferred method for backing up end user accounts and SharePoint sites, and
- Select which service connector you would like to back up.

To configure client account settings:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.
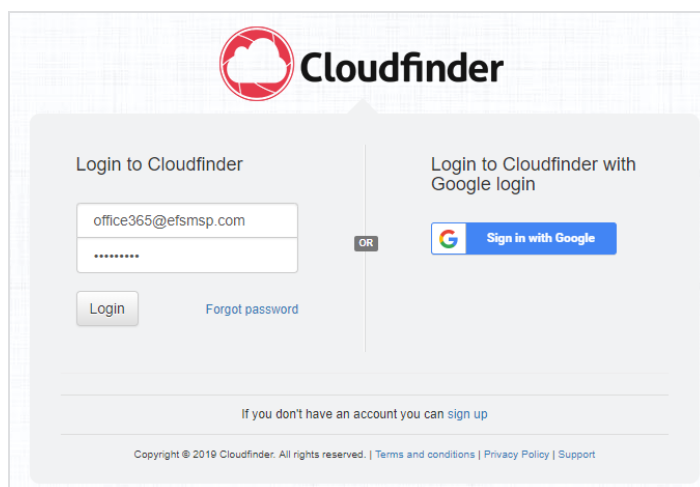
STEP 2: Navigate to the Settings Page

In the left-hand navigation menu, click the **Settings** tab. The *Settings* page displays, showing all settings for the client account.
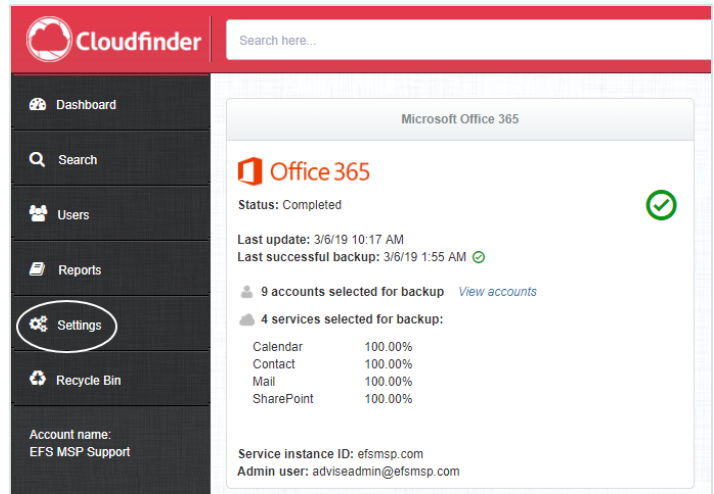

STEP 3: Optionally, Add a Service

In the *Settings* page, scroll down to find the *Service Settings* section.

In the Microsoft 365 panel, click the **Add Service** button and configure information about the service. You can also add services from your reseller account. For instructions, please reference the **Adding Services to Client Accounts** section of this guide.
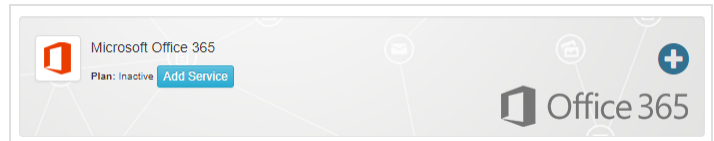
STEP 4: Enable Service Connectors and Configure Service Settings

While still in the *Service Settings* section, update settings for each service instance.

- In the *User Filter* subsection, click the **External** checkbox to automatically exclude external end users from backup. These accounts will not be listed in the *Users* tab.

- In the *New Users* subsection, use the checkboxes to select whether you want to automatically back up new end users or SharePoint Site Collections. For more information, please reference the Manually Selecting End User Accounts for CloudFinder Backups and Manually Selecting SharePoint Site Collections for CloudFinder Backups sections of this guide.

- In the *Select Services* subsection, you can select or deselect service connectors, including:

    - Microsoft 365 Calendar,

    - Microsoft 365 Contact,

    - Microsoft 365 Mail,

    - Microsoft 365 OneDrive, and

    - Microsoft 365 SharePoint.

- Click the **Save Settings** button when you are finished.

Automatically Backing Up End User Accounts in CloudFinder

After you configure service information for a client account, you can specify the end user accounts that will be backed up. Optionally, you can configure CloudFinder to automatically back up new user accounts.

CloudFinder might take up to 24 hours to back up selected end user accounts. The initial back up might take up to 72 hours to complete. Future backups are automatically scheduled to run multiple times per day.

To back up end user accounts with CloudFinder:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Navigate to the Users Page

In the left-hand navigation menu, click the **Settings** tab. The *Settings* page displays, showing settings for the client account.
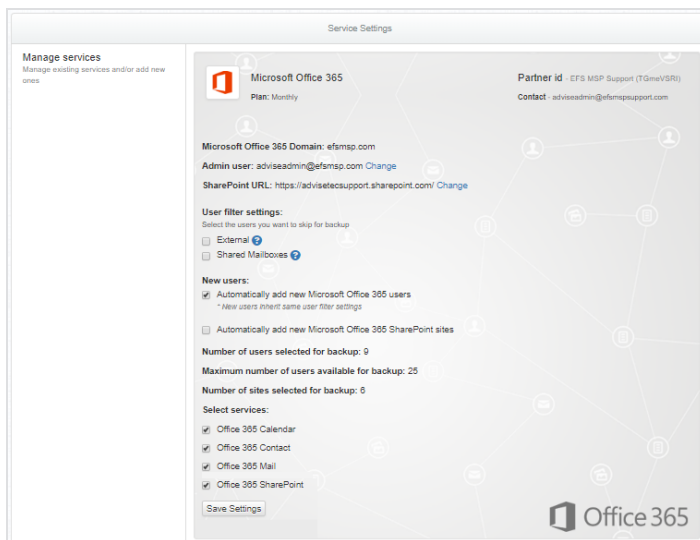

STEP 3: Find the Service

In the *Settings* page, scroll down to find the *Service* section, which displays each service instances you have configured for the client account. Find the appropriate service instance.

STEP 4: Update Settings

In the *New Users* section, click the **Automatically add new Microsoft 365 users** checkbox to automatically back up Microsoft 365 end users in CloudFinder.

Click the **Save Settings** button to save your changes.
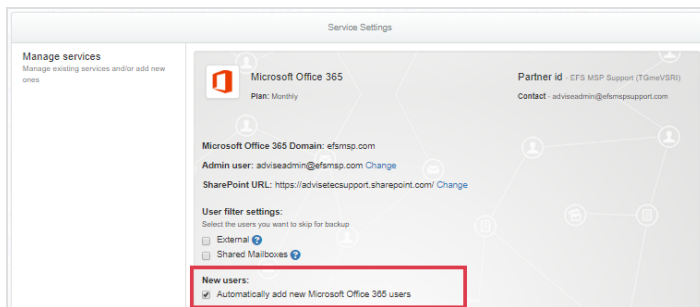
Manually Selecting End User Accounts for CloudFinder Backups

After you configure service information for a client account, you can specify the end user accounts that will be backed up. If you decide *not* to automatically back up end user accounts, you can manually select end user accounts in the *Accounts* page.

CloudFinder might take up to 24 hours to back up selected end user accounts. The initial back up might take up to 72 hours to complete. Future backups are automatically scheduled to run multiple times per day.

To manually select end user accounts for CloudFinder backups:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.
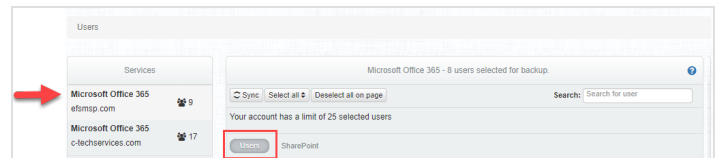
STEP 2: Navigate to the Users Page

In the left-hand navigation menu, click the **Users** tab. The *Users* page displays, showing a list of end users that belong to the selected service instance.


STEP 3: Filter Users

In the *Services* column, click a **service** to show only users who belong to that specific service.

Then, click the **Users** tab to view only user accounts.

STEP 4: Select an End User

Use the checkboxes to select the end user accounts that will be backed up. Please note that depending on your settings, end user accounts might be automatically selected when they are added to Microsoft 365. For more information, please reference the **Automatically Backing Up End User Accounts in CloudFinder** section of this guide.
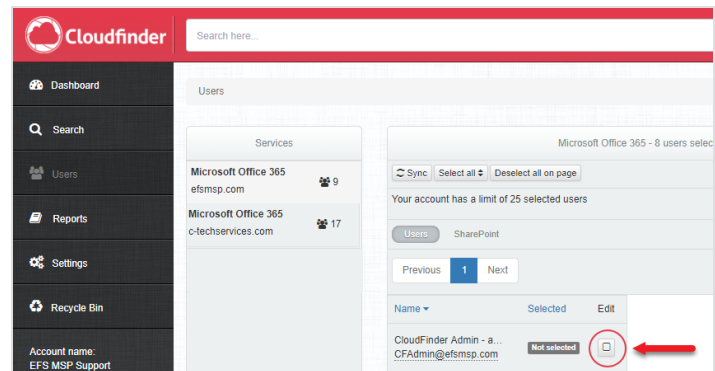
Automatically Backing Up SharePoint Site Collections in CloudFinder

After you configure service information for a client account, you can specify the SharePoint Site Collections that will be backed up. Optionally, you can configure CloudFinder to automatically back up new SharePoint Site Collections.

CloudFinder might take up to 24 hours to back up selected Site Collections. The initial back up might take up to 72 hours to complete. Future backups are automatically scheduled to run multiple times per day.

To back up SharePoint Site Collections with CloudFinder:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Navigate to the Users Page

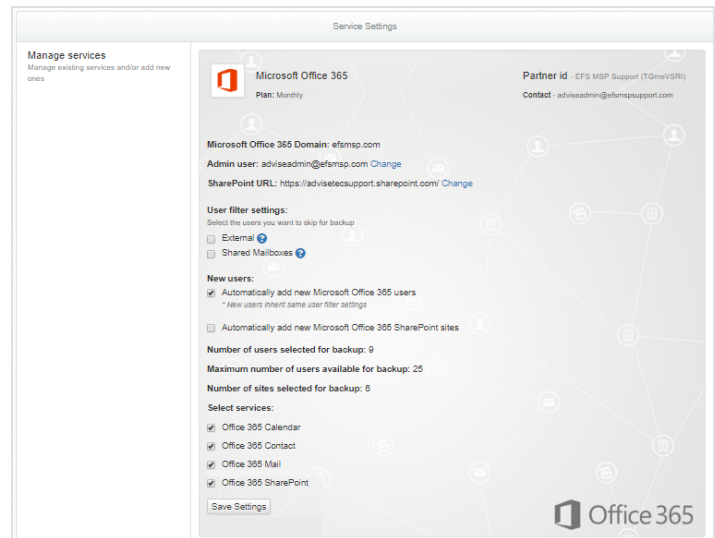In the left-hand navigation menu, click the **Settings** tab. The *Settings* page displays, showing settings for the client account.


STEP 3: Find the Service

In the *Settings* page, scroll down to find the *Service* section, which displays each service instances you have configured for the client account. Find the appropriate service instance.

STEP 4: Update Settings

In the *New Users* section, click the **Automatically add new Microsoft 365 SharePoint sites** checkbox to automatically back up new SharePoint Site Collections.

