FileCloud Online

23.253

Third Party Integrations Settings

17 December, 2025

Table of Contents

Third Party Integrations

Third Party Integrations settings enable you to integrate external tools such as ClamAV, ICAP and reCaptcha with FileCloud. If you are using the Advanced edition, you can set up access to FileCloud through Salesforce or include security information, CASB, and event management (SIEM) software features in FileCloud.

In this section:

Integrating FileCloud with Salesforce

⚠ The Salesforce Plugin reached End-of-Sale (EoS) on June 1, 2025 and is no longer be available for download or new installations.
EoS will be followed by End-of-Life (EoL) on September 1, 2025, at which point support will no longer be generally available for the Salesforce Plugin.
FileCloud will continue to offer technical support to customers with active support contracts for the Salesforce Plugin until the defined EoL date. No replacement product is planned.

Salesforce Integration
FileCloud makes files stored in any on-premises, public or hybrid cloud available within Salesforce.
To configure this function, integrate FileCloud with Salesforce.
Key benefits:

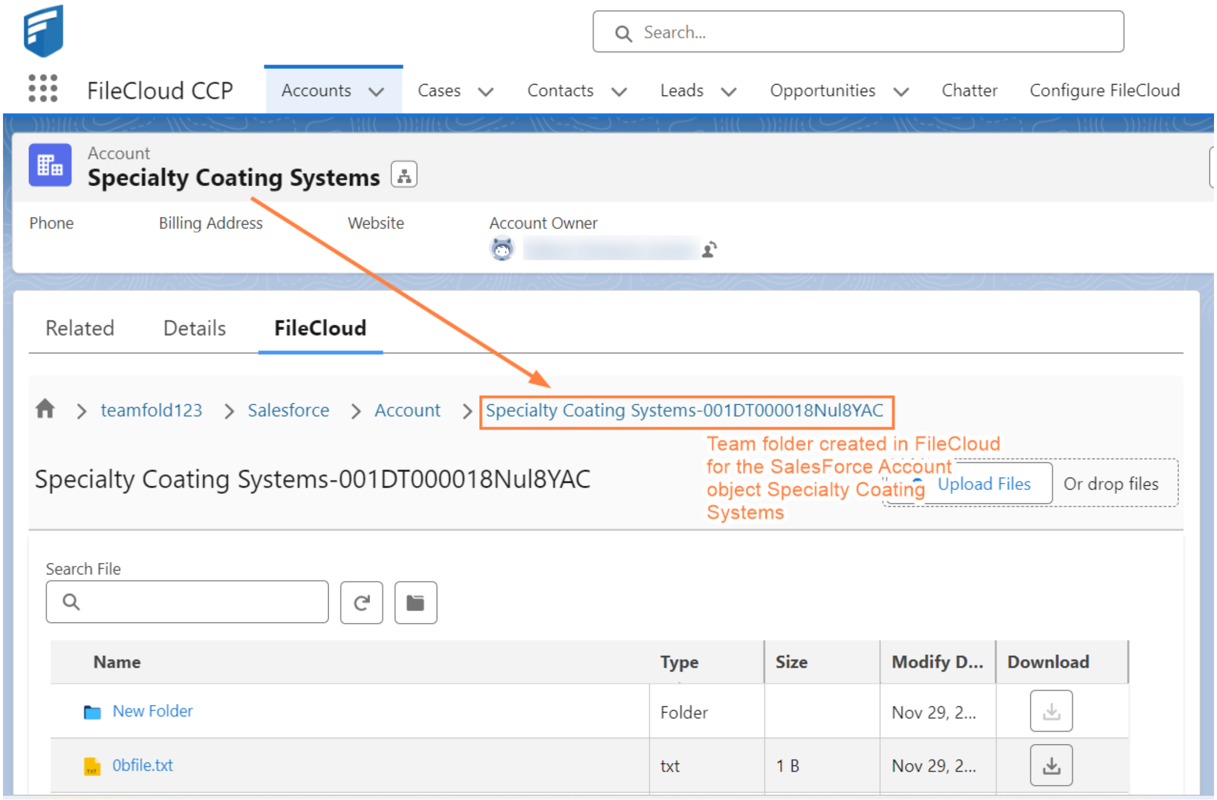
- Upload, download, access and share remote files from within Salesforce.
- Store files on-premises or in the public cloud (Amazon AWS, Microsoft Azure). Access files securely inside Salesforce from anywhere.
- Share files and collaborate with team members, even if they are not Salesforce users.
- Integrate Salesforce with existing file servers and file permissions.
- Get advanced file analytics about who has shared and downloaded files.
- Link FileCloud content to specific Salesforce records.

⚠ **Limitations**

- To be able to integrate FileCloud with Salesforce, you must have the Salesforce component in your license.
- You cannot give External users access to FileCloud's integration with Salesforce.
- Only one Salesforce account and one FileCloud account can be mapped together. Mapping occurs the first time the user logs in to FileCloud through Salesforce. If a user tries to map a second FileCloud account to a Salesforce account, or a second Salesforce account to a FileCloud account, an error message is returned.

To integrate FileCloud with Salesforce, create a Salesforce Team Folder in FileCloud. When you create Salesforce objects (Accounts, Cases, Contacts, etc.), sub-folders are created in the Salesforce Team Folder in FileCloud for each object.

You can access FileCloud in the Salesforce interface to access the an object's Team Folders to perform FileCloud operations on them.



Team folder created in FileCloud for the SalesForce Account object Specialty Coating Systems

Name	Type	Size	Modify D...	Download
New Folder	Folder		Nov 29, 2...	
0bfile.txt	txt	1 B	Nov 29, 2...	

You can configure the Salesforce Team Folders so that only the owner (creator) of the object and users you have designated as managers have access to each object's Team Folder. If you do not add this configuration, anyone with access to the parent Salesforce Team Folder has access to all objects' Team Folders.

Adding FileCloud to Salesforce

Configuring FileCloud with Salesforce

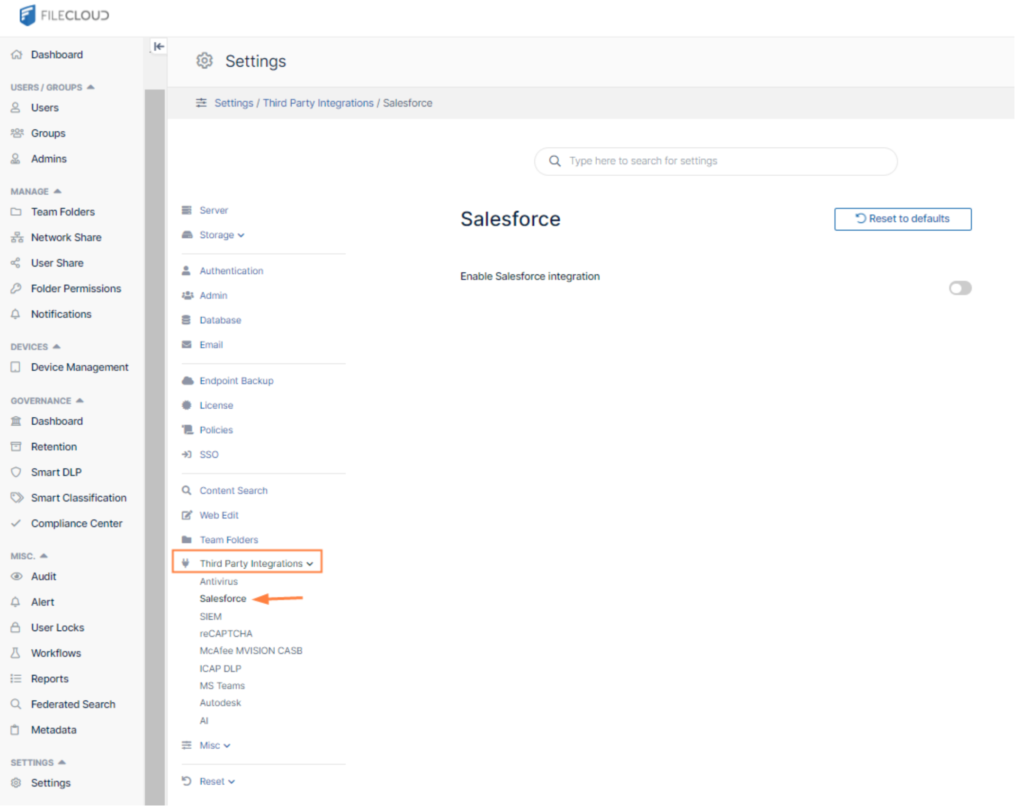
After you install/integrate FileCloud with Salesforce, complete the following:

After you install/integrate FileCloud with Salesforce, complete the following:

1. First Contact FileCloud Support to enable integration with Salesforce in your FileCloud configuration.
   a. Configure Salesforce in FileCloud.
      i. In the FileCloud admin portal, open the **Salesforce** settings page.
      In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.**

      Then, on the **Settings** navigation page, click **Third Party Integrations** .

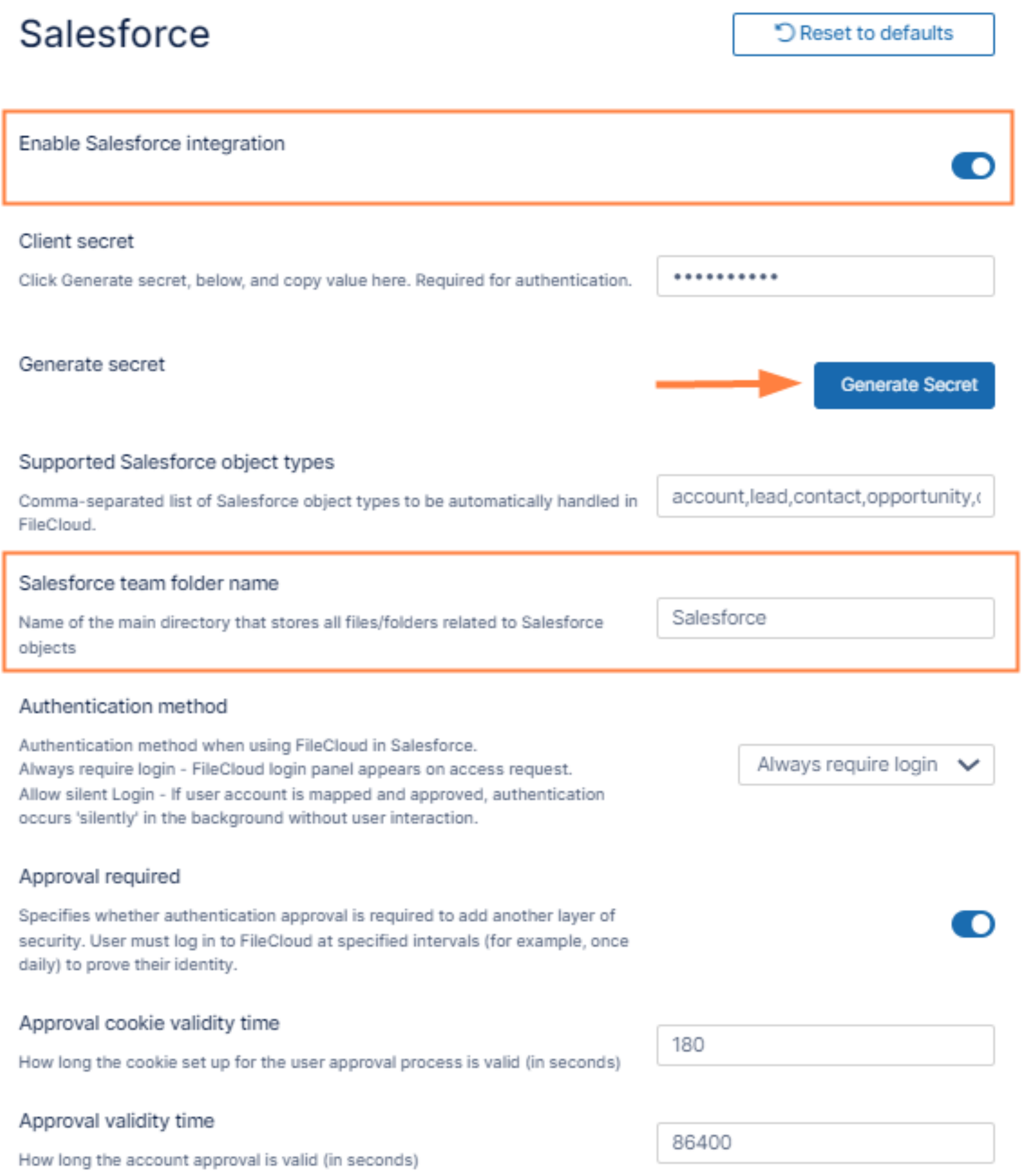
ii. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **Salesforce**, as shown below.



The Salesforce settings page opens.

2. Enable the **Enable Salesforce integration** setting.
3. Click **Generate Secret**, then copy the key and click **Save**.
4. In FileCloud Team Folders, create a Team Folder named **Salesforce**. Sub-folders for your Salesforce objects will automatically be created in this Team Folder. (If you have given the folder another name, but make sure you change the folder name entered in **Salesforce team**

folder name to match it.)



Salesforce

Enable Salesforce integration

Client secret
Click Generate secret, below, and copy value here. Required for authentication. ••••••••••

Generate secret

Supported Salesforce object types
Comma-separated list of Salesforce object types to be automatically handled in FileCloud. account,lead,contact,opportunity,c

Salesforce team folder name
Name of the main directory that stores all files/folders related to Salesforce objects Salesforce

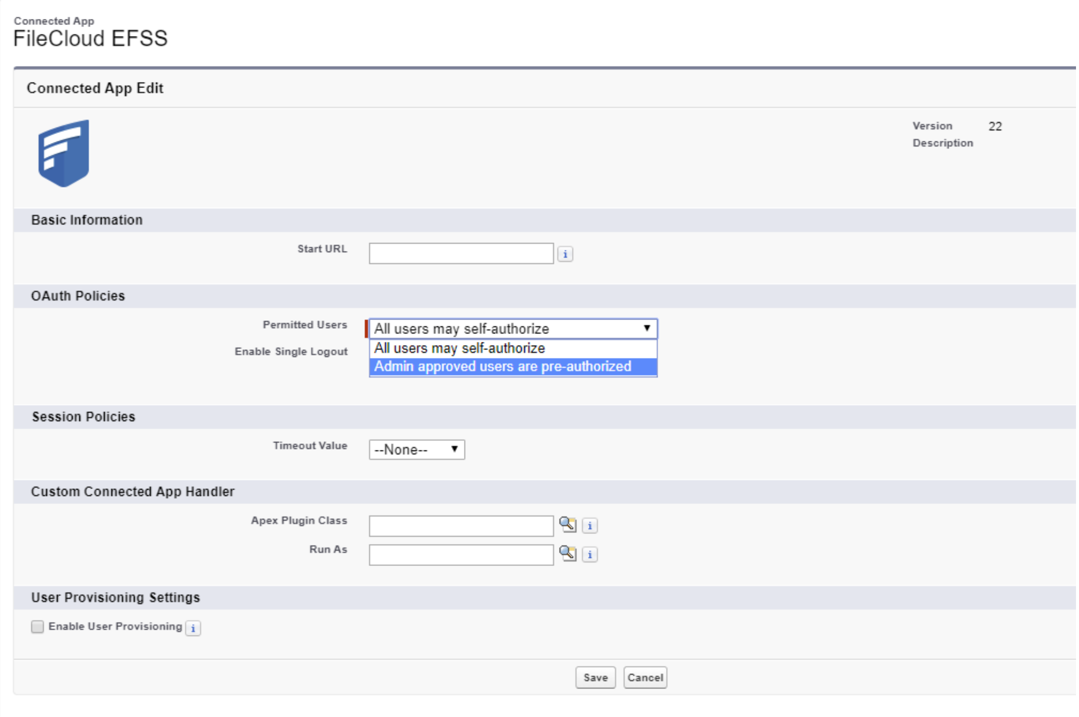
Authentication method
Authentication method when using FileCloud in Salesforce.
Always require login - FileCloud login panel appears on access request.
Allow silent Login - If user account is mapped and approved, authentication occurs 'silently' in the background without user interaction.
Always require login

Approval required
Specifies whether authentication approval is required to add another layer of security. User must log in to FileCloud at specified intervals (for example, once daily) to prove their identity.