Click the **Save Settings** button to save your changes.
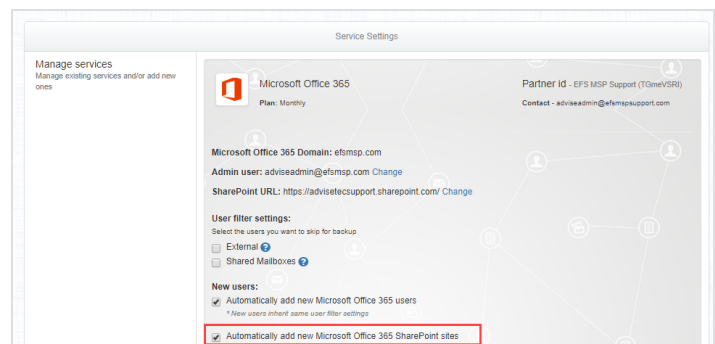
# Manually Selecting SharePoint Site Collections for CloudFinder Backups

After you configure service information for a client account, you can specify the SharePoint Site Collections that will be backed up. If you decide *not* to automatically back up SharePoint Site Collections, you can manually select SharePoint Site Collections in the *Accounts* page.

CloudFinder might take up to 24 hours to back up selected SharePoint Site Collections. The initial back up might take up to 72 hours to complete. Future backups are automatically scheduled to run multiple times per day.

To manually select SharePoint Site Collections for CloudFinder backups:
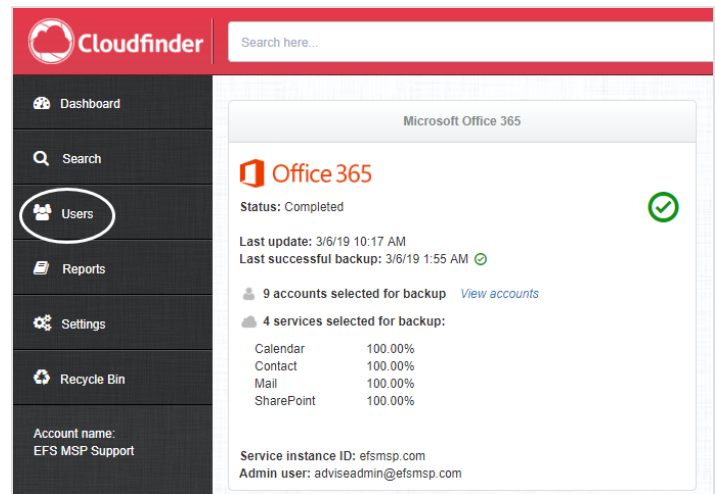
STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.
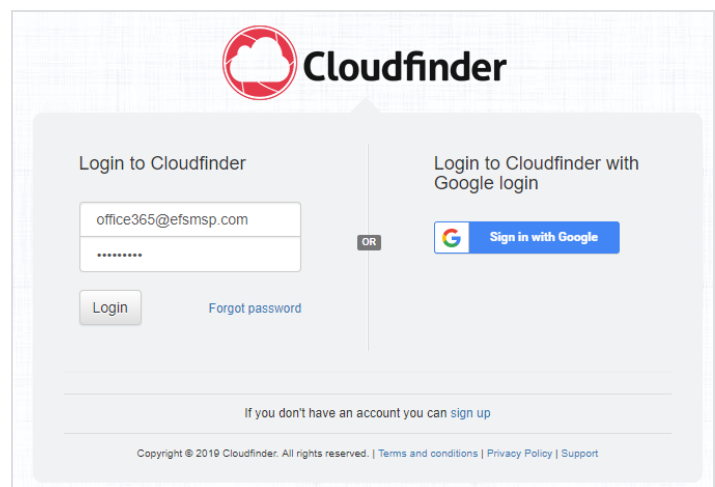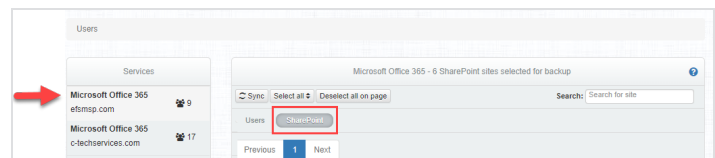
STEP 2: Navigate to the Users Page

In the left-hand navigation menu, click the **Users** tab. The *Users* page displays.

## STEP 3: Filter SharePoint Site Collections

In the *Services* column, click a **service** to show that specific service.

Then, click the **SharePoint** tab to view only SharePoint Site Collections.

STEP 4: Select a SharePoint Site Collection

In the *SharePoint* page, use the checkboxes to select the SharePoint Site Collections that will be backed up. Please note that depending on your settings, SharePoint Site Collections might be automatically selected when they are added to Microsoft 365. For more information, please reference the **Automatically Backing Up SharePoint Site Collections in CloudFinder** section of this guide.
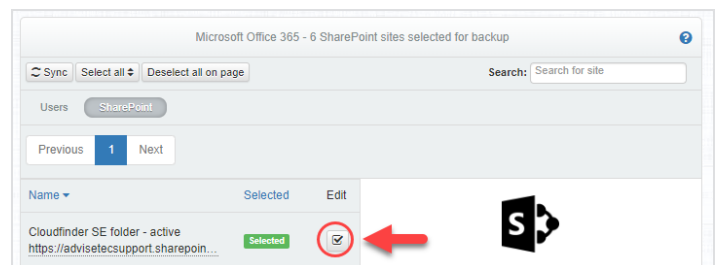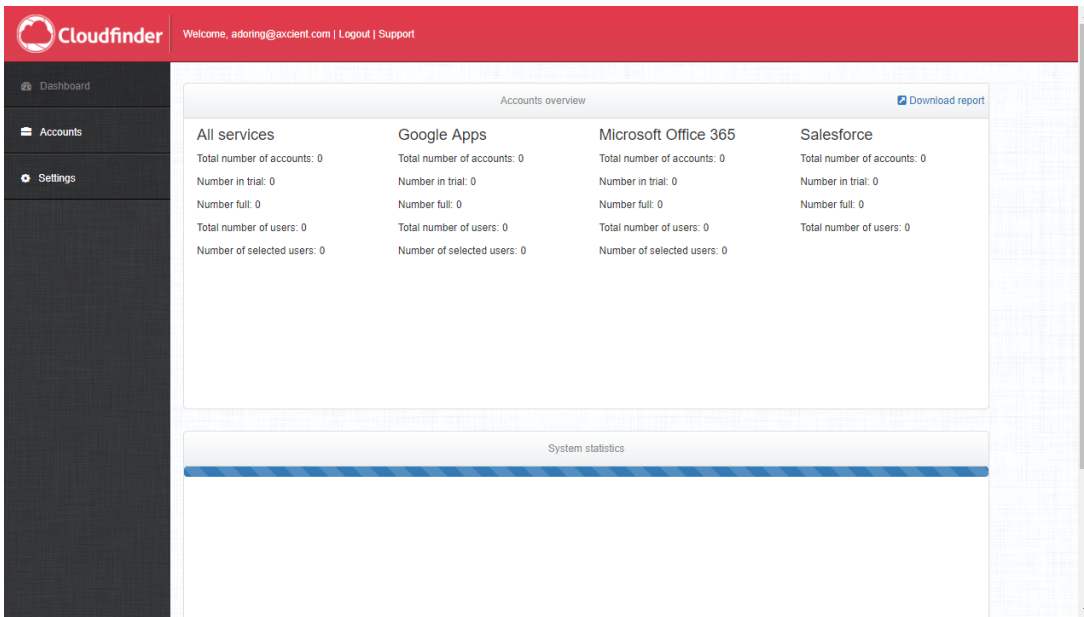
Chapter 3: Navigating CloudFinder

The CloudFinder navigation menu changes based on whether you are logging in with your reseller account or a client administrator account.

This section of the guide will review CloudFinder navigation elements for both the reseller account and the client account.
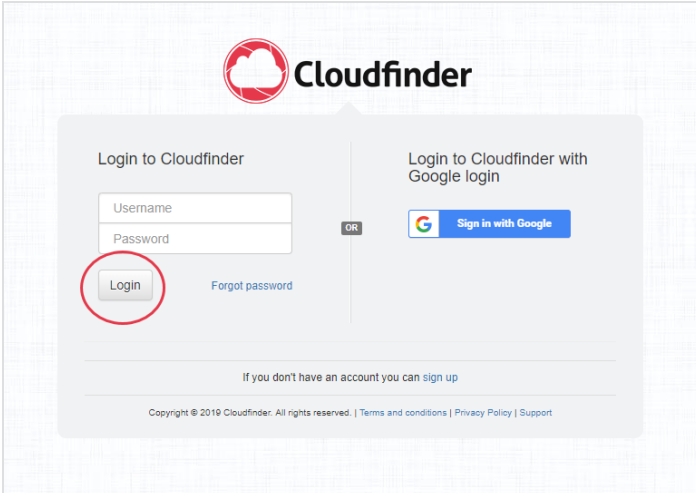
Navigating Your CloudFinder Reseller Account

Your CloudFinder reseller account allows you to:

- View overview information for each service instance that you support,
- Create and update client accounts,
- Create and update administrator users for client accounts,
- View backup reports for client accounts,
- Add service instances to client accounts, and
- Manage settings for client accounts.

To navigate your CloudFinder reseller account:

STEP 1: Log In to Your CloudFinder Reseller Account

From your preferred browser, navigate to the **CloudFinder web site**. Log in using your CloudFinder reseller account credentials and click the **Login** button.

View the Dashboard Tab

Click the *Dashboard* tab to view the *Dashboard* page. The reseller account *Dashboard* page allows you to quickly view a count of all services you manage, as well as an overview of system statistics.

Optionally, click the **Download Report** link to download this data in CSV format.
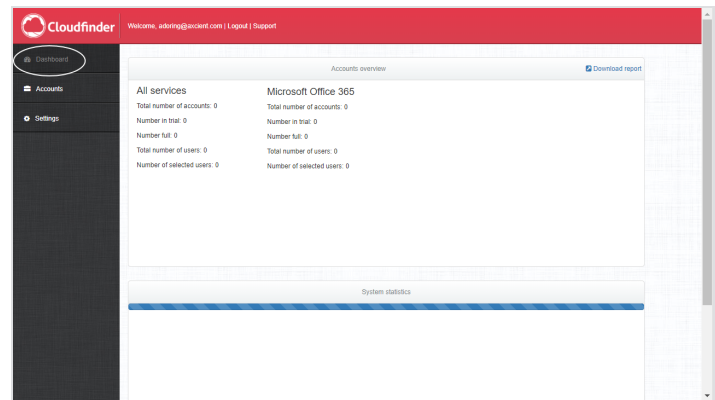
View the Accounts Tab

Click the *Accounts* tab to view the *Accounts* page. The reseller account *Accounts* page allows you to add client accounts for each client that you support.