Approval cookie validity time
How long the cookie set up for the user approval process is valid (in seconds) 180

Approval validity time
How long the account approval is valid (in seconds) 86400

5. Configure which users have access to FileCloud's integration with Salesforce.
    a. In the Salesforce **App Manager,** click the drop-down list across from **FileCloud EFSS**, and click **Manage**.
    b. Click **Edit Policies**.
    c. Under **OAuth policies**, in the **Permitted Users** drop-down list choose **Admin approved users are pre-authorized**.



Connected App

FileCloud EFSS

Connected App Edit

Version 22

Description

Basic Information

Start URL

OAuth Policies

Permitted Users: All users may self-authorize

Enable Single Logout

All users may self-authorize
Admin approved users are pre-authorized

Session Policies

Timeout Value: --None--

Custom Connected App Handler

Apex Plugin Class

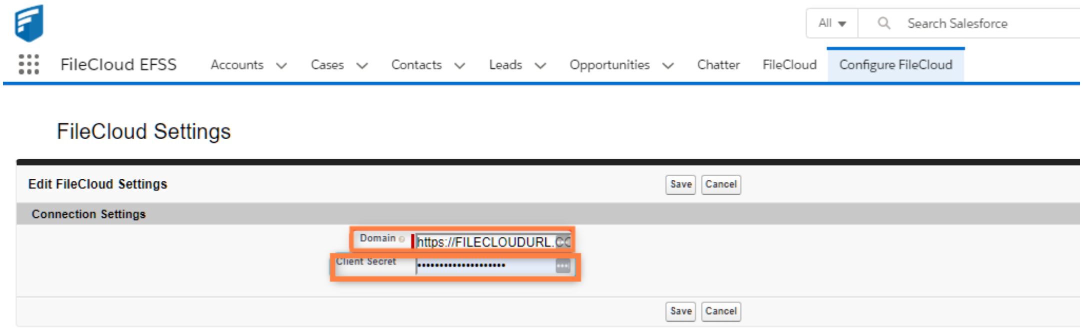
Run As

User Provisioning Settings

□ Enable User Provisioning

d. Click **Save**.

6. Proceed with the configuration of FileCloud within Salesforce.
   a. Access Salesforce and click on the **Configure FileCloud** tab.
   b. On the **Configure FileCloud** tab click edit.
   c. Add your FileCloud URL under **Domain** and paste the Secret Key generated in Step 2 into **Client Secret.**
   d. Click **Save**.



FileCloud Settings

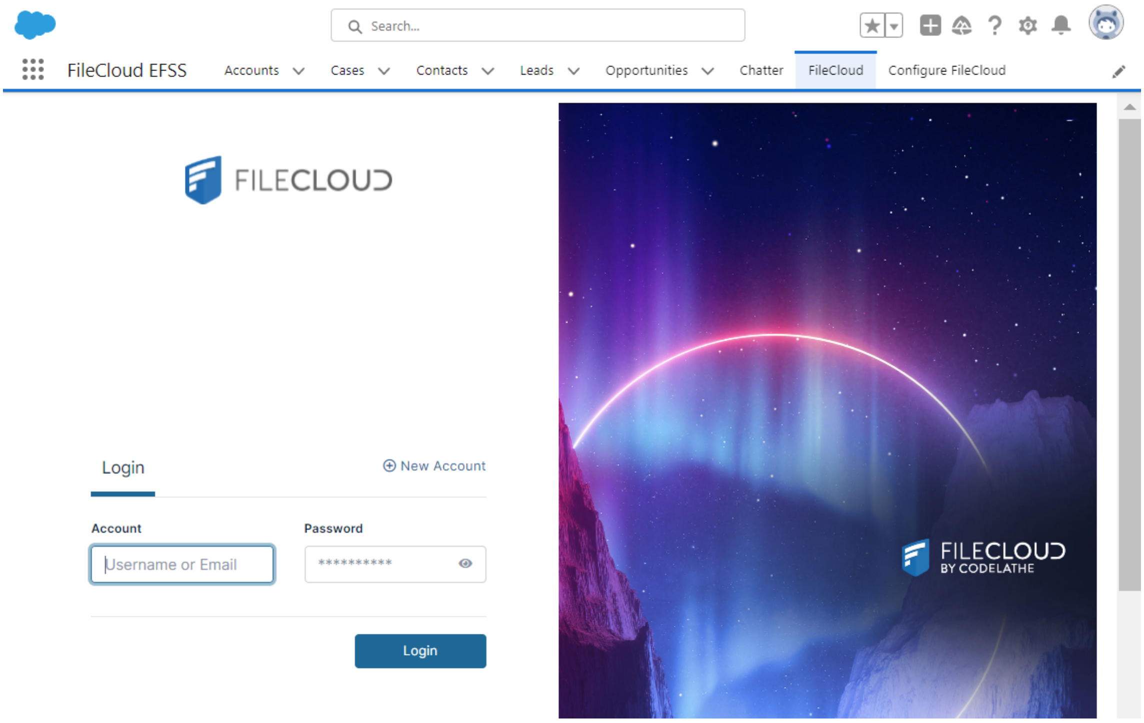
Edit FileCloud Settings

Connection Settings

Domain: https://FILECLOUDURL.CO

Client Secret: ••••••••••••••••••••

7. **Click the FileCloud tab (to the left of Configure FileCloud tab).**
   FileCloud should load and allow you to log in.


Search...
FileCloud EFSS
Accounts
Cases
Contacts
Leads
Opportunities
Chatter
FileCloud
Configure FileCloud
FILECLOUD
Login
New Account
Account
Username or Email
Password
****
Login
FILECLOUD
BY CODELATHE

SIEM Integration

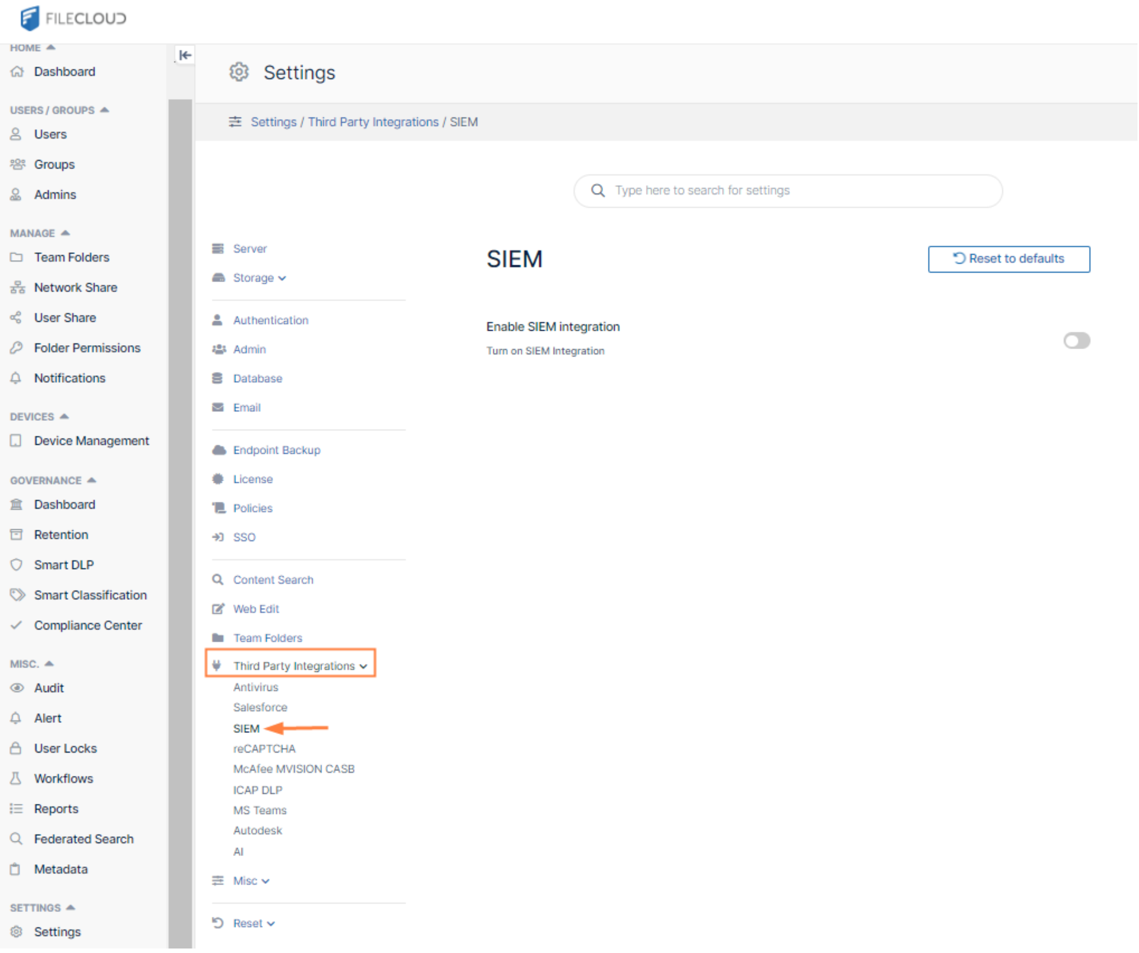
Security information and event management (SIEM) products and services provide analysis of security alerts generated by applications and network hardware.

FileCloud can integrate its system alerts and auditing with external SIEM systems, enabling you to monitor all alerts and potential security issues in one place.

Open the SIEM settings page

To go to the SIEM settings page

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** .
2. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **SIEM**, as shown below.

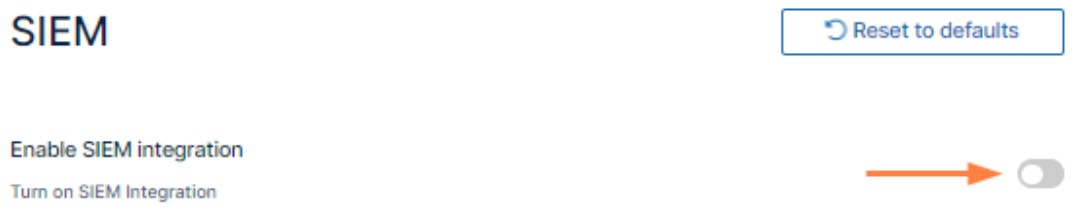


Enable SIEM integration
Turn on SIEM Integration

The **SIEM** settings page opens.

Set up SIEM

1. To activate SIEM integration, click the grayed out **Enable SIEM integration** button.

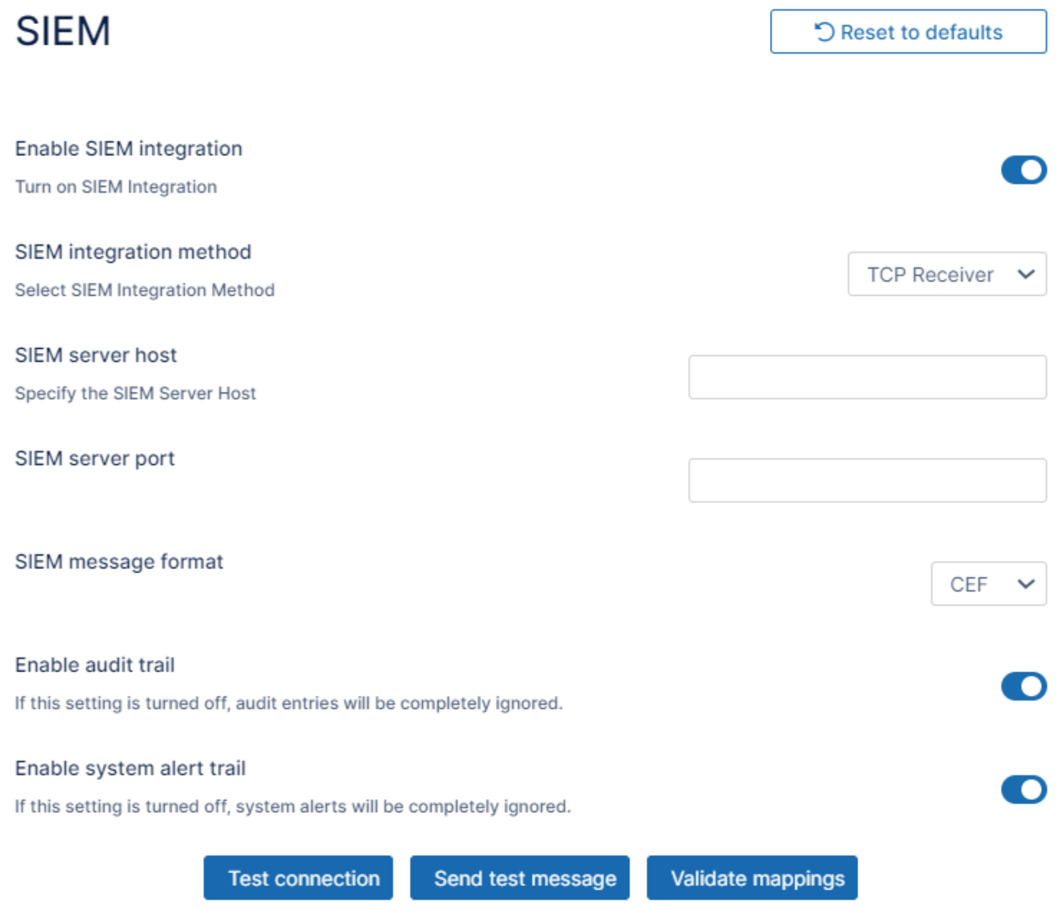


SIEM

Enable SIEM integration

Turn on SIEM Integration

SIEM integration fields appear.



SIEM

Enable SIEM integration

Turn on SIEM Integration

SIEM integration method

Select SIEM Integration Method

TCP Receiver

SIEM server host

Specify the SIEM Server Host

SIEM server port

SIEM message format

CEF

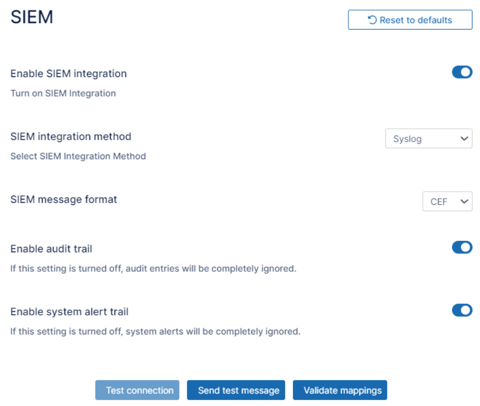
Enable audit trail

If this setting is turned off, audit entries will be completely ignored.

Enable system alert trail

If this setting is turned off, system alerts will be completely ignored.

2. Modify the settings using the information in the following table.

Option	Description
SIEM integration method	Specifies the SIEM Integration method. Following options are available: - **TCP Receiver** - messages are sent to the specified SIEM server endpoint (host and port) via TCP socket connection. - **UDP Receiver** - messages are sent to the specified SIEM server endpoint (host and port) via UDP socket connection. - **Syslog** - messages are written directly to the Syslog, which can be imported by the SIEM server. If you choose **Syslog**, the **SIEM server host** and **SIEM server port** fields are not shown, and the **Test connection** button is disabled.  SIEM Enable SIEM integration Turn on SIEM Integration SIEM integration method: Syslog Select SIEM Integration Method SIEM message format: CEF Enable audit trail If this setting is turned off, audit entries will be completely ignored. Enable system alert trail If this setting is turned off, system alerts will be completely ignored. Reset to defaults Test connection Send test message Validate mappings **Note:** SIEM software providers should specify supported integration methods in the SIEM documentation.
SIEM server host (TCP and UDP integration only)	URL or IP Address of the SIEM server.
SIEM server port (TCP and UDP integration only)	Port exposed by the SIEM Server for the given socket connection.
SIEM message format	Specifies the SIEM Message format. The following formats are available: - **CEF** - Common Event Format - **LEEF** - Log Event Extended Format. If you select **LEEF** the fields **LEEF Version** and **LEEF Message Delimiter** also appear: SIEM message format: LEEF LEEF version: 1.0 LEEF message delimiter: whitespace NOTE: SIEM software provider should specify supported formats in the SIEM documentation.

Option	Description
LEEF version (LEEF Format only)	Specifies the version of the LEEF format message. Available versions: • 1.0 • 2.0
LEEF message delimiter (LEEF Format only)	The delimiter to be used for LEEF messages. The options are **whitespace** and **tab**. Choose the option that is compatible with the SIEM tool you are using.
Enable audit trail	Specifies whether Audit records should be processed and send to the SIEM Server. Please check the Managing SIEM mappings section for more details.
Enable system alert trail	Specifies whether System Alerts generated within FileCloud should be processed and send to the SIEM Server. Please check the Managing SIEM mappings section for more details.
Test connection (TCP and UDP integration only)	Tests connection to the server specified by the Host and Port. **NOTE: All settings have to be saved first. Connection tests are based on the *currently* saved settings.**
Send test message	Sends a test message in the given format (CEF/LEEF) to the SIEM server specified by the Host and Port or saves a test message to the Syslog. **NOTE: All settings have to be saved first. Connection tests are based on the *currently* saved settings.**
Validate mappings	Validates all defined mappings. Please check the Managing SIEM mappings section for more details.

3. Click **Save**.

Managing SIEM Mappings

The biggest challenge when working with the external SIEM servers is to map messages existing in the system in the correct CEF/LEEF format. In order to allow administrators to have full control over how to represent FileCloud's System Alerts and Audit records in the external SIEM system a flexible mapping syntax is supported.

SIEM Mappings - general rules

Create and access SIEM mappings files

Access **WWWROOT.** It is typically located at:

Windows	Linux
c:\xampp\htdocs	**/var/www/html**

Navigate to the following directory:

```
WWWROOT/app/siem/maps
```

It contains the following files:

```
auditmap-sample.php
systemalertsmap-sample.php
```

These files store mappings for audit and system alerts.

Modify the mappings to correspond to your system, and save them as **auditmap.php** and **systemalertsmap.php**.

- **auditmap.php** enables FileCloud to convert audit entries to valid SIEM messages.
- **systemalertsmap.php** enables FileCloud to convert FileCloud's system alerts to valid SIEM messages.

ℹ Mappings are stored in the .php file, so they have to follow all PHP syntax rules as well as internal mappings rules and syntax. To validate all mappings, navigate to **Settings > Third Party Integrations > SIEM** and click on **Validate mappings**.

SIEM mapping format

A sample SIEM mapping is a PHP array entry, which itself is an array. It contains the following fields:

id (required) - identifies the SystemAlert / Audit entry this map refers to.
Note that it can be a string literal that matches the audit operation name or one of the SiemArea values available in FileCloud, an array of values, or a wildcard '' that specifies that the mapping is applied to all audit entries/system alerts.*

prefilter (optional) - A collection of preconditions that an event has to meet in order to be processed and sent to the SIEM system. It is an array of filters, where each filter has the following format:
property => value

where:

- property is a valid property available for the Audit/System Alert record
- value is a value that has to be matched in order to process the Audit / System Alert record, i.e.

Sample System Alert Mappings

```
    'prefilter' => [
        'level' => SysAlert::SYSALERT_LEVEL_MELTDOWN
    ],
```

specifies that only System Alerts with the Meltdown criticality level would be sent to the SIEM server.

map (Required) - specifies the actual mapping between the FileCloud object being processed and the SIEM-formatted message that will be sent to the SIEM server. SIEM object to contain the following four fields:

- eventClass - class of the event in the SIEM system.
- eventName - The name of the event.
- severity - this is a SIEM side severity, which is a number from the 1-10 range.
- extension - a collection (array) of additional key-value pairs that will be stored in the SIEM system (i.e. the user that performed the action, IP address of the request, etc.). The key can be any arbitrary string.

To resolve mappings, provide values in any of the following ways:

- As a literal value (string or number)

  Sample System Alert Mappings

  ```
  'eventClass' => 'authentication',
  'eventName' => 'invalid login',
  'severity' => 3
  ```

- As a property binding that resolves the value with the actual value provided by the FileCloud audit system alert being processed:

  Sample System Alert Mappings

  ```
  'eventClass' => '$siemArea',
  'eventName' => '$description',
  'user' => '$username',
  'filename' => '$request.filename', //Access a field in the request object/array
  'filePath' => '$realpath > $request.path > $notes' //The filePath will be resolved
  to the first non-empty value
  'ip' => '$ip'
  ```

  Properties should appear on the right-hand side of the arrow operator (=>). The property name must be prefixed with a dollar sign ($). Properties can take one of the following values:

  - A standalone value - '$property'

    - An array of values of an object with properties. The following syntax can be used to access any of the values: '$array.field' or '$object.field', for example, '$request.filename'. This can be applied recursively if the internal field is also an array or object, for example, '$response.meta.type'.
    - As a chain of fallback properties ('$property1 > $property2.field > $property3') - the value is resolved to the first non-empty property value. For example, the following syntax is resolved to filename if present or to the $request.fname otherwise: 'fname' => '$filename > $request.fname'. This allows the admin to provide more generic rules.
- As a method call:

  Sample System Alert Mappings

  ```
  'severity' => [[SiemConversionHelper::class, 'getSysAlertSeverity'], ['$level']],
  ```

  NOTE: Users can create and use their own methods here. The first parameter is the PHP callback (class, method name) and the second parameter is the array of values (optional) that is processed by that callback. Parameters can be set to literal values or runtime-resolvable properties as described earlier. In FileCloud 19.2 *getSysAlertSeverity* is the only method available out of the box. It assigns internal System Alerts a severity of 1-10 as required by SIEM integration in the following way:

    - Meltdown: 10
    - Critical: 7
    - Warning: 4
    - Information: 1

Shared properties

Properties listed below can be used in both System Alerts and Audit mappings.

Property	Description	Values
who	Author of the operation	Name of the user or process that has triggered the operation
ip	IP Address	A regular IPv4 address
ts	Operation timestamp	Timestamp

Audit mappings

Audit stores information about actions being performed within the system. Currently, audit stores information about 200+ unique operations being performed within FileCloud. Each Audit record contains some generic information, shared with the System Alerts properties (see Shared Properties, above), common for each audit entry, and some unique properties, stored only for a group of actions.

Shared Audit Properties

Property	Description	Values
request	Request payload	The full request payload provided as a collection of key-value pairs that can be extracted in the mapping. Each operation carries a unique request. The request can be mapped as a full object, and its info will be sent to the SIEM server as a string. For example: `'request' => '$request'`, will be sent as `{"op":"loginguest","userid":"john.doe","password":"xxx"}` Each field can also be sent individually if provided in the mapping: `'loggedUser' => '$request.userid'`, where `userid` is one of the parameters of the request.
response	Response payload	Similar to the request, the response provides a collection of key-value pairs that can be extracted in the mapping or sent as a string. Each operation has a different response, so it is better to use this for dedicated rules. NOTE: Responses are not stored in audit by default, and they have to be enabled in **Admin > Settings > Admin (Audit Settings section) > Audit Logging Level (FULL)**, This is not recommended for production as it may affect performance and usually is not needed for auditing.
notes	Context of the operation	This field provides the most important information about each operation. The content is unique for each operation.
userAgent	The User-Agent that triggered the operation	NOTE: Web browser is used as a generic user-agent for all web browsers.
userName	Name of the user that triggered the operation	
operation	Name of the operation that was triggered	
resultCode	Result of the operation	1 - the operation was performed successfully (for example, login attempt was successful, a file was deleted) 0 - operation failed (for example, login was not possible, a file was not deleted due to invalid permissions)

Property	Description	Values
recordId	A MongoDB id of the audit entry	This is a MongoDB ObjectId
hostname	A name of the host	The name of the current host. This allows SIEM to differentiate tenants.

Operation-specific Audit Properties

Property	Description	Values	Supported operations
auditArea	Provides information about the system area of the operation	Name of the system area	Currently only supported for operations from the following groups: • workflows • retention
serviceId	Additional information about the operation target	Carries additional information about the operations such as the name of the workflow or the id of the retention policy that was updated	Available only when the auditArea field is present
bandwidth	Information about the size of the file	File size in bytes	Available for the following operations: • upload (file upload operation) • downloadfile
realpath	File or folder realpath	FileCloud's original location of the file/folder, for example. /johndoe/document/internal/doc.txt	Available only for retention-related and dlp operations

Property	Description	Values	Supported operations
metadata	A list of non-empty, custom attributes assigned to the file or folder	Any non-empty attributes assigned by the Custom metadata sets as a result of the Smart Classification rule	The following operations are supported: • downloadfilemulti - Download multiple files • downloadfile - Download single file • getaudio - Play audio file • getvideo - Play video file • getfsslideimage - View image file • docconvert - Open/view file • quickshare - Quick share • addusertoshare - Add specific users to share • addgrouptoshare - Add specific groups to share • setallowpublicaccess - Make share public (after sharing only with certain users/ groups)
deviceInfo	Name of the client application	Name of the application, i.e. FileCloud Drive	Any operation that is performed by one of the client apps: Drive or Sync