You can also click the **organization name** of each client account to view and update administrator accounts and services.
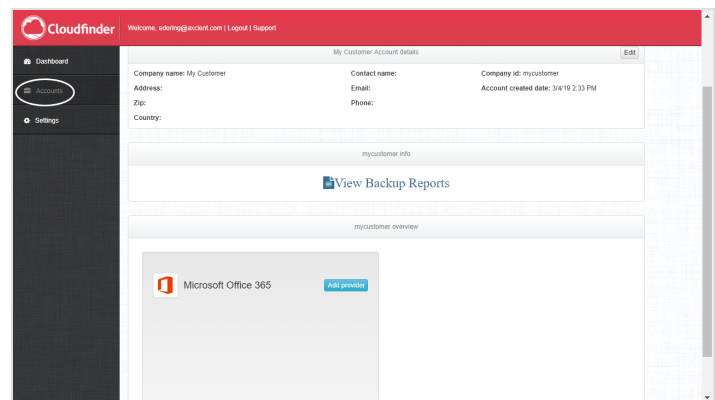
View the Settings Tab

Click the *Settings* tab to view the *Settings* page. The reseller account *Settings* page allows you to:

- View and edit your reseller account information,
- Add reseller user accounts,
- Manage warnings and notifications, and
- View the status of your reseller account.
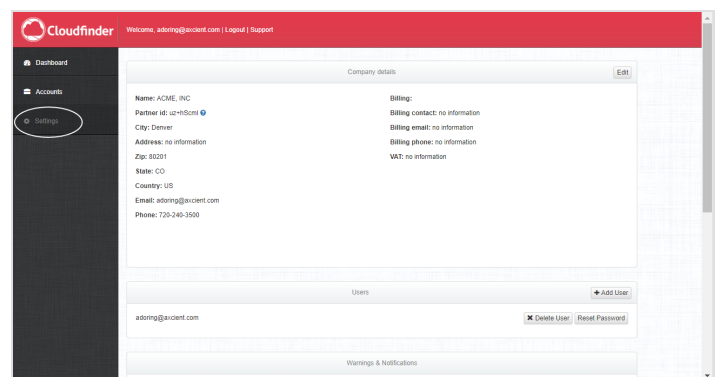
Navigating a CloudFinder Client Account

When you configure CloudFinder, you will create a new client account for each client that you support. As part of the account creation process, you will create an administrator user for each client account. You can use administrator login credentials to log in to each CloudFinder client account that you support.

Within each CloudFinder client account, you can:

- View summary information of all service instances and backups for the client account,
- Search, export, and restore data for a protected end user,
- Add and manage end users protected by CloudFinder,
- View Backup, Restore, Export, Audit, and Archive reports for the client account,
- Manage key settings for the client account, and
- View and restore data from the client account Recycle Bin.

To navigate your CloudFinder client account:

STEP 1: Log In to a CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Log in using your CloudFinder client account credentials and click the **Login** button.

View the Dashboard Tab

Click the *Dashboard* tab to view the *Dashboard* page. The client account *Dashboard* page allows you to quickly view a count of all service instances connected to the client account. Each service instance displays in its own panel.

You can also view a summary of backups in the *Backup Overview* panel.
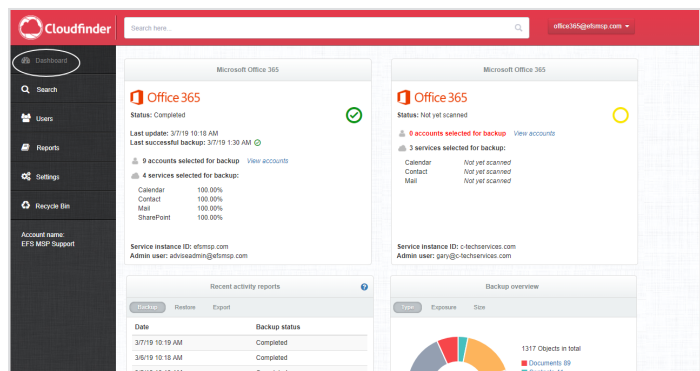
View the Search Tab

Click the *Search* tab to view the *Search* page. The client account *Search* page allows you to find backed up objects, like documents, events, and email messages. The search toolbar provides advanced filter options, allowing you to search by date, service instance, object type, user, or collection.

You can also use this page to export, migrate, or restore data.
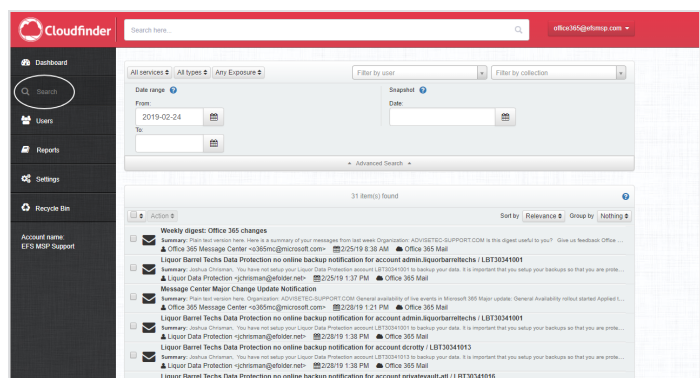
View the Users Tab

Click the *Users* tab to view the *Users* page. The client account *Users* page allows you to view all end users being protected by CloudFinder. You can also use this page to turn on backups for users, delete users, or restore users.
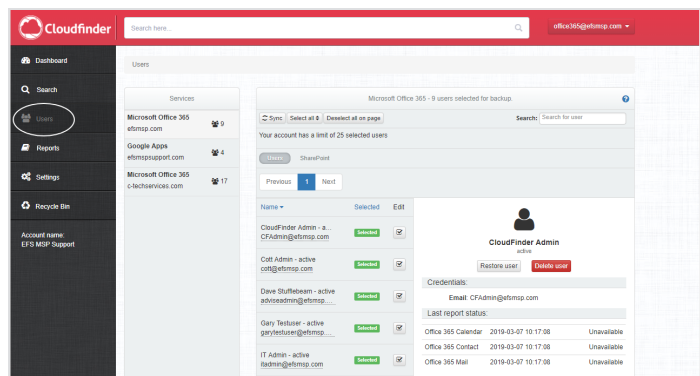
View the Reports Tab

Click the *Reports* tab to view the *Reports* page. The client account *Reports* page allows you to view CloudFinder reports, including:

- The Backup report,
- The Restore report,
- The Export report,
- The Audit report, and
- The Backup archive.
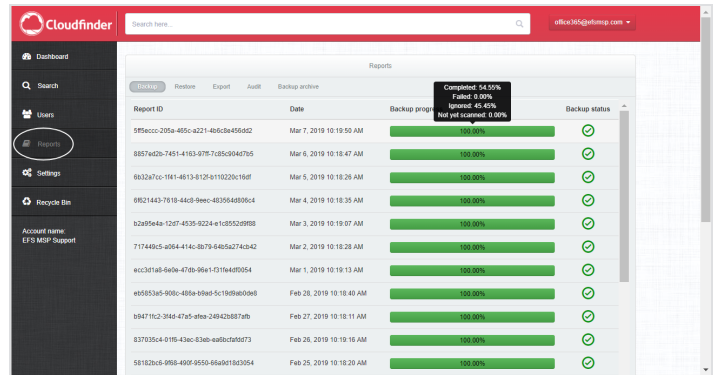
View the Settings Tab

Click the *Settings* tab to view the *Settings* page. The client account *Settings* page allows you to:

- View and edit client account information,
- Add administrator user accounts,
- Manage warnings and notifications,
- Manage the Backup digest, and
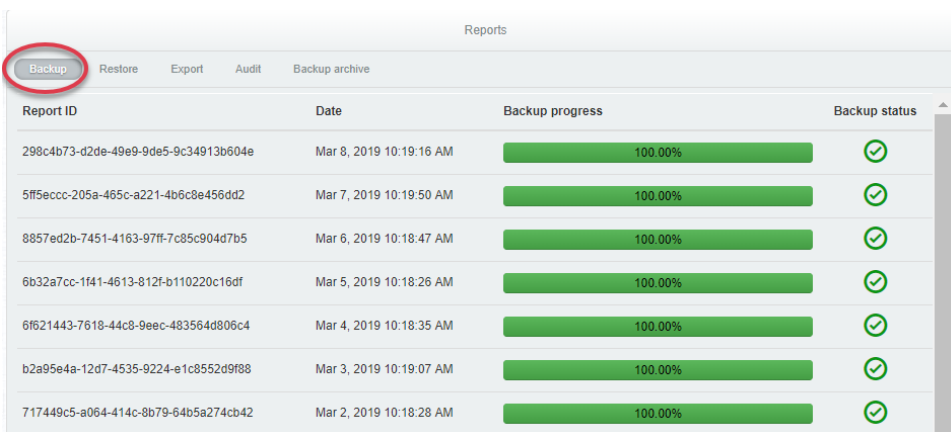- Manage service settings.
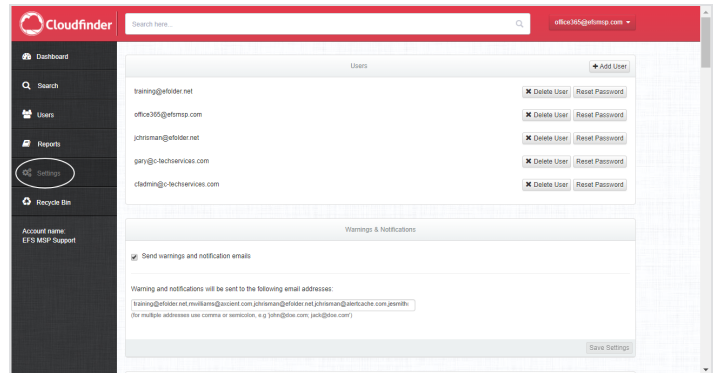
View the Recycle Bin Tab

Click the *Recycle Bin* tab to view the *Recycle Bin* page. The client account *Recycle Bin* page displays deleted data for 30 days, allowing you to restore this data if needed. After 30 days, data will be deleted permanently.
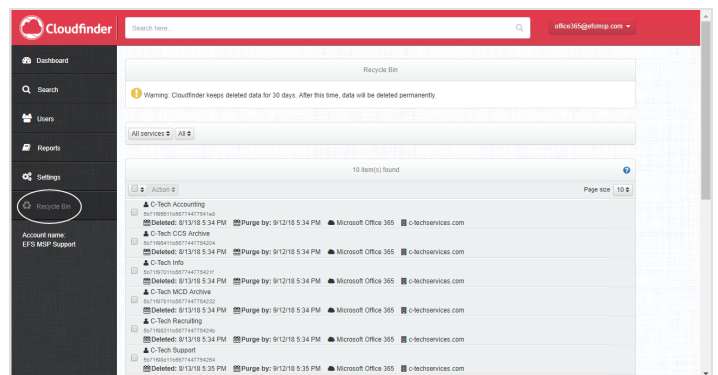
Chapter 4: Managing CloudFinder

As a CloudFinder administrator, you are responsible for managing the health of client account backups and restoring data if needed. This section of the guide will review common management tasks, including:

- Monitoring the Dashboard,

- Searching for data,

- Restoring or migrating data,

- Monitoring user data, and

- Viewing reports.

Monitoring the Dashboard

When you first log in to a client account, you will be presented with the *Dashboard* page. You can use this page to view connected services, activity reports, and backup statistics.

To monitor the Dashboard:

## STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Navigate to the Dashboard

When you first log in, you will be presented with the *Dashboard* page.

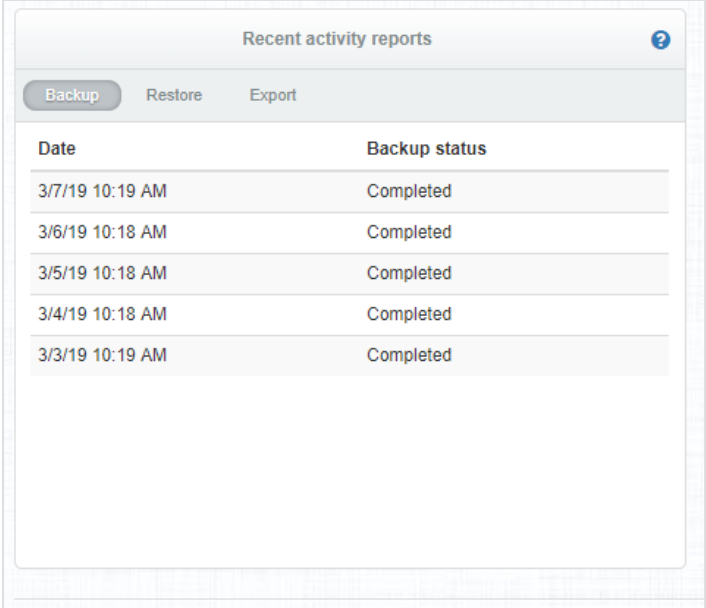Alternatively, click the **Dashboard** tab to access the *Dashboard* page.
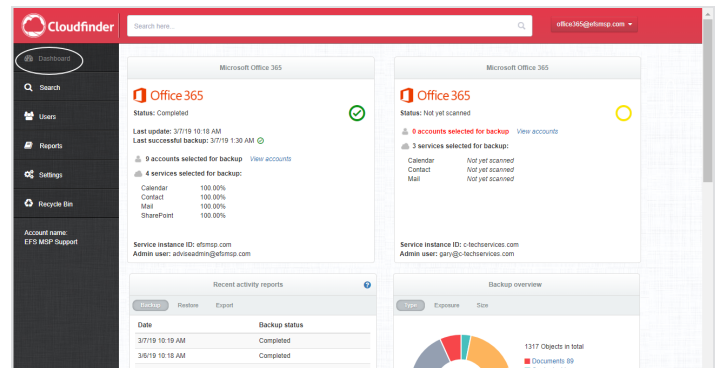
STEP 3: Review the Recent Activity Report Panel

In the *Dashboard* page, find the *Recent Activity Reports* panel. This panel displays a summary view of the most recent Backup, Restore, and Export reports. Click each tab to view the date and status of each report type.

You can also access these reports in the **Reports** tab.

STEP 4: Review the Backup Overview Panel

In the *Dashboard* page, find the *Backup Overview* panel. This panel presents a graphical display of objects being backed up.

- Click the **Type** tab to view a breakdown of each backup object by type (document, contacts, events, and emails).
- Click the **Exposure** tab to view a breakdown of each backup object by exposure status (private and external).
- Click the **Sites** tab to view a breakdown of each backup object by Site Collection.
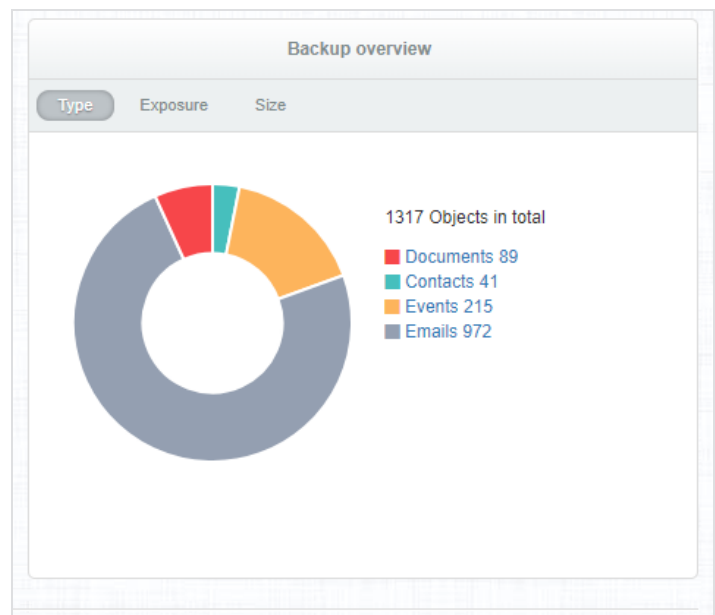
Searching and Viewing in CloudFinder

With CloudFinder's SmartSearch tool, you can quickly perform full-text search operations across all user accounts and connected services to find one or more objects. You can even search historical snapshots and version history. When you find what you're looking for, you can view documents and emails directly within the CloudFinder browser, without needing to download content or navigate away from the system.

Searching Best Practices

As a best practice, please consider the following when using CloudFinder's SmartSearch tool:

- CloudFinder defines data as *objects*. Objects include emails, contacts, calendars, calendar events, files, documents, and similar data.

- Searching in CloudFinder is *not* case sensitive.

- For fast and reliable searches, enter specific search criteria. This is especially helpful when trying to find text-heavy objects, like emails or documents.

Search Filters

In addition to utilizing the CloudFinder Search toolbar, you can also search using the following filters:

Services:	This filter will segregate objects by services available for the client account.
Types:	This filter will segregate objects by content type (document, email, event, and contact).
Exposure:	This filter will segregate objects by sharing status. For example:
	- *Private* objects have not been shared.
	- *Internal* objects have been shared with users from the same domain.
	- *External* objects have been shared with users from outside domains.
	- *Public* objects have been shared with everyone.
Filter by User:	This filter will segregate objects by the selected email address.
Filter by Collection:	This filter segregates objects by directory.

Search Fields

You can search for CloudFinder objects using the following fields:

Email Objects:	- sender

|	• to
	• cc
	• content
	• subject
	• receivedDate
Contact Objects:	• firstName
	• lastName
	• workEmails
	• homeEmails
	• lastUpdated
Document Objects:	• title
	• authors
	• content
	• fileName
	• lastUpdated
Event Objects:	• title
	• lastUpdated
	• location
	• lastUpdated

Search Syntax Examples

The following search syntax examples can help you quickly narrow your search results:

| Example	Syntax
You need to find an email with the subject containing the word, *application*.	*subject: application*
You need to find a file within a SharePoint Document Library.	*"sites/MySite/Shared Documents/"*
You need to find all files within a SharePoint Site Collection.	*collections: sites\/MySiteCollection\/**
You need to search a specific field that contains one word or another.	*title:(contract OR paper)*
You want to search a specific field containing an exact match.	*from:"John Smith"*
You want to perform a relevant search but you are unsure of the spelling.	*title:grene~*
You want to retrieve all objects within a date range.	*receivedDate:[2019-01-15 TO 2019-01-28*
You want to break down the search results with very specific criteria.	*financial AND document) OR (finansiell AND dokumentera) AND*

To use CloudFinder's SmartSearch tool:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.
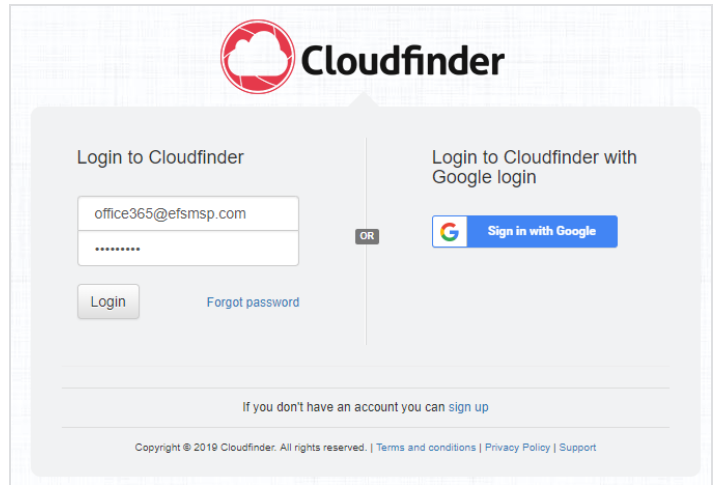
## STEP 2: Access the Search Page

In the left-hand navigation menu, click the **Search** tab. The *Search* page displays, giving you access to a search toolbar and filtering options.
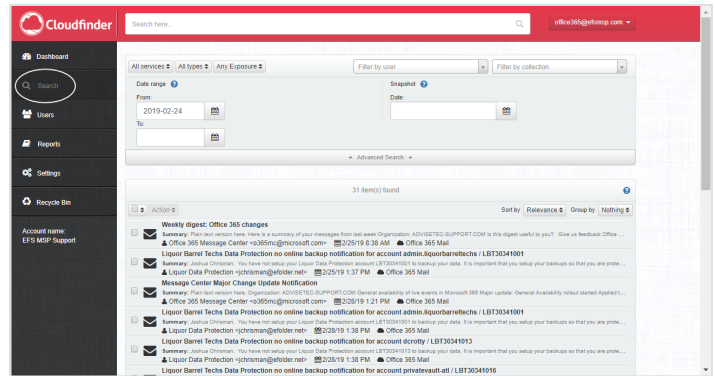
STEP 3: Use the Filters

In the *Search* page, use the search bar or search filters to find your data. For example, you can:

a. Filter by service instance, type (document, email, event, or contact), or exposure (private or external),
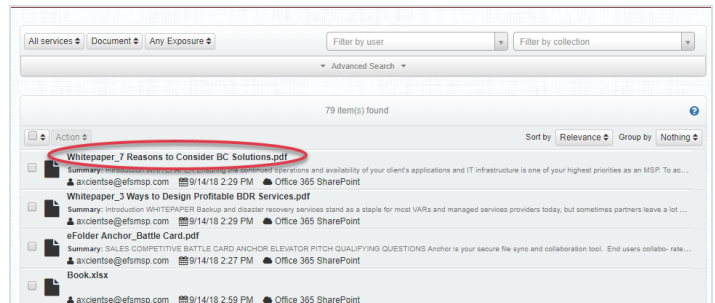
b. Filter by user or collection,
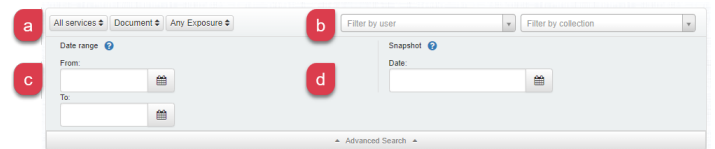
c. Filter by date range, or

d. Filter by exact snapshot date.

The page will refresh to show you filtered results.

STEP 4: Select the Object

Click the title of the object you want to view. The page expands to display a right-hand browser window.

STEP 5: View and Manage the Object

In the right-hand browser window, you can view metadata about the object, including name, date, and folder location.

Optionally, click the **View File** button to preview the first 1000 characters of the file or email. If this is a file, you can also use the *Version* drop-down menu to view a previous version of the file, if available.
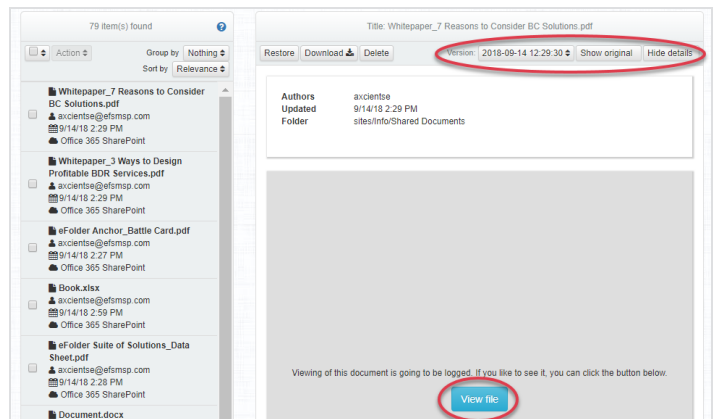
You can also restore, download, or delete this object. Please reference the **Restoring or Migrating Backup Objects** section of this guide for more information.

Restoring or Migrating Backup Objects

After using the CloudFinder SmartSearch tool to find a backup object, you can optionally perform restore or migration operations on this object.