Sample mappings

The following shows sample mappings for the most common operations:

```
/***************************************** Downloads
*****************************************/
// Download file
$mappings[] = [
    'id' => 'downloadfile',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'FileOperations',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'fname' => '$request.filename > $notes', // $notes is a fallback for
downloadfilemulti operation
```

```
            'filePath' => '$realpath > $request.filePath', // realpath is used for 
downloadfilemulti
            'fsize' => '$bandwidth',
            'cs1' => '$metadata',
            'cs1Label' => 'Metadata assigned to the file'
        ]
    ]
];

/***************************************** Uploads 
*****************************************/
// Upload
$mappings[] = [
    'id' => 'upload',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'FileOperations',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'fname' => '$request.filename', // $notes can be used as well
            'filePath' => '$request.path',
            'fsize' => '$bandwidth'
        ]
    ]
];

/****************************************** Shares 
*****************************************/
// addusertoshare - Adding user to the existing share
$mappings[] = [
    'id' => 'addusertoshare',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Shares',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'filePath' => '$notes',
            'duser' => '$request.userid',
            'cs1' => '$metadata',
            'cs1Label' => 'Metadata assigned to the file'
        ]
    ]
];

// updateshare - updating existing share
```

```
$mappings[] = [
    'id' => 'updateshare',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Shares',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'filePath' => '$request.sharelocation',
            'cs1' => '$metadata',
            'cs1Label' => 'Metadata assigned to the file'
        ]
    ]
];

// setuseraccessforshare - sets user permissions for share
$mappings[] = [
    'id' => 'setuseraccessforshare',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Shares',
        'eventName' => '$operation',
        'severity' => 6, // this can be a potentially risky operation since data
exposure and leakage might happen
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'filePath' => '$notes',
            'duser' => '$request.userid',
            'cs1' => '$metadata',
            'cs1Label' => 'Metadata assigned to the file',
            'cs2' => '$request.shareid',
            'cs2Label' => 'Share Identifier'
        ]
    ]
];

// setallowpublicaccess - happens when a share is mad public
$mappings[] = [
    'id' => 'setallowpublicaccess',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Shares',
        'eventName' => '$operation',
        'severity' => 6, // this can be a potentially risky operation since data
exposure and leakage might happen
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'filePath' => '$notes',
            'ispublic' => '$request.allowpublicaccess', // 1 - public share, 0 -
private share
            'cs1' => '$metadata',
            'cs1Label' => 'Metadata assigned to the file',
            'cs2' => '$request.shareid',
            'cs2Label' => 'Share Identifier'
        ]
    ]
];

/***************************************** Smart DLP
*****************************************/
// DLP Violation
$mappings[] = [
    'id' => 'dlp',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'DLP Violation',
        'eventName' => '$operation',
        'severity' => 6,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'filePath' => '$realpath',
            'msg' => '$notes.message',
            'shareTargetEmail' => '$notes.shareTargetEmail',
            'cs1' => '$metadata',
            'cs1Label' => 'Metadata assigned to the file',
            'cs3' => '$request.op', // operation that triggered the violation /
$notes.action can be uses as well for a less granular info: DOWNLOAD / SHARE / LOGIN
            'cs3Label' => 'DLP Violation trigger',
            // Additional information can be grabbed from the request object
            'cs4' => '$notes.violatedRule', // DLP rule that was violated
            'cs4Label' => 'DLP Violation rule'
        ]
    ]
];

/************************************ Smart Classification
************************************/
// Smart Classification - apply match action
$mappings[] = [
    'id' => 'ccsapplymatchaction',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'CCE match',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'msg' => '$notes',
            'filePath' => '$realpath',
            'cs5' => '$svcid',
            'cs5Label' => 'Content classification rule name'
        ]
    ]
];

/********************************************* Login
*****************************************/
//Failed login attempt
$mappings[] = [
    'id' => 'loginguest',
    'prefilter' => [
        //List of conditions that audit entry has to met in order to be processed (or
filtered out if excluded option is there)
        'resultCode' => '0', //incidents only
        'exclude' => false // optional 'include' is used by default
    ],
    'map' => [
        'eventClass' => 'login',
        'eventName' => 'Invalid login attempt',
        'severity' => 2,
        'extension' => [
            'user' => '$userName',
            'ip' => '$ip',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
        ]
    ]
];


//Failed SSO login attempt
$mappings[] = [
    'id' => 'samlsso',
    'prefilter' => [
        //List of conditions that audit entry has to met in order to be processed (or
filtered out if excluded option is there)
        'resultCode' => '0', //incidents only
        'exclude' => false // optional 'include' is used by default
    ],
    'map' => [
        'eventClass' => 'login',
        'eventName' => 'Invalid SSO login attempt',
        'severity' => 2,
        'extension' => [
            'user' => '$userName',
            'ip' => '$ip',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
        ]
    ]
```

```
];

//Successful SSO login attempt
$mappings[] = [
    'id' => 'samlsso',
    'prefilter' => [
        //List of conditions that audit entry has to met in order to be processed (or
filtered out if excluded option is there)
        'resultCode' => '1',
        'exclude' => false // optional 'include' is used by default
    ],
    'map' => [
        'eventClass' => 'login',
        'eventName' => 'Successfull SSO login attempt',
        'severity' => 2,
        'extension' => [
            'user' => '$userName',
            'ip' => '$ip',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
        ]
    ]
];

 /************************************* AV - Virus removed
***********************************/
// When AV finds and removes the file containing a Virus (i.e. ICAP AV)
$mappings[] = [
    'id' => 'virusremoved',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'virusremoved',
        'eventName' => 'Virus Removed',
        'severity' => 8,
        'extension' => [
            'user' => '$userName',
            'userAgent' => '$userAgent',
            'ip' => '$ip',
            'fname' => '$request.filename',
            'filePath' => '$request.path',
            'notes' => '$notes'
        ]
    ]
];

/******************************* Group management
*****************************************/

// Group rename
$mappings[] = [
    'id' => 'updategroup',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Groups',
        'eventName' => '$operation',
        'severity' => 6,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'msg' => '$notes'
        ]
    ]
];

$mappings[] = [
    'id' => 'addmembertogroup',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Groups',
        'eventName' => '$operation',
        'severity' => 5,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'duser' => '$request.userid',
            'msg' => '$notes'
        ]
    ]
];

$mappings[] = [
    'id' => 'deletememberfromgroup',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Groups',
        'eventName' => '$operation',
        'severity' => 5,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'duser' => '$request.userid',
            'msg' => '$notes'
        ]
    ]
];

/******************************** User management
******************************************/

$mappings[] = [
    'id' => 'adduser',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Users',
        'eventName' => '$operation',
        'severity' => 5,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'duser' => '$request.username', // name of the user that has been added
            'msg' => '$notes' // More info about the user
        ]
    ]
];

// Admin status change
$mappings[] = [
    'id' => 'setadminstatus',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Users',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'duser' => '$request.profile',
            'msg' => '$request.adminstatus'
        ]
    ]
];

// User password changed by admin
$mappings[] = [
    'id' => 'setuserpassword',
    'prefilter' => [],
    'map' => [
        'eventClass' => 'Users',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName', // Admin who performed the operation
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'duser' => '$request.profile' // User whose password has been changed
        ]
    ]
];



/****************************************** Generic
****************************************/
// A generic map for all events
```

```
$mappings[] = [
    'id' => '*',
    'prefilter' => [],
    'map' => [
        'eventClass' => '$operation',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'suser' => '$userName',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
            'requestClientApplication' => '$userAgent',
            'src' => '$ip',
            'msg' => '$notes',
            'fname' => '$request.filename',
            'filePath' => '$realpath > $request.path > $request.filepath',
            'duser' => '$request.userid'
        ]
    ]
];
```

System Alert mappings

FileCloud allows admins to create mappings for System Alerts generated by the system due to unexpected or unwanted behaviors. System Alert mappings contain properties that can be sent to the SIEM server or logged in the syslog for further processing.

Supported properties

Property	Description	Values

siemArea	System area where the alert was raised	One of the following values:
		`SiemArea::INFECTED_FILE`
		`SiemArea::INVALID_FILE_TYPE`
		`SiemArea::AV_CHECK_FAILED`
		`SiemArea::UNHANDLED_EXCEPTION`
		`SiemArea::SYSTEM_ERROR`
		`SiemArea::DISK_SPACE_EXCEEDED`
		`SiemArea::INDEX_DB_FAILURE`
		`SiemArea::RMC_INVALID_POLICY`
		`SiemArea::SEND_EMAIL_FAILED`
		`SiemArea::BACKGROUNDING_FAILED`
		`SiemArea::METADATA_HEALTH_CHECK`
		`SiemArea::WORKFLOW`
		`SiemArea::ZIP_BACKUP_FAILURE`
		`SiemArea::SIEM_SERVER_CONNECTION`
		`SiemArea::DLP_SHARE_KILL`

level	System alert critical level	One of the following values:
		`SysAlert::SYSALERT_LEVEL_MELTDOWN`
		`SysAlert::SYSALERT_LEVEL_CRITICAL`
		`SysAlert::SYSALERT_LEVEL_WARNING`
		`SysAlert::SYSALERT_LEVEL_INFORMATION`

type	Type of system alert	One of the following values:
		`SysAlert::SYSALERT_TYPE_DLP_SHARE_KILL_FAILED`
		`SysAlert::SYSALERT_TYPE_DLP_SHARE_KILLED`
		`SysAlert::SYSALERT_TYPE_CODE_CONFIGURATION_ERRROR`
		`SysAlert::SYSALERT_TYPE_CODE_AV_FAILURE`
		`SysAlert::SYSALERT_TYPE_CODE_SIGNATURE_FAILURE`
		`SysAlert::SYSALERT_TYPE_CODE_EXCEPTION`
		`SysAlert::SYSALERT_TYPE_CODE_ERROR`
		`SysAlert::SYSALERT_TYPE_QUOTA_EXCEEDED`

description	Alert description	

Property	Description	Values
notes	Alert notes	
username	The user whose actions raised the alert	
alertContext	Additional information, related to the alert	Various contexts, depending on the Alert. For example: **file** - filename for the File version deletion operation **filePath** - file location for the Infected file **fileName** - file name for the Infected file

Sample mappings

Sample System Alert Mappings

```
//Report all meltdowns
$mappings[] = [
    'id' => '*', //Wildcard denotes all Alerts
    'prefilter' => [
        'level' => SysAlert::SYSALERT_LEVEL_MELTDOWN
    ],
    'map' => [
        'eventClass' => '$siemArea',
        'eventName' => '$description',
        'severity' => 10,
        'extension' => [
            'user' => '$username',
            'ip' => '$ip'
        ]
    ]
];

//AV system alert - infected file found
$mappings[] = [
    'id' => SiemArea::INFECTED_FILE,
    'map' => [
        'eventClass' => 'System Error',
        'eventName' => '$description',
        'severity' => [[SiemConversionHelper::class, 'getSysAlertSeverity'],
['$level']],
        'extension' => [
            'user' => '$username',
            'ip' => '$ip',
            'path' => '$alertContext.filePath',
            'file' => '$alertContext.fileName'
        ]
    ]
];

//Type mismatch report
$mappings[] = [
    'id' => SiemArea::INVALID_FILE_TYPE,
    'map' => [
        'eventClass' => 'System Error',
        'eventName' => '$description',
        'severity' => [[SiemConversionHelper::class, 'getSysAlertSeverity'],
['$level']],
        'extension' => [
            'user' => '$username',
            'ip' => '$ip',
            'path' => '$alertContext.file'
        ]
    ]
];
```

SIEM Integration with Splunk Enterprise

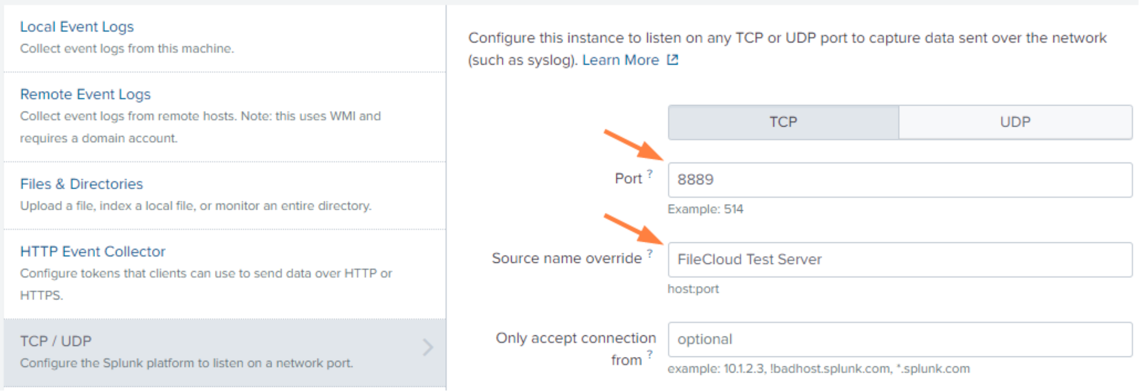
You can set up FileCloud's SIEM Integration feature with your Splunk server to receive audit logs and send event alerts to the administrator's email.

Splunk Server Configuration

To configure Splunk server to receive data inputs from FileCloud through a designated TCP port and a specified source type, create a TCP Data Input entry that specifies the port that receives messages from the FileCloud and create a custom source type for FileCloud..

1. Log in to Splunk.
2. Click **Add Data**.
3. In the **TCP** row, click **Add new**.
   An **Add Data** wizard opens.

4. In the **Select Source** screen, in **Port**, enter the port that will receive messages from FileCloud. In **Source name override**, enter a name for the FileCloud server.



Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

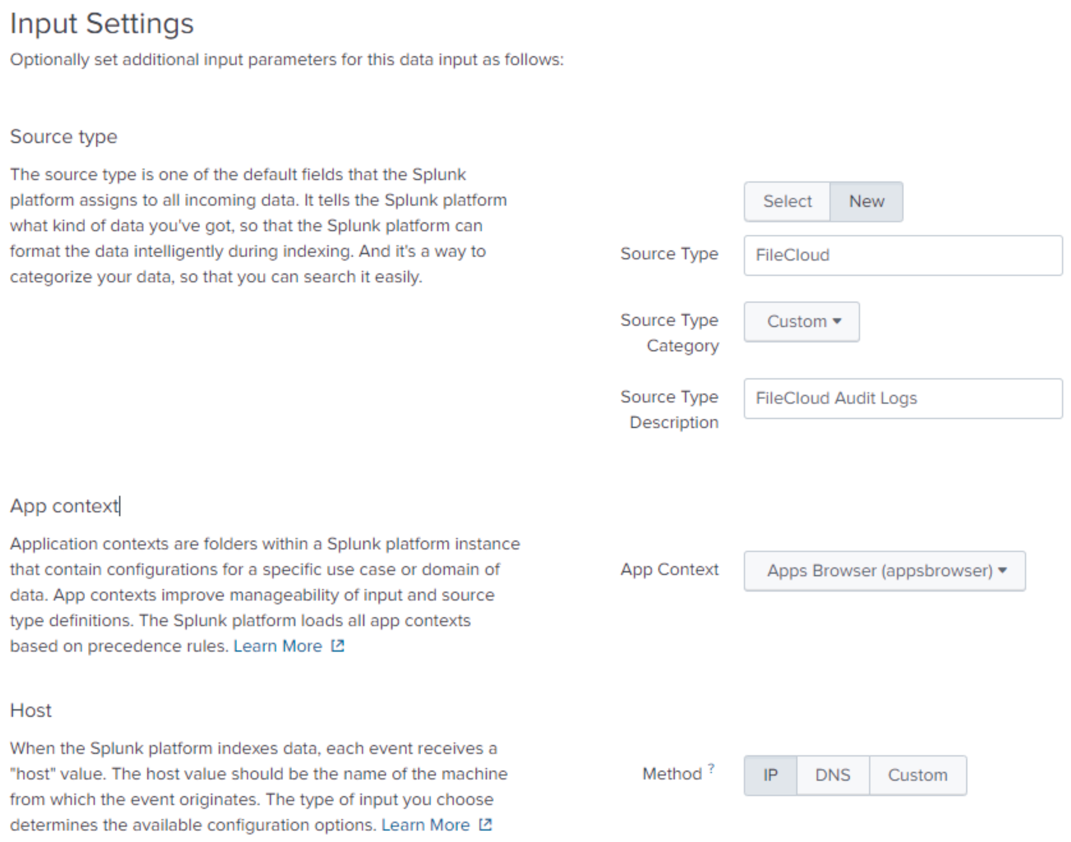
Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

Port: 8889
Example: 514

Source name override: FileCloud Test Server
host:port

Only accept connection from: optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

5. Go to the next screen.
6. In the **Input Settings** screen**,** enter the following settings:
   - Click **New**.
   - In **Source Type**,enter **FileCloud**.
   - In **Source Type Category**, choose **Custom**.
   - In **Source Type Description**, enter **FileCloud Audit Logs**.
   - In **App Context**, choose **Apps Browser (appsbrowser)**.
   - For **Host**, choose one of the following:
     - **IP** - Uses IP address of the host where the event originated.
     - **DNS** - Uses Doman Name Services (DNS) to convert the IP address to a host name that events are tagged with.
     - **Custom** - When you click this option, a **Host field value** field appears. This option uses the value you enter in **Host field value** to tag events.
   - Set **Index** to **Default**.