For example, you can restore or migrate the following object types:

- Document (for example, from a SharePoint Document Library or OneDrive)
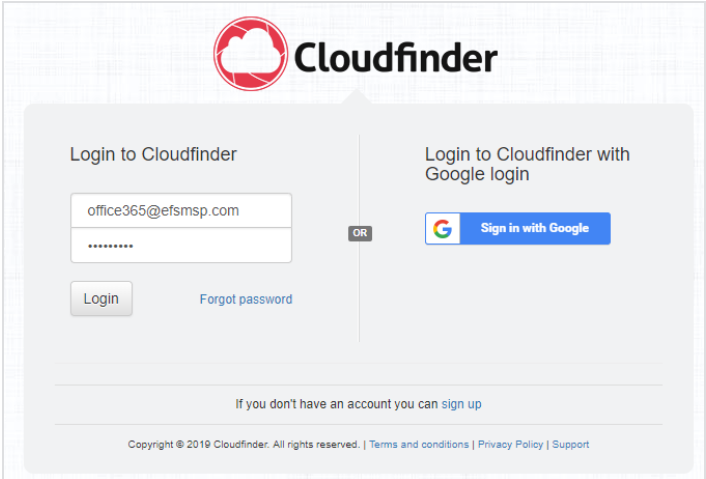- Email
- Event
- Contact

**Note**: Nested folders need to be restored individually.

To restore backup data:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Access the Search Page

In the left-hand navigation menu, click the **Search** tab. The *Search* page displays, giving you access to a search toolbar and filtering options.
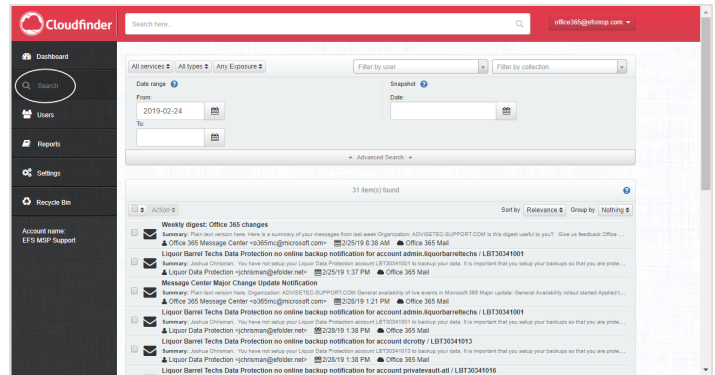
STEP 3: Select the Object

In the *Search* page, use the filters to find your data.

For more information on searching best practices, please reference the [Searching and Viewing in CloudFinder](#) section of this guide.
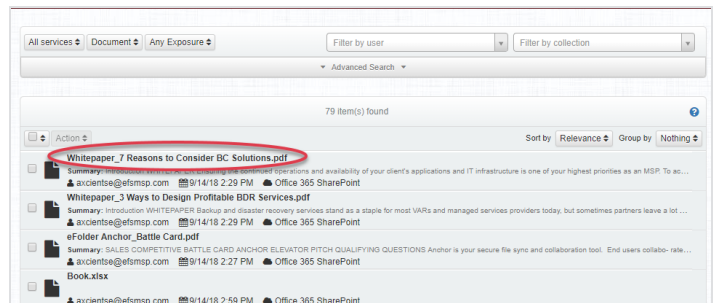
When you find the correct item, click the **title** of the object you want to view. The page expands to display a right-hand browser window.

STEP 4: View the Object

Optionally, click the **View File** button to preview the first 1000 characters of the file or email. If this is a document, you can also use the *Version* drop-down menu to view a previous version of the file, if available.

If you cannot view the details of a file, you might need to turn on Content Visibility settings. For instructions, please reference the [Configuring Basic Client Account Settings](#) section of this guide.

Note: In certain instances, you might not be able to view the content of very large backup objects. You can still,
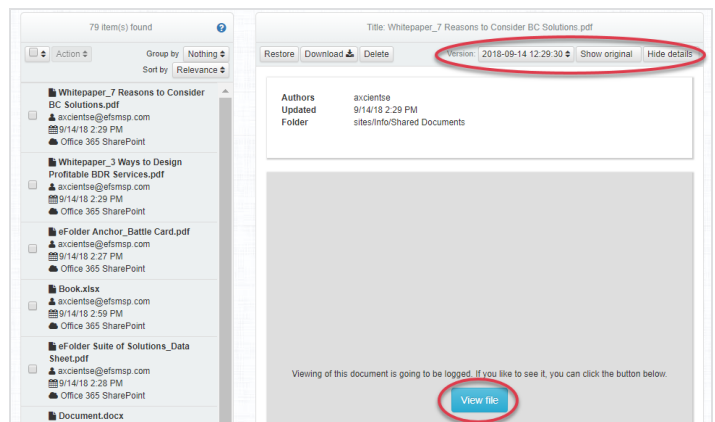
however, view metadata or download the object if needed.

STEP 5: Optionally, Restore or Migrate the Object

Optionally, click the **Restore** button to restore the file or email to the same user account or a different user account.

In the pop-up window, use the *Restore Item To* drop-down menu to select the **site** where this item will be restored.
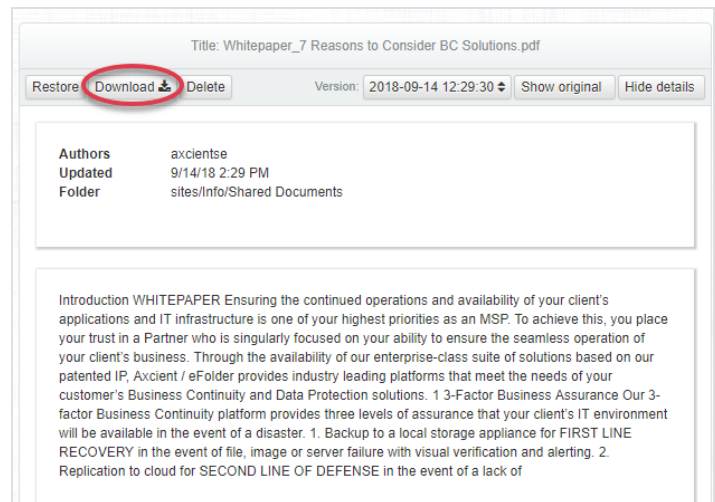
Then use the *Restore to User* drop-down menu to select the **user account** where this item will be restored.

Click the **Proceed** button to complete the restore process.
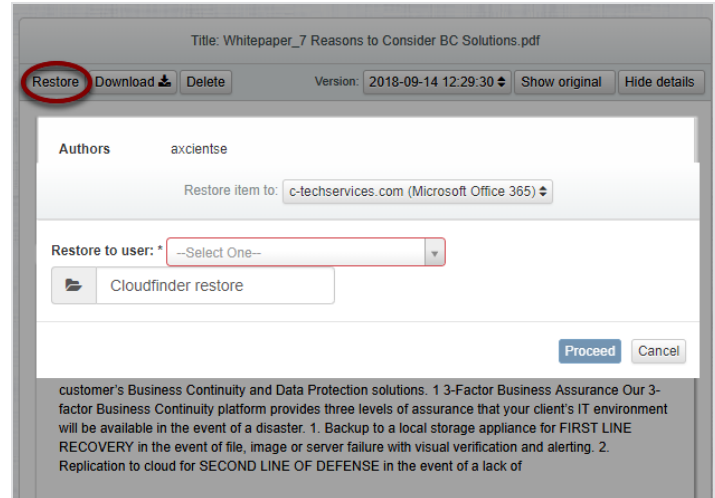
STEP 6: Optionally, Download the Object

Optionally, click the **Download** button to download the file to your local machine.

STEP 7: Optionally, Manage Multiple Objects

You can also manage multiple items at one time. For example, you can restore, export, or delete items in bulk.

Using the checkboxes, select all items that you want to manage. Then, click the **Action** drop-down menu and select from the follow:

- Click the **Restore** button to restore all selected items.

- Click the **Export** button to export all selected items. A zip file will generate and become available in the *Reports* page.

- Click the **Delete** button to delete all selected items.
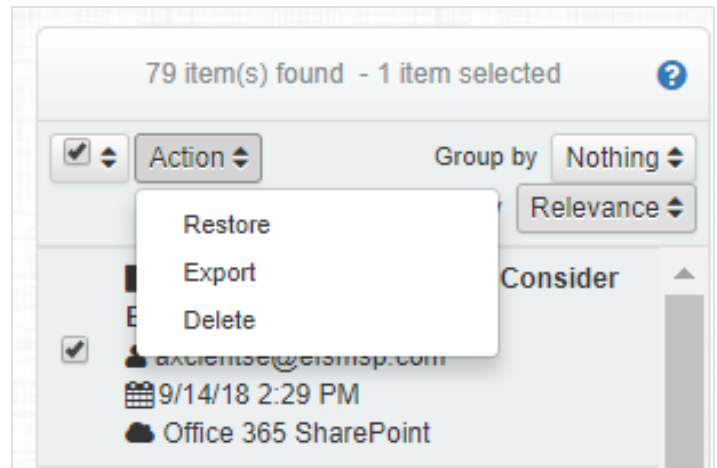
Restoring or Migrating End User Accounts

In addition to restoring, migrating, or deleting individual objects, you can also restore or migrate an entire end user account. This process is useful if an entire end user account has been lost, or if an end user account needs to be completely migrated to a different account.

To restore, migrate, or delete end user accounts:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.


STEP 2: Access the Users Page

In the left-hand navigation menu, click the **Users** tab. The *Users* page displays, giving you access to advanced end user management tools.
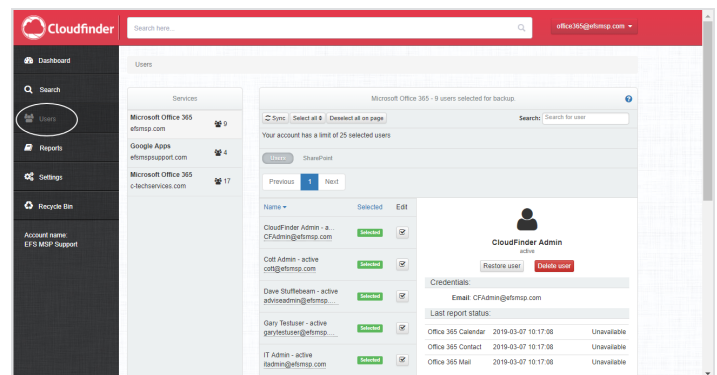
STEP 3: Search for the End User

In the *Search* bar, search for the end user you want to manage.

Then, in the left-hand results window, click the name of the end user you want to manage. End user details will display in the right-hand browser window.
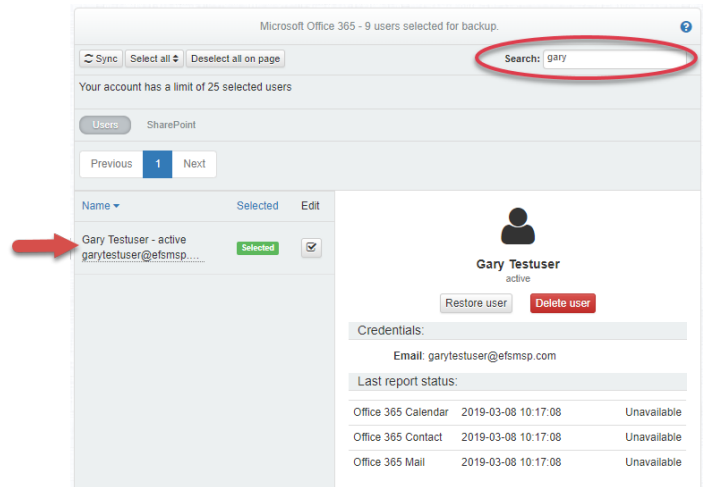
STEP 4: Restore or Migrate the End User

Optionally, in the right-hand browser window, click the **Restore** button to restore end user backup data to the same user or a different end user account.

In the pop-up window, select your restore options:

- In the *Backup Date and Time* drop-down menu, select the **snapshot** you want to restore.

- In the *Which Services do you Want to Restore* section, click the **checkboxes** to select which items should be restored.

- In the *Restore to User* drop-down menu, select the **end user account** where this data will be restored. You can select the same end user or a different end user account.

- In the *Name of the Restore Folder* field, type the **name of the folder** where the restored data will reside.

Click the **Proceed** button to complete the restore process.
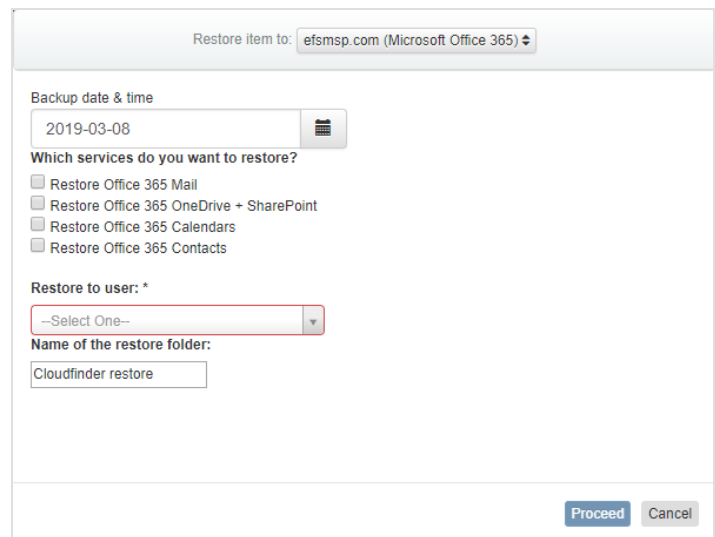
Viewing Reports

As a CloudFinder administrator, you can view reports to help manage backups, the restore process, the export process, auditing information, and archives. These reports give you detailed insight into activity that occurs in the system.

To view reports:

## STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.
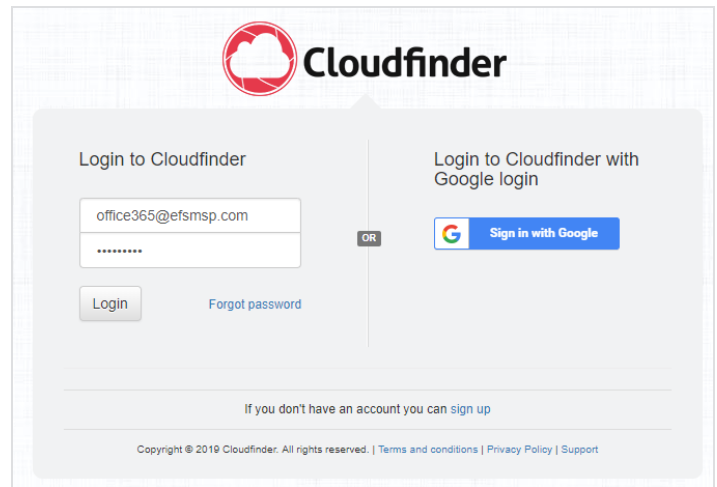
STEP 2: Access the Reports Page

Click the **Reports** tab. The *Reports* page displays, giving you access to the following:

- Backup report
- Restore report
- Export packages
- Audit information
- Backup archives
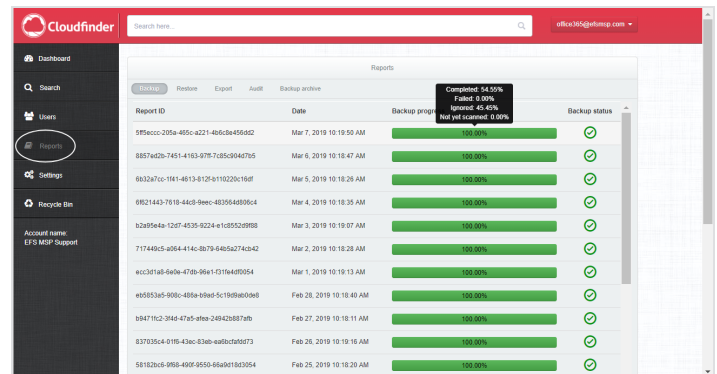
STEP 3: View the Status of Backups

Click the **Backup** subtab to view the backup status of all services. As you scroll down the window, the page will refresh to load more historical backup information. This report allows you to view:

- Report ID generated for the service,
- Date of the backup,
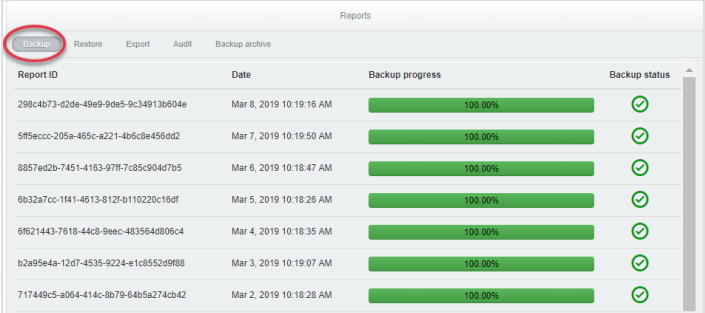- Backup progress, and
- Backup status.

You can optionally hover your mouse over the backup progress status bar to view more information about the status of the backup:

- *Completed* indicates that the backup completed successfully.
- *Failed* indicates that the backup did not complete.
- *Ignored* indicates that a user did not have a particular service configured.
- *Not yet scanned* indicates that a backup did not yet start for a user.

To view more details about these statuses, click the **Report ID** or the **backup status bar** to drill down into the report.

Note: Each Backup report represents the status of backups performed within 24 hours prior to the report.

A failed report does not indicate that backups are corrupt or in an invalid state. A failed report simply indicates that CloudFinder did not back up data from the past 24 hours.
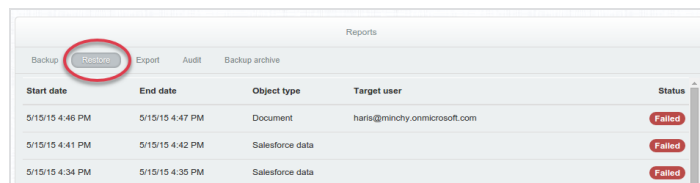
STEP 4: View the Status of Restores

Click the **Restore** subtab to view the status of restore processes. This report allows you to view:

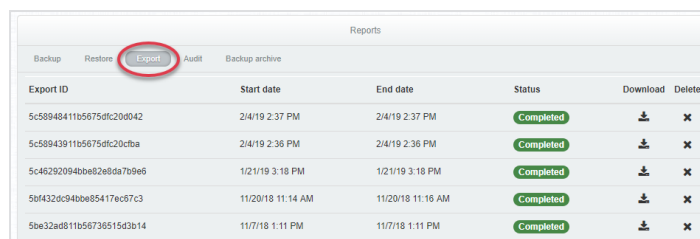- Start date,

- End date,

- Object type, and

- Target user.

STEP 5: View the List of Exports

Click the **Export** subtab to access content that has been exported from the *Search* tab.

You can optionally download exported content to your local machine in ZIP file format.

STEP 6: View Auditing Information

Click the **Audit** subtab to view audit information generated by users. For example, you can see:

- User name performing the action,

- IP address of the machine,

- Date of the activity, and

- Activity type (for example, restore, search, edit, and so forth).

You can optionally click each activity to drill down and view more information.
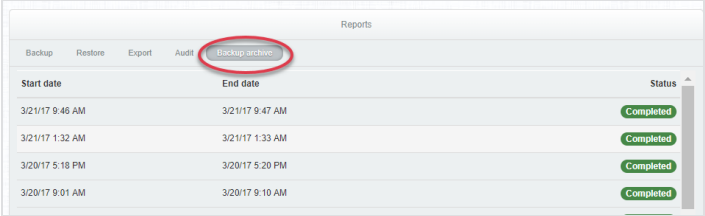
STEP 7: View Backup Archives

Click the **Backup Archives** subtab to view historical backup data. For example, you can see:

- Start date,

- End date, and

- Status.

You can optionally click each activity to drill down and view more information.

Chapter 5: Managing Deleted Objects and End User Accounts

As a CloudFinder administrator, you can optionally delete objects and end user accounts from CloudFinder backups. When an item is deleted, it will not be backed up by CloudFinder, nor will it appear in search results.

Deleted items will be moved to the Recycle Bin for 30 days and then permanently purged after this retention period ends. During the 30 day retention period, you can optionally restore these items from the Recycle Bin.

This chapter will review:

- Deleting backup objects, such as documents, emails, events, and contacts, and

- Deleting end user accounts.
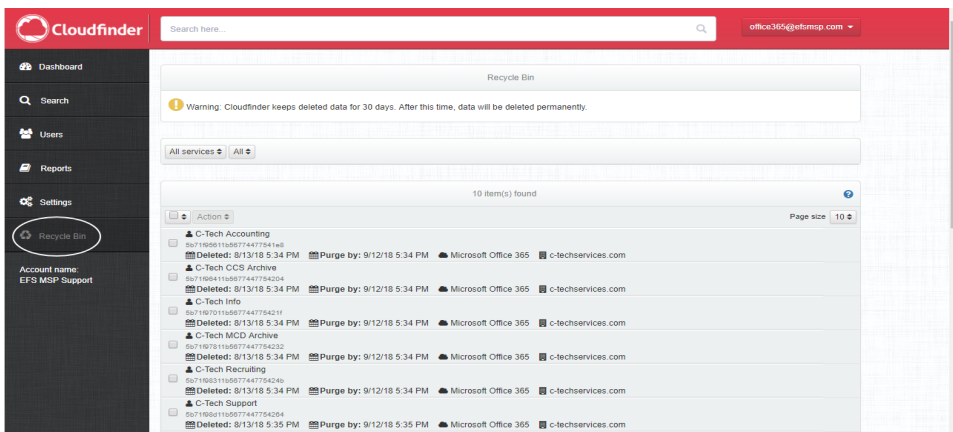
Deleting Backup Objects

After using the CloudFinder SmartSearch tool to find a backup object, you can optionally delete the object from CloudFinder.

To delete backup objects:
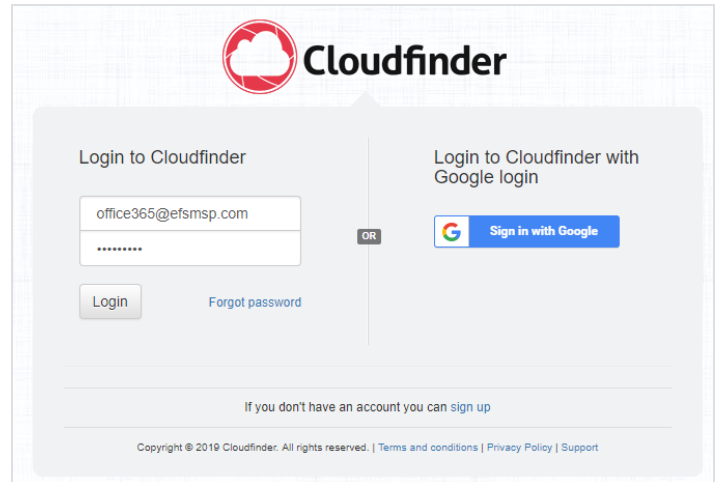
STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Access the Search Page

In the left-hand navigation menu, click the **Search** tab. The *Search* page displays, giving you access to a search toolbar and filtering options.
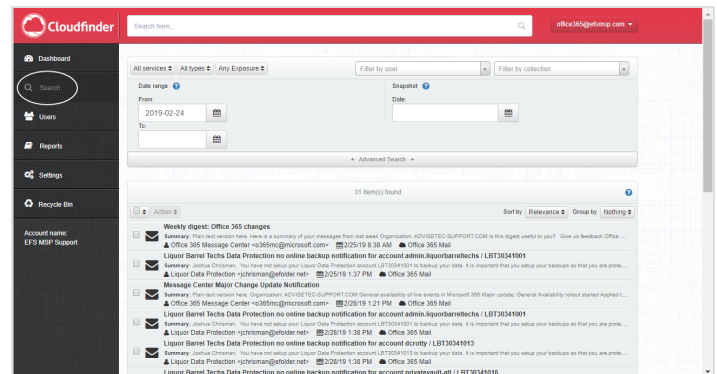
STEP 3: Find and Select the Object

In the *Search* page, use the filters to find your data.