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Source Type: FileCloud

Source Type Category: Custom ▾

Source Type Description: FileCloud Audit Logs

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Apps Browser (appsbrowser) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

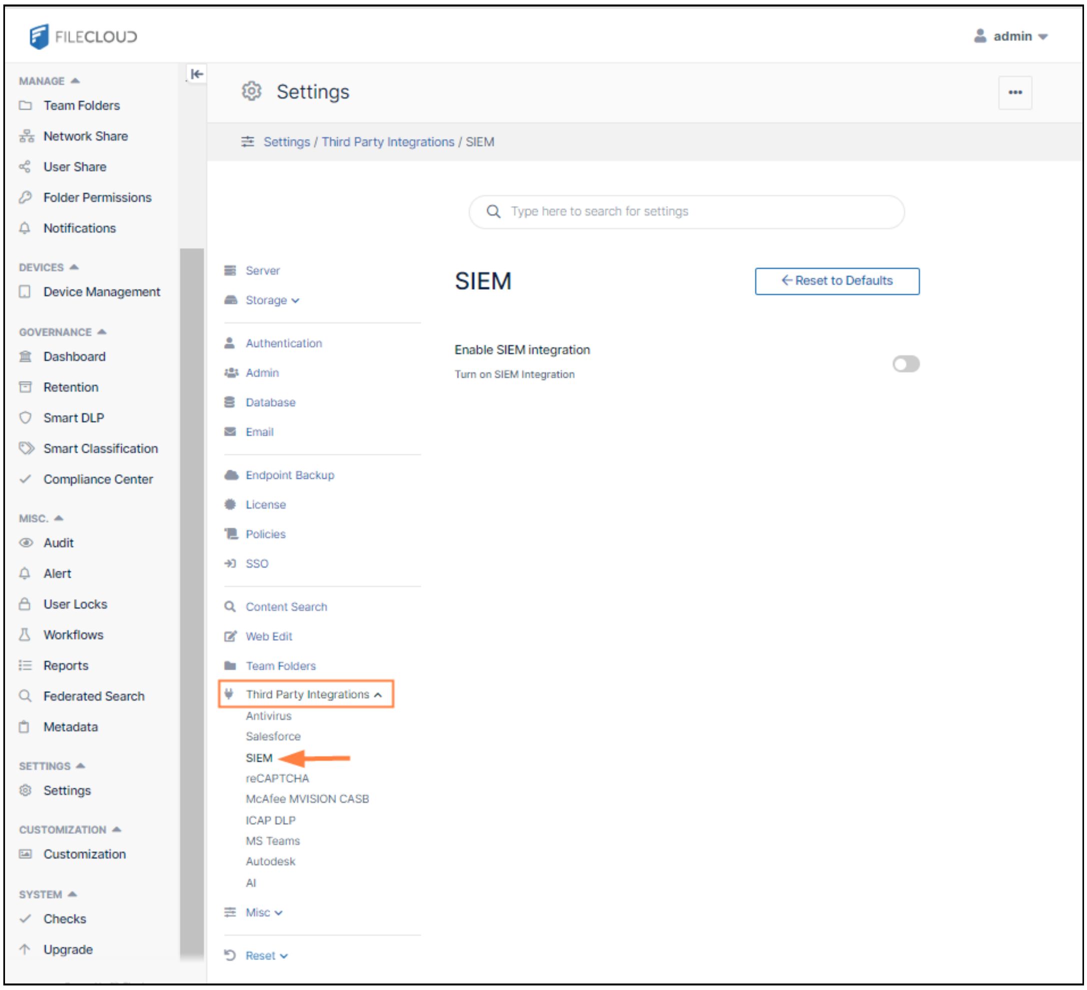
Method ?: IP | DNS | Custom

7. Go to the next screen in the wizard, **Review**, and check your settings.
8. Click next to complete your TCP Data Input entry configuration.

Setting up FileCloud to connect to the Splunk Server

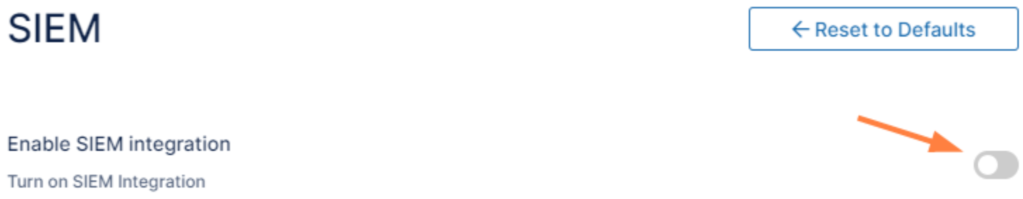
Once the TCP Data Input entry is configured in Splunk, configure the SIEM Integration settings in FileCloud.

1. Go to the **SIEM** settings page.
   To go to the SIEM settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** .
   b. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **SIEM**, as shown below.



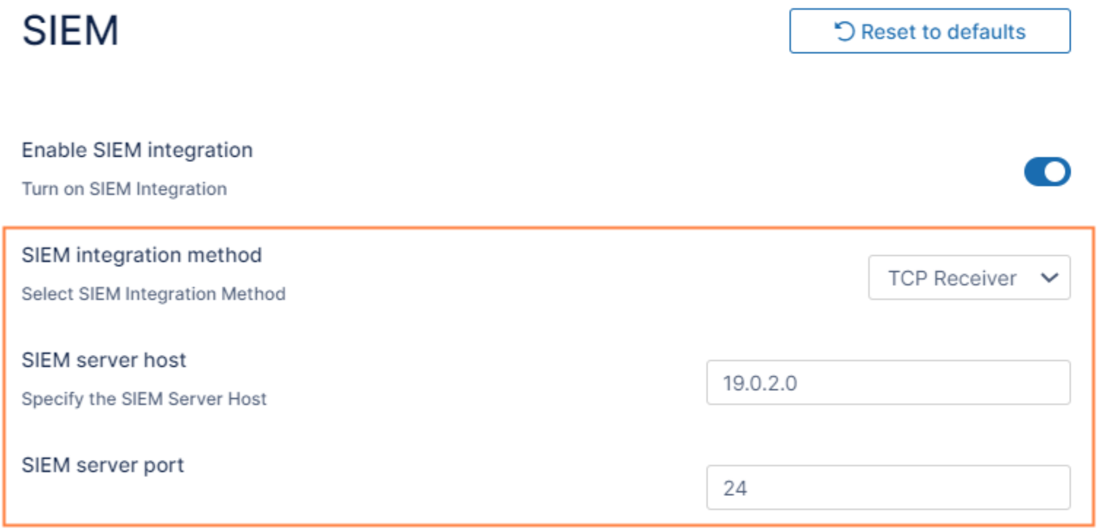
The **SIEM** settings page opens.

2. To activate SIEM integration, click the grayed out **Enable SIEM integration** button.



SIEM integration fields appear.

3. In **SIEM Integration Method**, choose **TCP Receiver**.
In **SIEM Server Host**, enter the IP address or the hostname of the Splunk server.
In **SIEM Server Port**, you may enter a unique port that is not currently used by the Splunk server for sending messages.
For the other settings, see SIEM Integration (see page 8).



SIEM

Reset to defaults

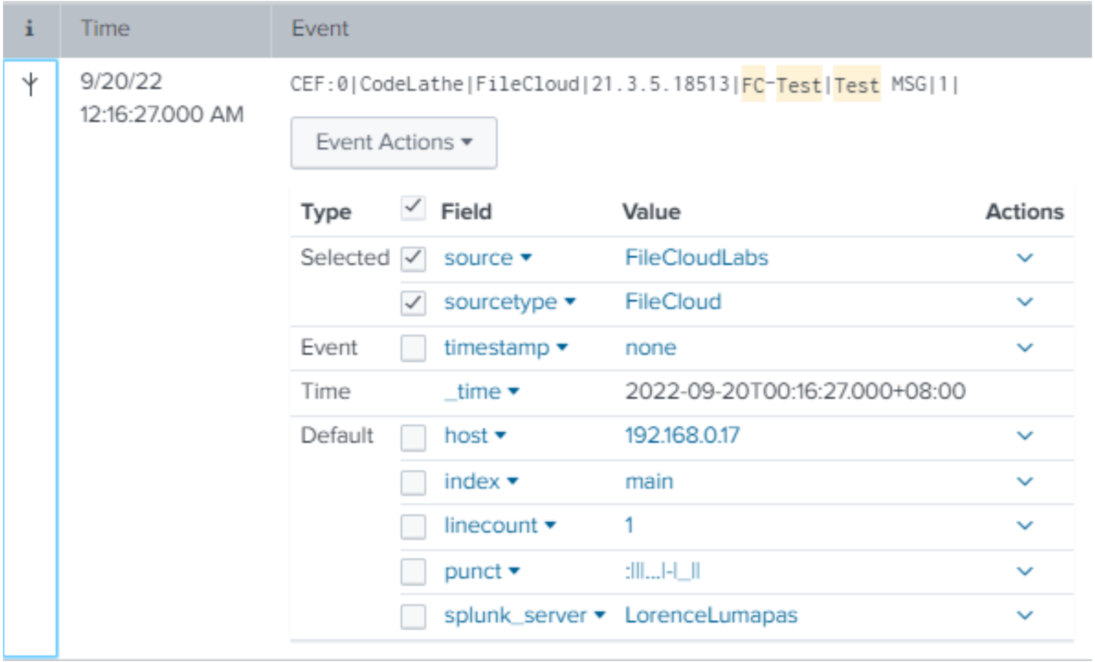
Enable SIEM integration
Turn on SIEM Integration

SIEM integration method
Select SIEM Integration Method
TCP Receiver

SIEM server host
Specify the SIEM Server Host
19.0.2.0

SIEM server port
24

4. Validate your configuration by clicking the **Test Connection**, **Send Test Message**, and **Validate Mappings** buttons. The **Send Test Message** button should send a test connection to the Splunk server, for example:



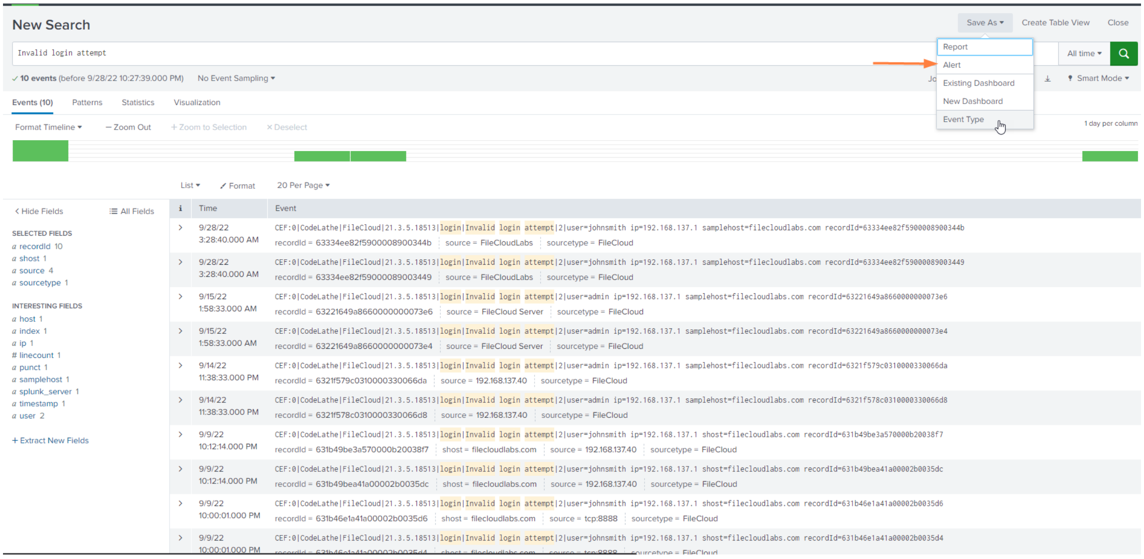
i	Time	Event
	9/20/22 12:16:27.000 AM	CEF:0|CodeLathe|FileCloud|21.3.5.18513|FC-Test|Test MSG|1|

Type	☑	Field	Value	Actions
Selected	☑	source ▾	FileCloudLabs	⌄
	☑	sourcetype ▾	FileCloud	⌄
Event	☐	timestamp ▾	none	⌄
Time		_time ▾	2022-09-20T00:16:27.000+08:00	
Default	☐	host ▾	192.168.0.17	⌄
	☐	index ▾	main	⌄
	☐	linecount ▾	1	⌄
	☐	punct ▾	:|||...|-|_||	⌄
	☐	splunk_server ▾	LorenceLumapas	⌄

NOTE: Additional fields can be added by modifying the mappings from the **auditmap.php** and **systemalertsmap.php** files in FileCloud. See Managing SIEM Mappings (see page 11) for more information.

Setting up FileCloud event alerts in Splunk

1. Run a search for the event type from the Splunk Search screen and confirm that you get the expected data from the results.
2. In the upper-right corner, in the **Save As** drop-down list choose **Alert**:



`Invalid login attempt`

✓ 10 events (before 9/28/22 10:27:39.000 PM)

Time	Event

9/28/22 3:28:40.000 AM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=johnsmith ip=192.168.137.1 samplehost=filecloudlabs.com recordId=63334ee82f5900008900344b`
	recordId = 63334ee82f5900008900344b source = FileCloudLabs sourcetype = FileCloud

9/28/22 3:28:40.000 AM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=johnsmith ip=192.168.137.1 samplehost=filecloudlabs.com recordId=63334ee82f59000089003449`
	recordId = 63334ee82f59000089003449 source = FileCloudLabs sourcetype = FileCloud

9/15/22 1:58:33.000 AM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=admin ip=192.168.137.1 samplehost=filecloudlabs.com recordId=63221649a8660000000073e6`
	recordId = 63221649a8660000000073e6 source = FileCloud Server sourcetype = FileCloud

9/15/22 1:58:33.000 AM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=admin ip=192.168.137.1 samplehost=filecloudlabs.com recordId=63221649a8660000000073e4`
	recordId = 63221649a8660000000073e4 source = FileCloud Server sourcetype = FileCloud

9/14/22 11:38:33.000 PM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=admin ip=192.168.137.1 samplehost=filecloudlabs.com recordId=6321f579c0310000330066da`
	recordId = 6321f579c0310000330066da source = 192.168.137.40 sourcetype = FileCloud

9/14/22 11:38:33.000 PM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=admin ip=192.168.137.1 samplehost=filecloudlabs.com recordId=6321f578c0310000330066d8`
	recordId = 6321f578c0310000330066d8 source = 192.168.137.40 sourcetype = FileCloud

9/9/22 10:12:14.000 PM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=johnsmith ip=192.168.137.1 shost=filecloudlabs.com recordId=631b49be3a570000b20038f7`
	recordId = 631b49be3a570000b20038f7 shost = filecloudlabs.com source = 192.168.137.40 sourcetype = FileCloud

9/9/22 10:12:14.000 PM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=johnsmith ip=192.168.137.1 shost=filecloudlabs.com recordId=631b49bea41a00002b0035dc`
	recordId = 631b49bea41a00002b0035dc shost = filecloudlabs.com source = 192.168.137.40 sourcetype = FileCloud