Then, click the **checkbox** adjacent to the object(s) you
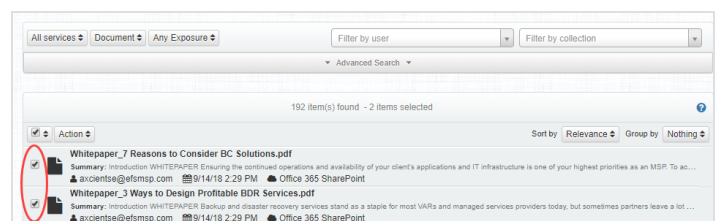
would like to delete. You can delete more than one object at one time.

STEP 4: Delete the Object

Click the **Action** drop-down button and select **Delete**.
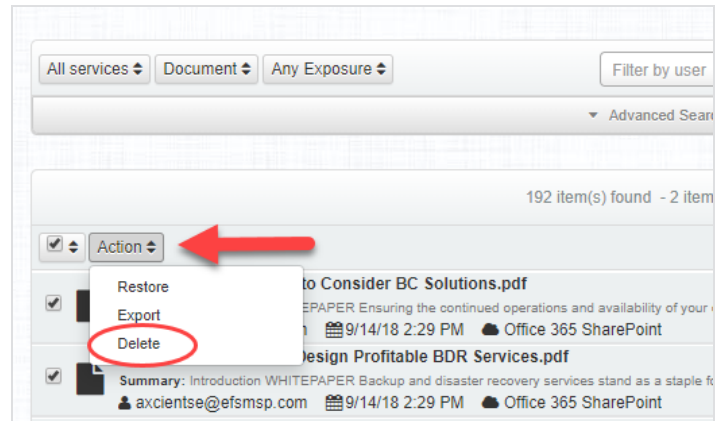
STEP 5: Confirm Deletion

In the *Delete* dialog box, you will be prompted to select each of the following checkboxes to indicate that you understand the warning message:

- Items will no longer be backed up.
- Items will not appear in search results.

Click the **Delete** button to complete the process. The object(s) will be deleted, including all previous versions.

For instructions on restoring objects within the 30 day retention window, please reference the **Restoring from the Recycle Bin** section of this guide.
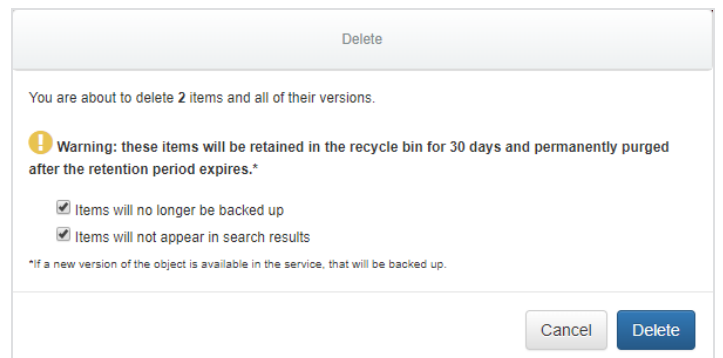
Deleting Versions of Backup Objects

In addition to deleting all versions of a backup object, you can optionally delete a single version of the backup object from CloudFinder.

To delete a version of a backup objects:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Access the Search Page

In the left-hand navigation menu, click the **Search** tab. The *Search* page displays, giving you access to a search toolbar and filtering options.

STEP 3: Select the Object
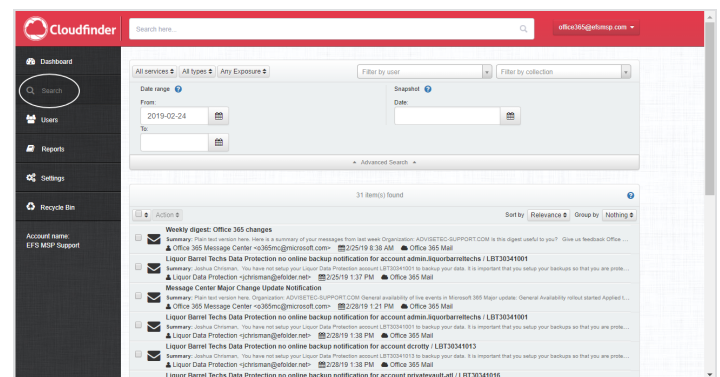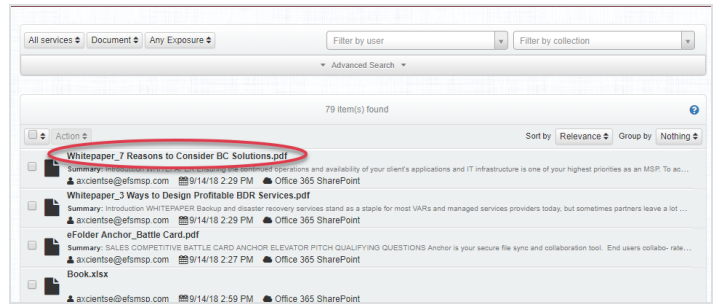
In the *Search* page, use the filters to find your data.

Then, click the title of the object you want to view. The page expands to display a right-hand browser window.

STEP 4: View the Object

Click the **View File** button to preview the first 1000 characters of the object. To change versions, click the the *Version* drop-down menu to select a **previous version**, if available.

Note: In certain instances, you might not be able to view the content of very large backup objects. You can still, however, view metadata or download the object if needed.
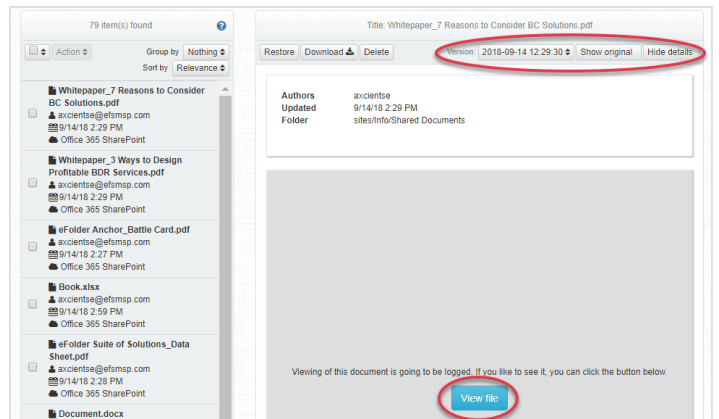
STEP 5: Delete the Object

Click the **Delete** button to delete the object. The email or file will be moved to the Recycle Bin for 30 days and then permanently purged after this retention period ends.

You will be prompted to check each of the following checkboxes to indicate that you understand the warning message:

- Version will no longer be backed up.
- Version will not appear in search results.

Click the **Delete** button to complete the process.

For instructions on restoring this object within the 30 day
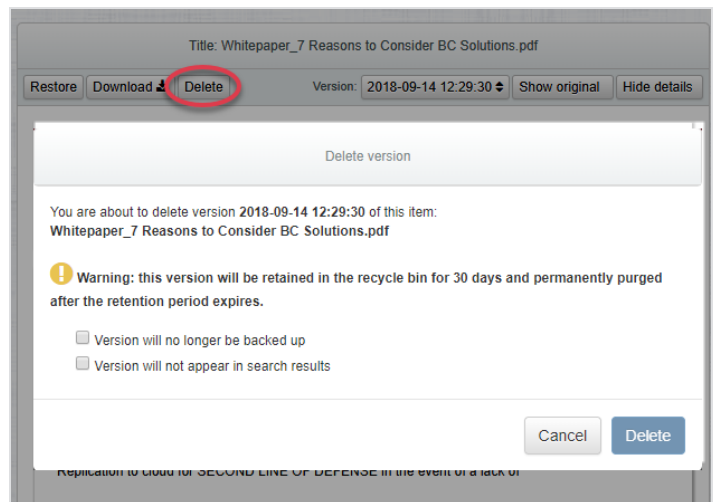
retention window, please reference the **Restoring from the Recycle Bin** section of this guide.

Deleting End User Accounts

In addition to deleting specific backup objects, you can optionally delete an entire end user account from CloudFinder so that CloudFinder no longer performs backup operations for this account.

To delete an end user account:

STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.

STEP 2: Access the Users Page

In the left-hand navigation menu, click the **Users** tab. The *Users* page displays, giving you access to advanced end user management tools.

STEP 3: Search for the End User

In the *Search* bar, search for the end user you want to manage.

Then, in the left-hand results window, click the name of the end user you want to manage. End user details will display in the right-hand browser window.
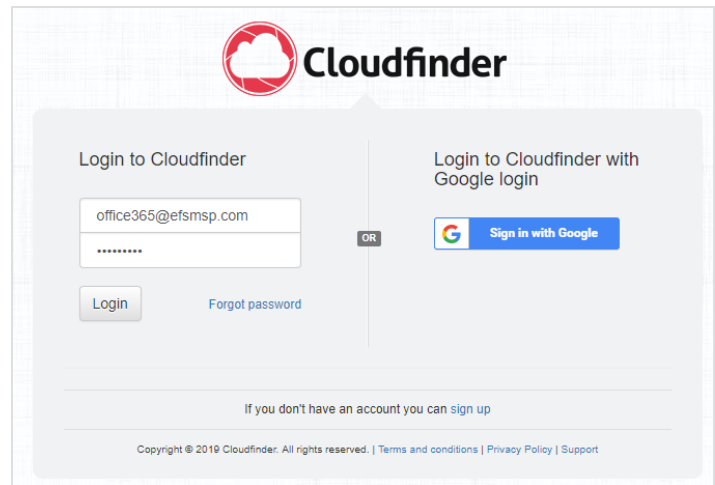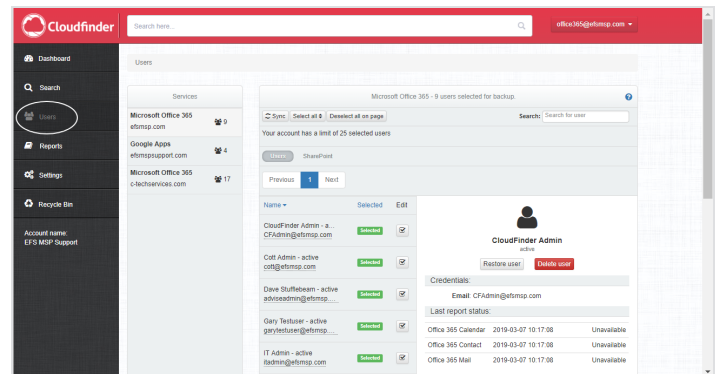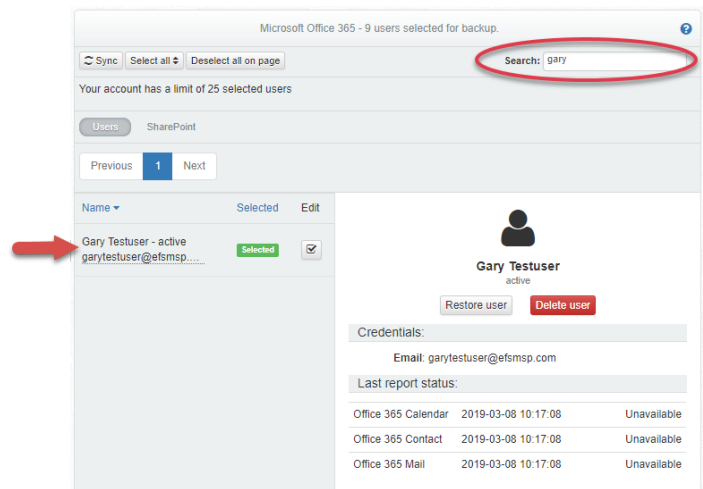
STEP 4: Delete the End User

Click the **Delete** button to delete the end user account. The end user account will be moved to the Recycle Bin for 30 days and then permanently purged after this retention period ends.

You will be prompted to check each of the following checkboxes to indicate that you understand the warning message:

- User will no longer be backed up.

- User files will not appear in search results.

Click the **Delete** button to complete the process.

For instructions on restoring this object within the 30 day retention window, please reference the **Restoring from the Recycle Bin** section of this guide.
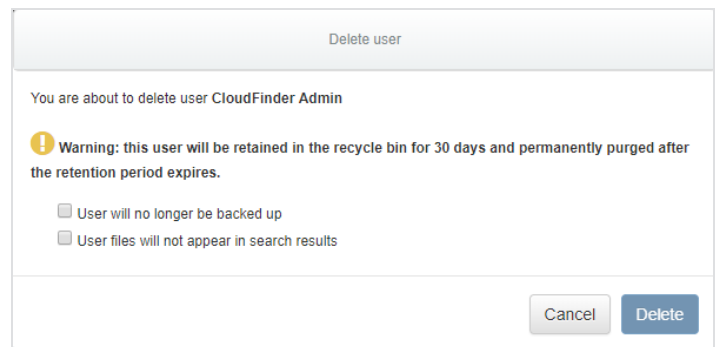
# Restoring from the Recycle Bin

If you delete a backup object (email, document, contact, or event) or an end user account, these deleted items will be moved to the Recycle Bin and remain there for 30 days. Items that are in the Recycle Bin are not backed up and do not display in search results.

As an administrator, you can restore content from the Recycle Bin within the 30 day retention period. After 30 days, the item will be permanently deleted.

To restore from the Recycle Bin:
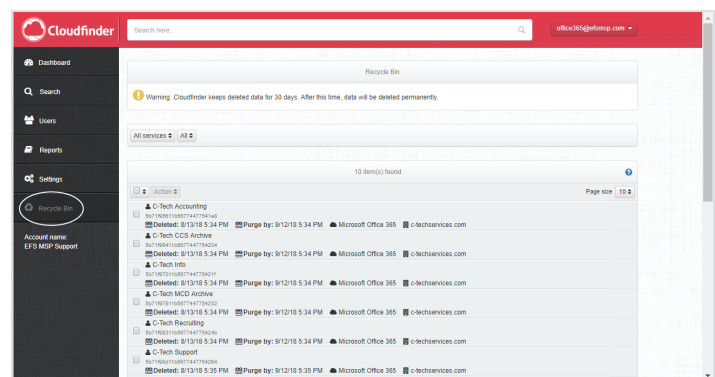
STEP 1: Log In to the CloudFinder Client Account

From your preferred browser, navigate to the **CloudFinder web site**. Enter account credentials associated with the client account and click the **Login** button.
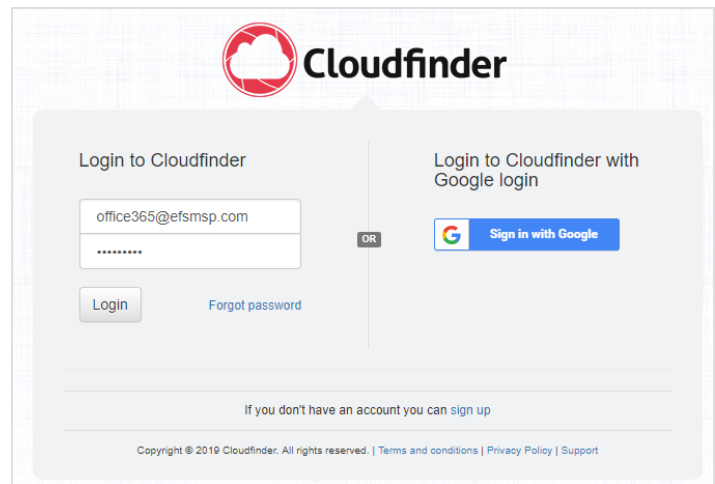

STEP 2: Access the Recycle Bin

In the left-hand navigation menu, click the **Recycle Bin** tab. The *Recycle Bin* page displays, giving you access to deleted items.

STEP 3: Filter Deleted Items

In the *Services* drop-down menu, click to select the **service instance** where the deleted item belongs. The Recycle Bin will refresh to show only deleted items belonging to that service instance.
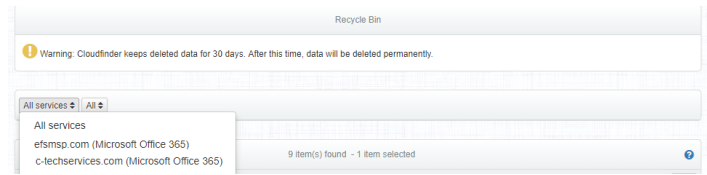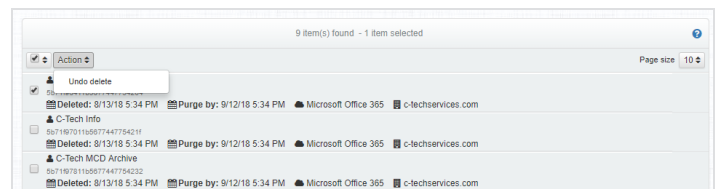

STEP 4: Restore Deleted Items

Use the checkboxes to select one or more items that you want to restore.

Then, click the *Action* drop-down menu and select **Undo Delete**.

The item will be restored to its original location. It will now be backed up and will display in search results.
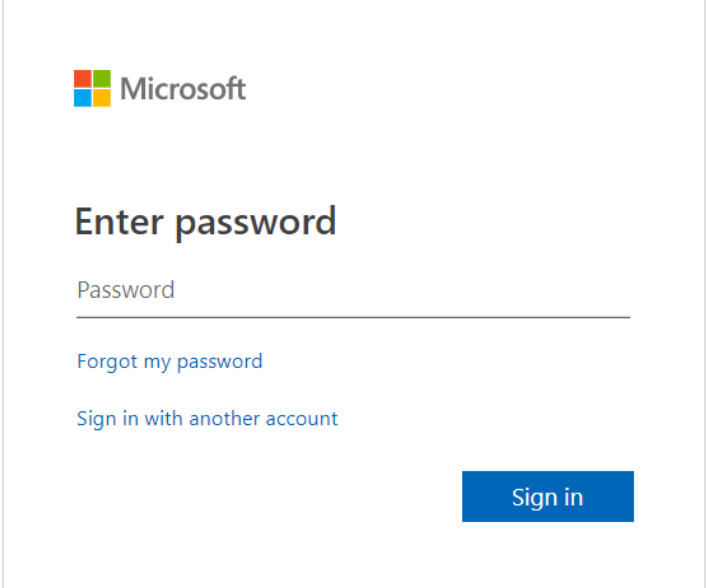
Appendix: Monitoring Service Health

As a best practice, we recommend periodically checking the overall health of your Microsoft 365 environment. This process is particularly useful in instances where content is not backing up.

To monitor the health of services:

STEP 1: Log In to Microsoft 365

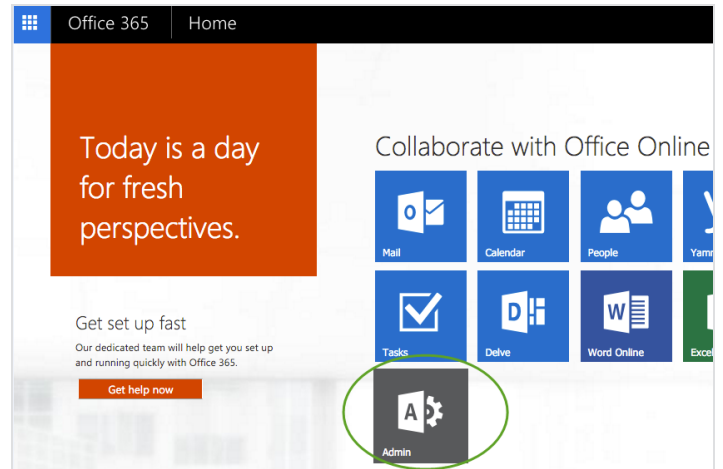Navigate to your Microsoft 365 site and log in as an Administrator. When you are authenticated, you will be presented with the *Microsoft 365 Home Panel*.
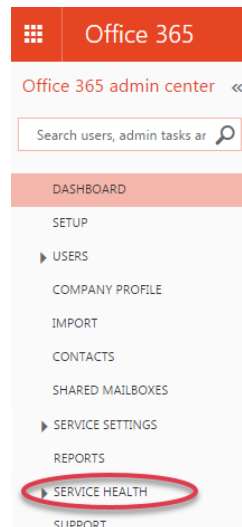
STEP 2: Access the Admin Center

From the *Microsoft 365 Home Panel*, click the **Admin** button. The *Admin Center* page displays.

STEP 3: Find Service Health

In the left-hand navigation menu, click the **Service Health** link. The *Service Health* page displays.

STEP 4: Review the Health Report

In the *Service Health* page, review details of your service.

In this example, the SharePoint service is degraded, as indicated by a yellow status bar.

All other services are healthy, as indicated by the green status bar.

Current health

Exchange	No issues
Identity Service	No issues
Office 365 Portal	No issues
SharePoint	Service degraded ▲

5/15/2015 8:29:30 PM
Current Status: Engineers have completed development of a fix and will be starting deployment over the weekend. It is estimated that this deployment will take several days to completely roll out across the affected environment. User Experience: Affected users are unable to see certain fields when attempting to edit their SharePoint Online user profile. Customer Impact: Customer impact appears to be limited at this time. This issue is only affecting customers who have chosen to switch to Yammer for their social functionality. Incident Start Time: Wednesday, May 13, 2015, at 12:00 AM UTC Preliminary Root Cause: As part of our efforts to improve user experiences, an update was deployed to optimize the visual layout of the user profile page; however, the update caused certain fields to not display properly for customers who have chosen to switch to Yammer for their social functionality. Next Update by: Tuesday, May 19, 2015, at 9:00 PM UTC view details

5/14/2015 9:18:06 PM
Current Status: Engineers have developed a fix to resolve the issue and are now testing it. Due to the complexity of the problem, it is anticipated to take several days to test all aspects of the fix. User Experience: Affected users see a blank page while attempting to view the Organization browser web part via the Silverlight view within SharePoint Online site collections. As a workaround, users can access the affected web parts from the HTML view. Customer Impact: A few customers are reporting that they are experiencing this issue. Incident Start Time: Tuesday, April 28, 2015, at 10:00 PM UTC Preliminary Root Cause: As part of our deployment process, the dynamic-link library required an additional activation step to enable Silverlight viewing capabilities; however, the deployment caused a code issue which affects users' ability to view the Organization browser web part from Silverlight. Next Update by: Tuesday, May 19, 2015, at 10:00 PM UTC view details