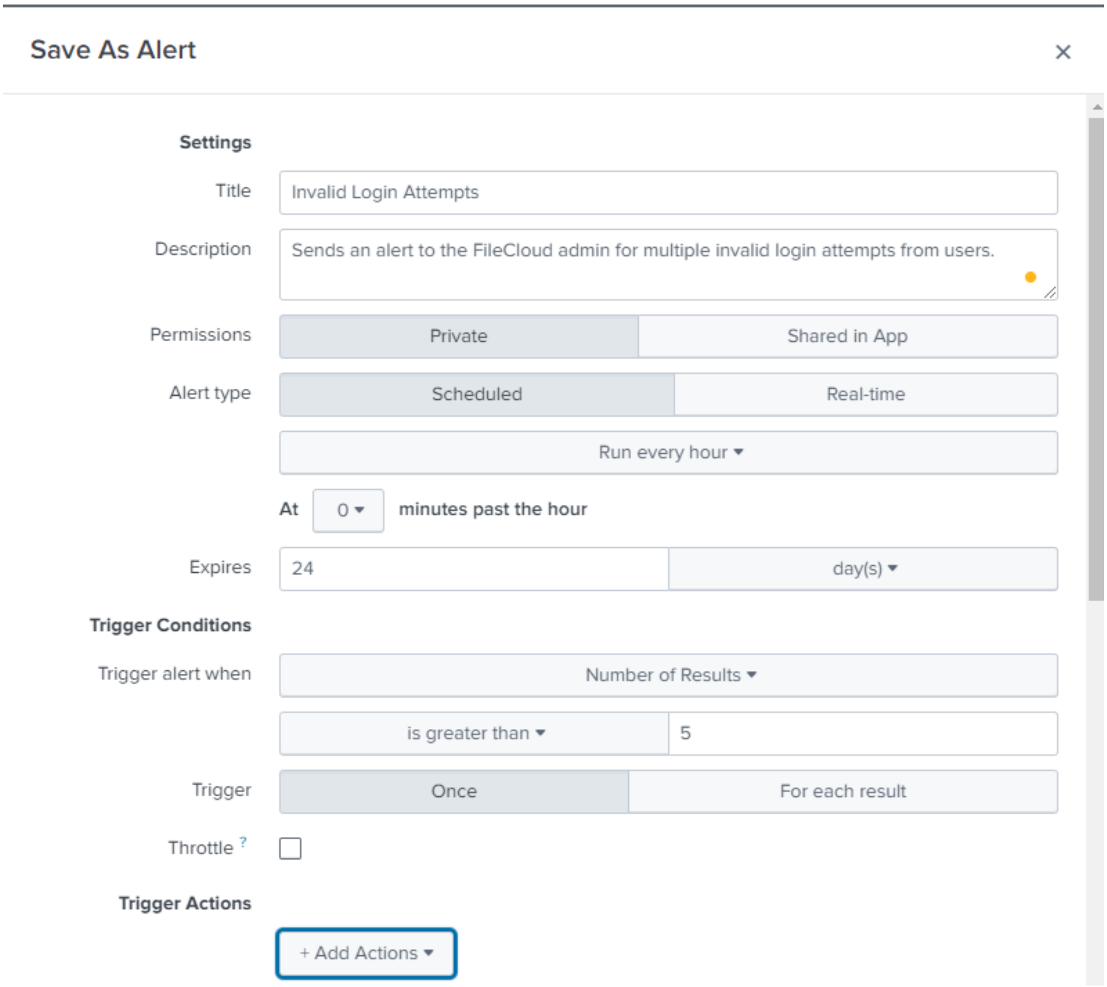
9/9/22 10:00:01.000 PM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=johnsmith ip=192.168.137.1 shost=filecloudlabs.com recordId=631b46e1a41a00002b0035d6`
	recordId = 631b46e1a41a00002b0035d6 shost = filecloudlabs.com source = tcp:8888 sourcetype = FileCloud

9/9/22 10:00:01.000 PM	`CEF:0|CodeLathe|FileCloud|21.3.5.18513|login|Invalid login attempt|2|user=johnsmith ip=192.168.137.1 shost=filecloudlabs.com recordId=631b46e1a41a00002b0035d4`
	recordId = 631b46e1a41a00002b0035d4 shost = filecloudlabs.com source = tcp:8888 sourcetype = FileCloud

The **Save As Alert** dialog box opens.

3. Fill in the fields. Enter the following fields as indicated:
   - **Alert Type -** Choose **Scheduled** to search for alert events on a schedule. Choose **Real-time** to trigger an alert when an alert event occurs.
     If you choose **Scheduled**, also choose a frequency in the drop-list below it.
   - **Trigger alert when** - Choose **Number of Results**, and enter a number.
   - In **Trigger Actions**, click **Add Actions**, and choose **Send email** as the action that is triggered by an alert.
   - In **To**, enter the recipient of the email.

4. Click **Save**.



Save As Alert

Settings

Title: Invalid Login Attempts

Description: Sends an alert to the FileCloud admin for multiple invalid login attempts from users.

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Expires: 24 day(s)

Trigger Conditions

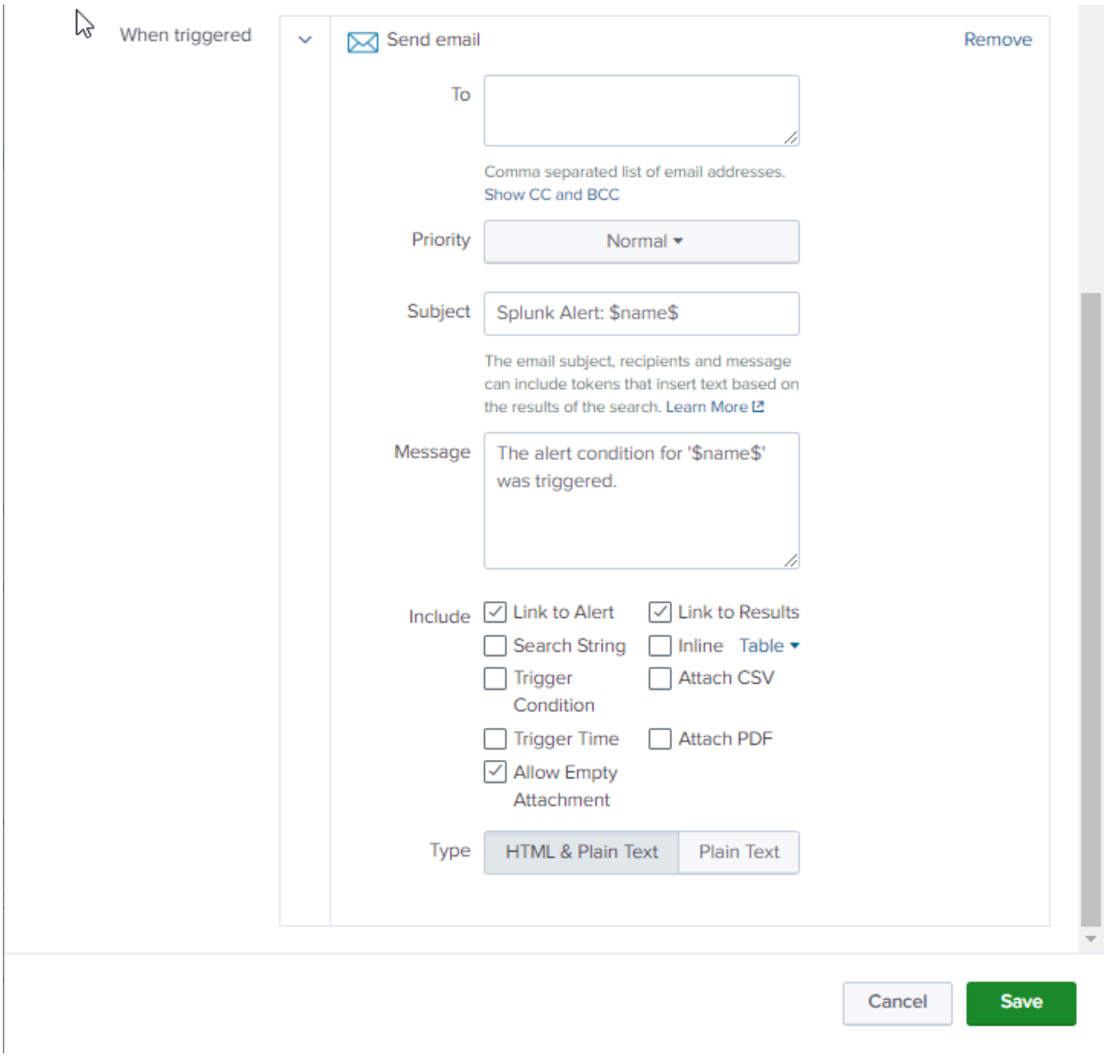
Trigger alert when: Number of Results

is greater than 5

Trigger: Once | For each result

Throttle ? □

Trigger Actions



When triggered

Send email

Remove

To

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal ▾

Subject: Splunk Alert: $name$

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for '$name$' was triggered.

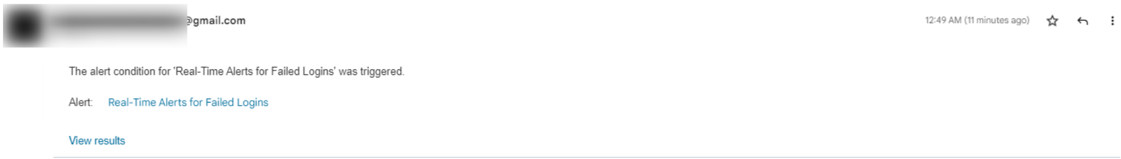
Include
☑ Link to Alert
☑ Link to Results
☐ Search String
☐ Inline Table ▾
☐ Trigger Condition
☐ Attach CSV
☐ Trigger Time
☐ Attach PDF
☑ Allow Empty Attachment

Type: HTML & Plain Text | Plain Text

Cancel

Save

5. Test to confirm that alerts are received by the mail in **To**, above. Below is an example of an email alert sent from Splunk.



[redacted]@gmail.com

12:49 AM (11 minutes ago)

The alert condition for 'Real-Time Alerts for Failed Logins' was triggered.

Alert: Real-Time Alerts for Failed Logins

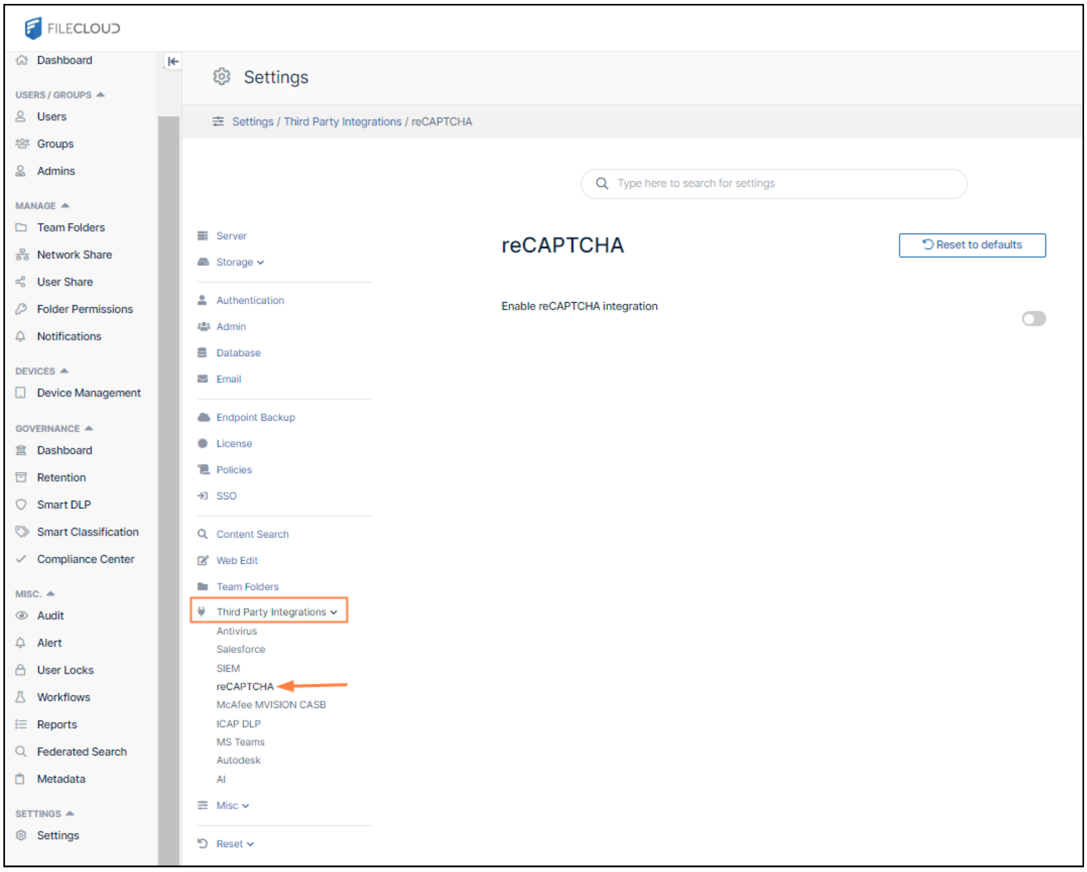
View results

reCaptcha Settings

FileCloud supports reCaptcha v2. When you enable reCaptcha integration, reCaptcha is applied when users log in to FileCloud and when they access a password-protected file or folder share.

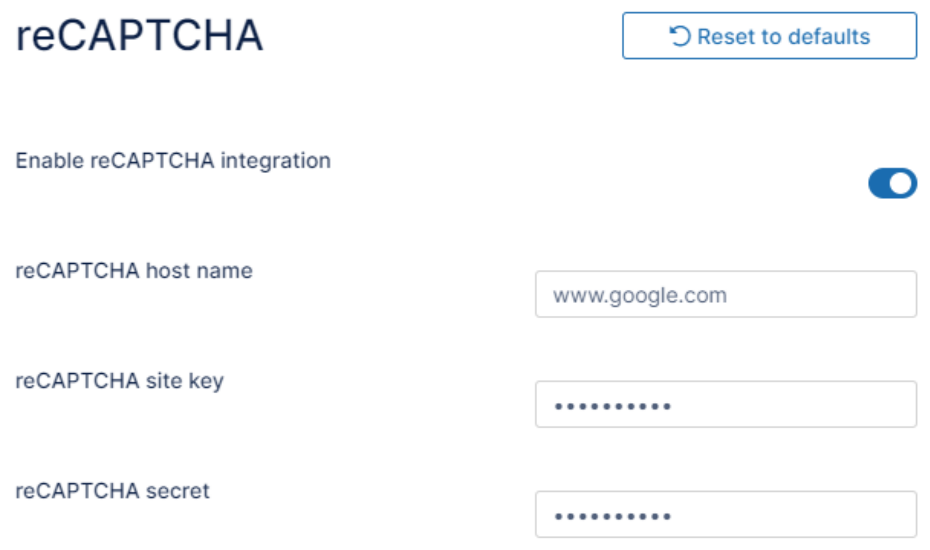
To configure reCaptcha:

1. Register your site at https://developers.google.com/recaptcha and get a key pair.
2. Open the ReCAPTCHA settings page.
   To go to the reCAPTCHA settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** .
   b. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **reCAPTCHA**, as shown below.



   The **reCAPTCHA** settings page opens.
   Open the **reCAPTCHA** settings page.
3. Enable the setting **Enable reCAPTCHA integration**.
   Additional reCAPTCHA settings appear.

4. If you plan to use a non-default reCAPTCHA site, enter the site hostname into **reCAPTCHA Host Name** in the format www.hostname.com.
   Note: If you are in a location that cannot access **www.google.com**, enter **www.recaptcha.net** (https://developers.google.com/recaptcha/docs/faq#can-i-use-recaptcha-globally)
5. Enter your key pair into **reCAPTCHA Site Key** and **reCAPTCHA Secret**.



reCAPTCHA

Enable reCAPTCHA integration

reCAPTCHA host name: www.google.com

reCAPTCHA site key: ••••••••••

reCAPTCHA secret: ••••••••••

6. Click **Save**.

SSO API: Configure Import of SSO Groups and Users

> Beginning in FileCloud 23.251, admins can import FileCloud groups and users from Okta, Google, and Azure SSO providers. In the future, importing groups and users from additional providers may be available.

Systems that authenticate users with Okta, Google, or Azure SSO can also import the users and their groups from the SSO provider. This requires integration of FileCloud and the SSO provider, separate from the configuration of the SSO provider(s) on the SSO settings page.

To set up the integration of the SSO provider and FileCloud for group and user import:

- Step 1: Set up FileCloud to integrate with the SSO provider for group/user import in the SSO provider's application.
- Step 2: Set up the SSO provider to integrate with FileCloud for group/user import in the FileCloud admin portal.

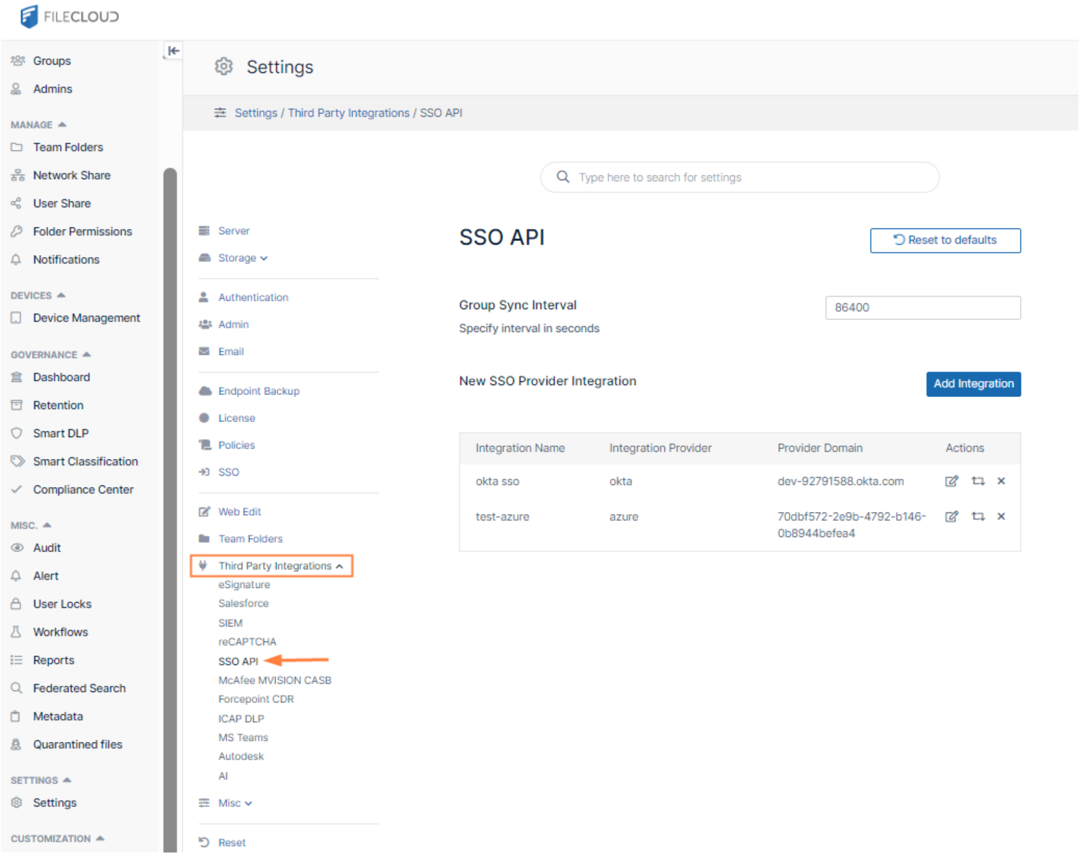
Step 1: Set up FileCloud to integrate with the SSO provider in the SSO provider's application:

Currently, the SSO providers available for integration with FileCloud for group/user import are Okta, Google, and Azure.

- Okta: Set Up FileCloud Integration for SSO Group/User Import (see page 53)
- Azure: Set up FileCloud Integration for SSO Group/User Import (see page 63)
- Google: Set up FileCloud Integration for SSO Group/User Import (see page 71).

Step 2: Set up the SSO provider for importing groups and users into FileCloud:

1. Open the **SSO API** page.
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** .
   b. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **SSO API**, as shown below.



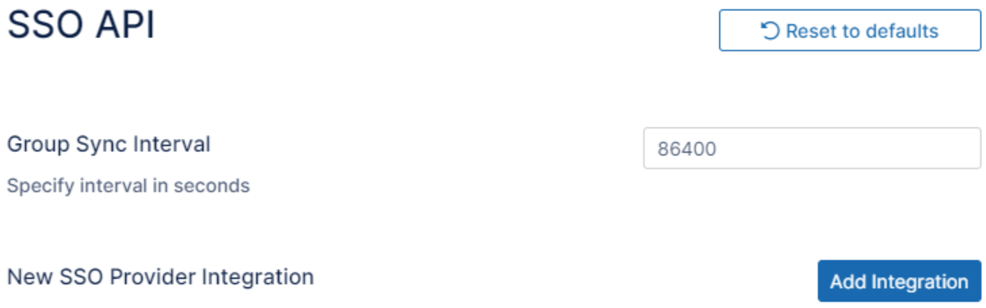
SSO API

Group Sync Interval 86400
Specify interval in seconds

New SSO Provider Integration

Integration Name	Integration Provider	Provider Domain	Actions
okta sso	okta	dev-92791588.okta.com	
test-azure	azure	70dbf572-2e9b-4792-b146-0b8944befea4	

The SSO API settings page opens.

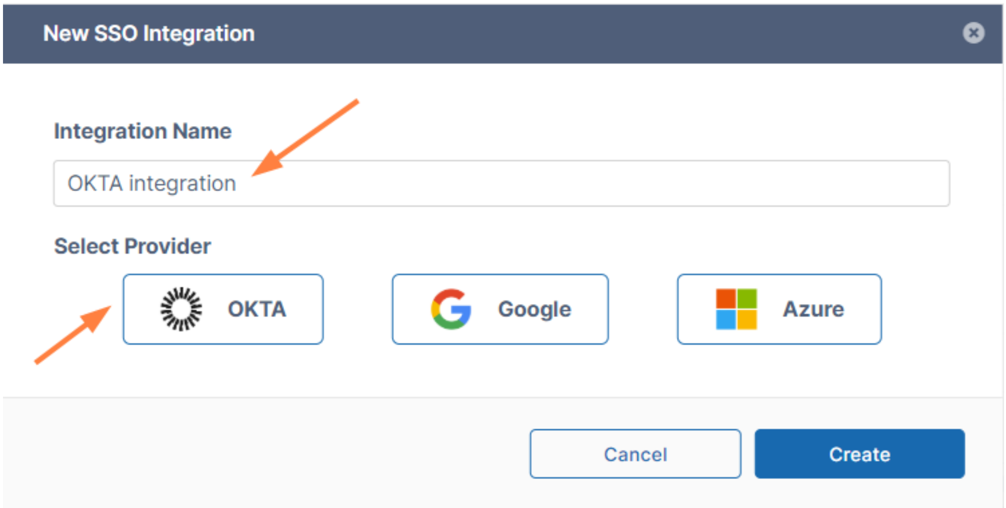


SSO API

Group Sync Interval 86400
Specify interval in seconds

New SSO Provider Integration

2. By default, the group sync is set to occur every 86400 seconds (once a day).
   To change how often group sync occurs, modify the value of **Group Sync Interval**. Specify the value in seconds.
3. Click **Add Integration**.
   The **New SSO Integration** dialog box opens.
4. Enter a name for the integration and click the button for the corresponding SSO provider:


New SSO Integration

Integration Name

OKTA integration

Select Provider

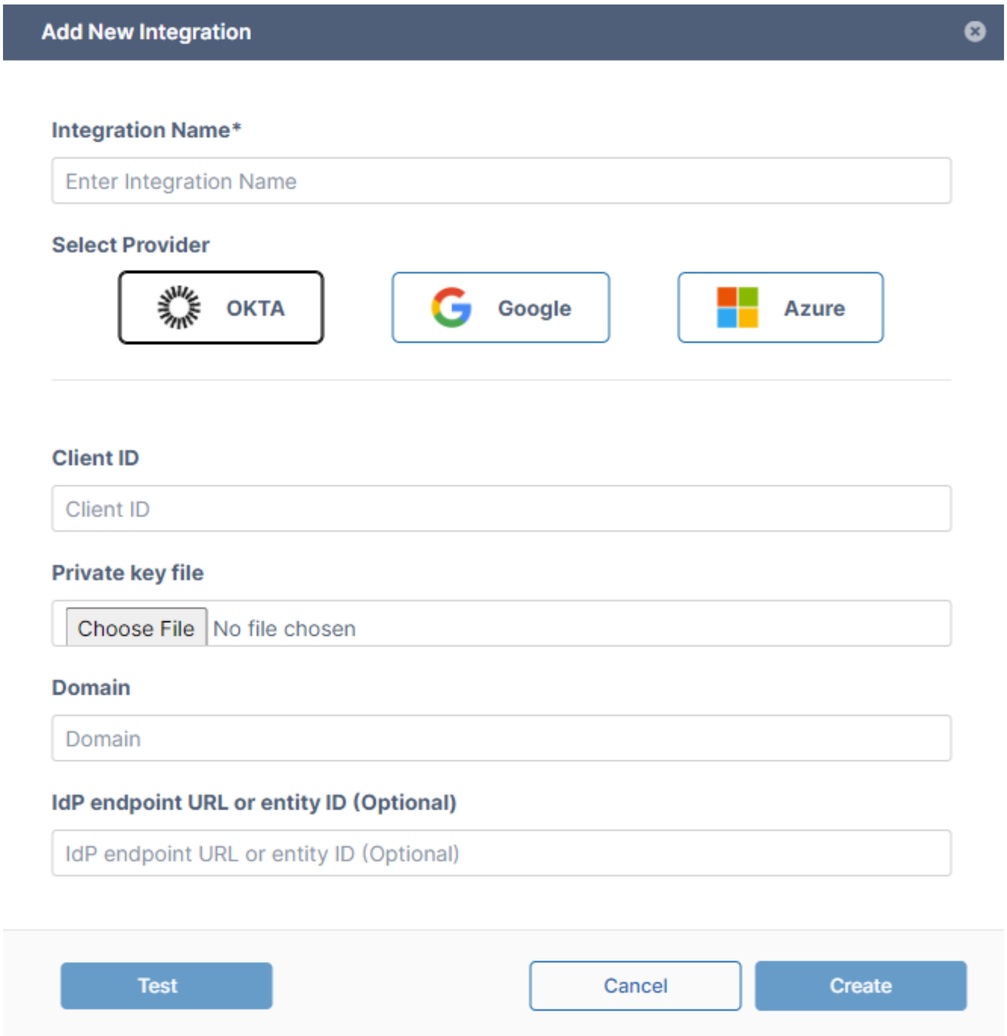
The dialog box expands.

Enter the integration values for the specific SSO provider:

OKTA

Enter integration values for Okta

1. When you click the **OKTA** button under **Select Provider**, the following settings appear. Enter the value for each as indicated in the table below.



Integration Name

You may enter any name.

Client ID

Enter the Client ID created for you when you set up the integration with FileCloud in Okta. You may copy it from the Okta Admin Console's listing for the application and paste it into the field. The following image shows where it appears in the Okta Admin Console.

Private key file

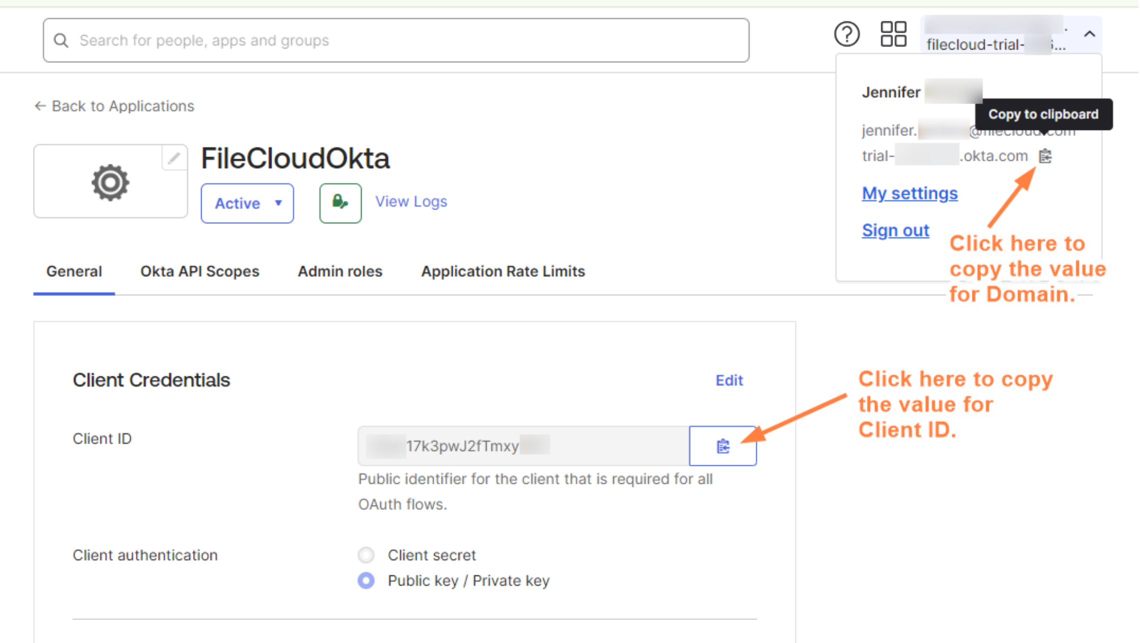
Choose the .pem file that you saved your private key in. You may have created the file and saved it when you were setting up the integration with FileCloud in Okta.

Domain

Enter the domain that Okta created for your user in Okta when you set up the integration with FileCloud in Okta. You may copy it from the Okta Admin Console's User drop-down box and paste it into the field. The following image shows where it appears in the Okta Admin Console.

IdP endpoint URL or entity ID (Optional)

Enter if you are using multiple IdP's. Enter the value in the field **IdP endpoint URL or entity ID** from the FileCloud SSO settings.



Search for people, apps and groups

filecloud-trial-[redacted]...

Jennifer [redacted]

jennifer.[redacted]@filecloud.com

trial-[redacted].okta.com

Copy to clipboard

My settings

Sign out

Click here to copy the value for Domain.

← Back to Applications

FileCloudOkta

Active ▾ View Logs

General | Okta API Scopes | Admin roles | Application Rate Limits

Client Credentials Edit

Client ID [redacted]17k3pwJ2fTmxy[redacted]

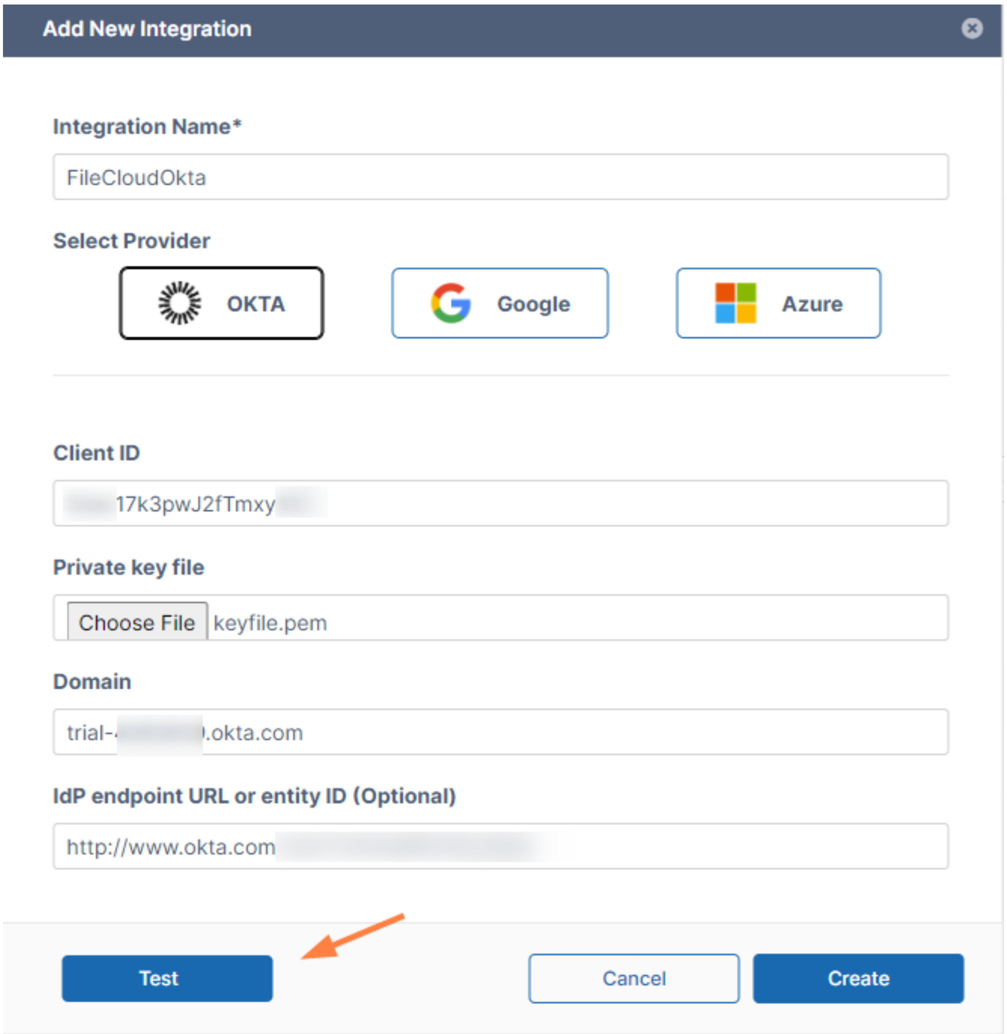
Public identifier for the client that is required for all OAuth flows.

Client authentication ○ Client secret ● Public key / Private key

Click here to copy the value for Client ID.

Location of values for FileCloud fields in Okta Admin Console

2. Once you have filled in the fields, click **Test** to make sure your integration works.



Add New Integration

Integration Name*

FileCloudOkta

Select Provider

Client ID

[redacted]17k3pwJ2fTmxy[redacted]

Private key file

Choose File keyfile.pem

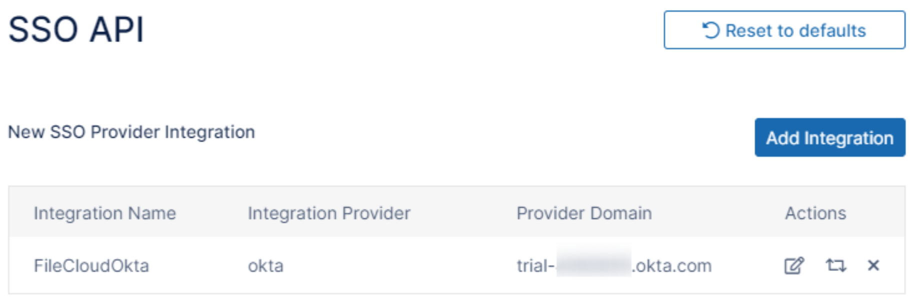
Domain

trial-[redacted].okta.com

IdP endpoint URL or entity ID (Optional)

http://www.okta.com[redacted]

3. If the test is successful, click **Create**.
   The integration is added to the list of SSO integrations:



SSO API

New SSO Provider Integration

Integration Name	Integration Provider	Provider Domain	Actions
FileCloudOkta	okta	trial-[redacted].okta.com	✎ ⇄ ×

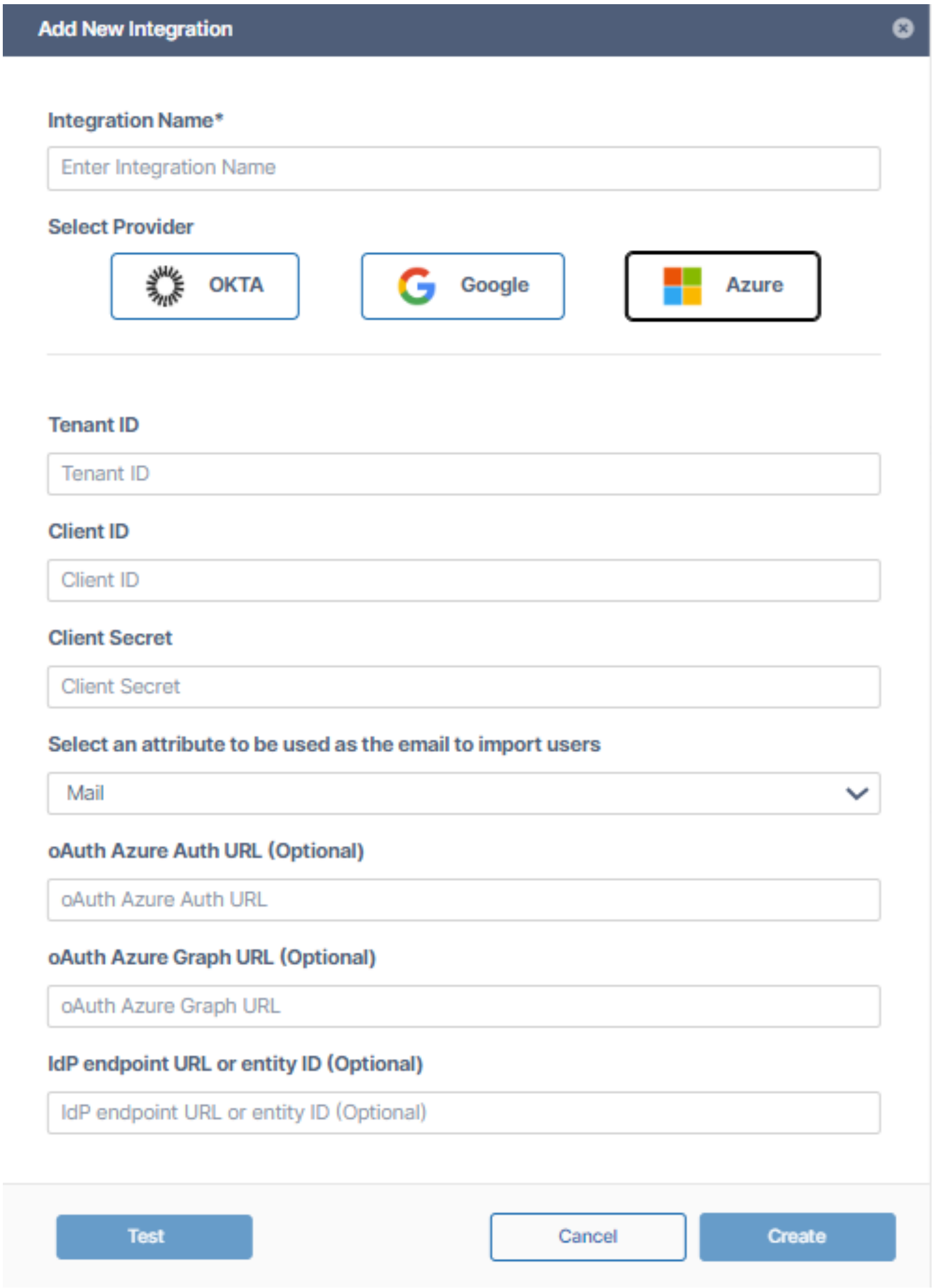
4. By default built-in OKTA groups are not listed when you import groups from OKTA.

   For help listing built-in OKTA groups, please Contact FileCloud Support.
   OKTA groups:

Azure

Enter integration values for Azure

1. When you click the **Azure** button under **Select Provider**, the following settings appear. Enter the value for each as indicated in the table below.



Add New Integration

Integration Name*

Enter Integration Name

Select Provider

OKTA | Google | Azure

Tenant ID

Tenant ID

Client ID

Client ID

Client Secret

Client Secret

Select an attribute to be used as the email to import users

Mail

oAuth Azure Auth URL (Optional)

oAuth Azure Auth URL

oAuth Azure Graph URL (Optional)

oAuth Azure Graph URL

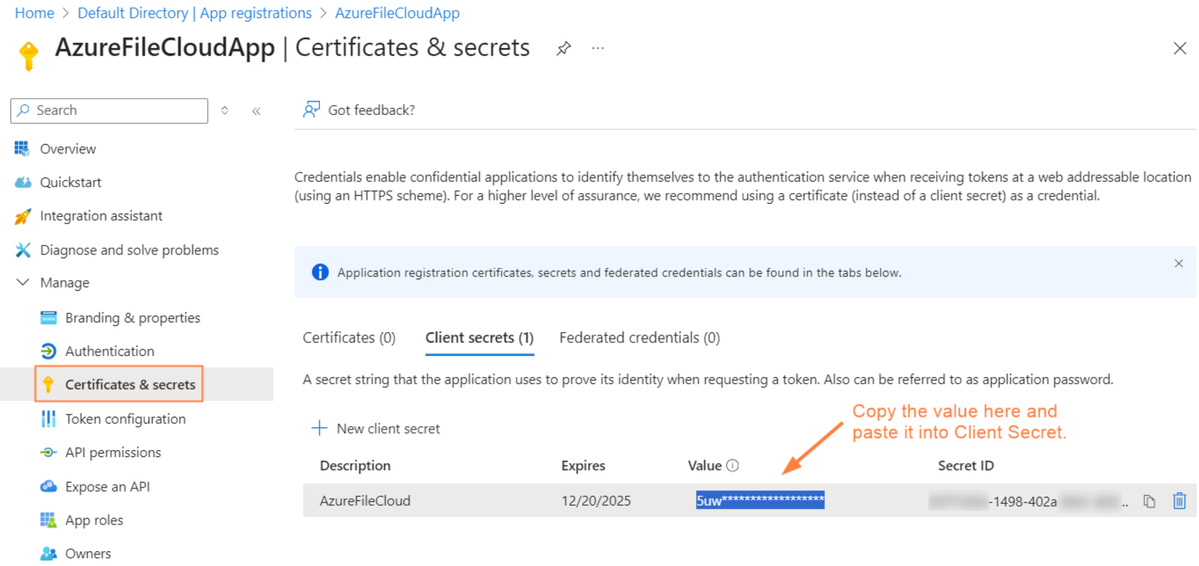
IdP endpoint URL or entity ID (Optional)

IdP endpoint URL or entity ID (Optional)

Test | Cancel | Create

Integration Name	You may enter any name.

Tenant ID	Enter the **Directory (tenant) ID** that you saved from the Overview page when you set up your integration with FileCloud in Azure (see page 63), or copy it directly from that page in the Azure portal and paste it into the **Tenant ID** field. The first of the images below shows where it appears in the Azure portal.
Client Secret	Enter the **Value** that you saved from the Certificates & secrets page when you set up your integration with FileCloud in Azure (see page 63), or copy it directly from that page in the Azure portal and paste it into the **Client Secret** field. The second of the images below shows where it appears in the Azure portal.
Client ID	Enter the **Application (client) ID** that you saved from the Overview page when you set up your integration with FileCloud in Azure (see page 63), or copy it directly from that page in the Azure portal and paste it into the **Client ID** field. The first of the images below shows where it appears in the Azure portal.
Select an attribute to be used as the email to import users	Select the attribute that is used to authenticate the user in SSO. Options are **Mail** or **userPrincipalName**.
oAuth Azure Auth URL (Optional)	In general, this is for use by Azure GovCloud users. Enter the URL of your Azure authorization domain.
oAuth Azure Graph URL (Optional)	In general, this is for use by Azure GovCloud users. Enter the URL of your Azure graph domain.
IdP endpoint URL or entity ID (Optional)	Enter if you are using multiple IdP's. Enter the value in the field **IdP endpoint URL or entity ID** from the FileCloud SSO settings.



Home > Default Directory | App registrations > AzureFileCloudApp

AzureFileCloudApp | Certificates & secrets

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | Client secrets (1) | Federated credentials (0)

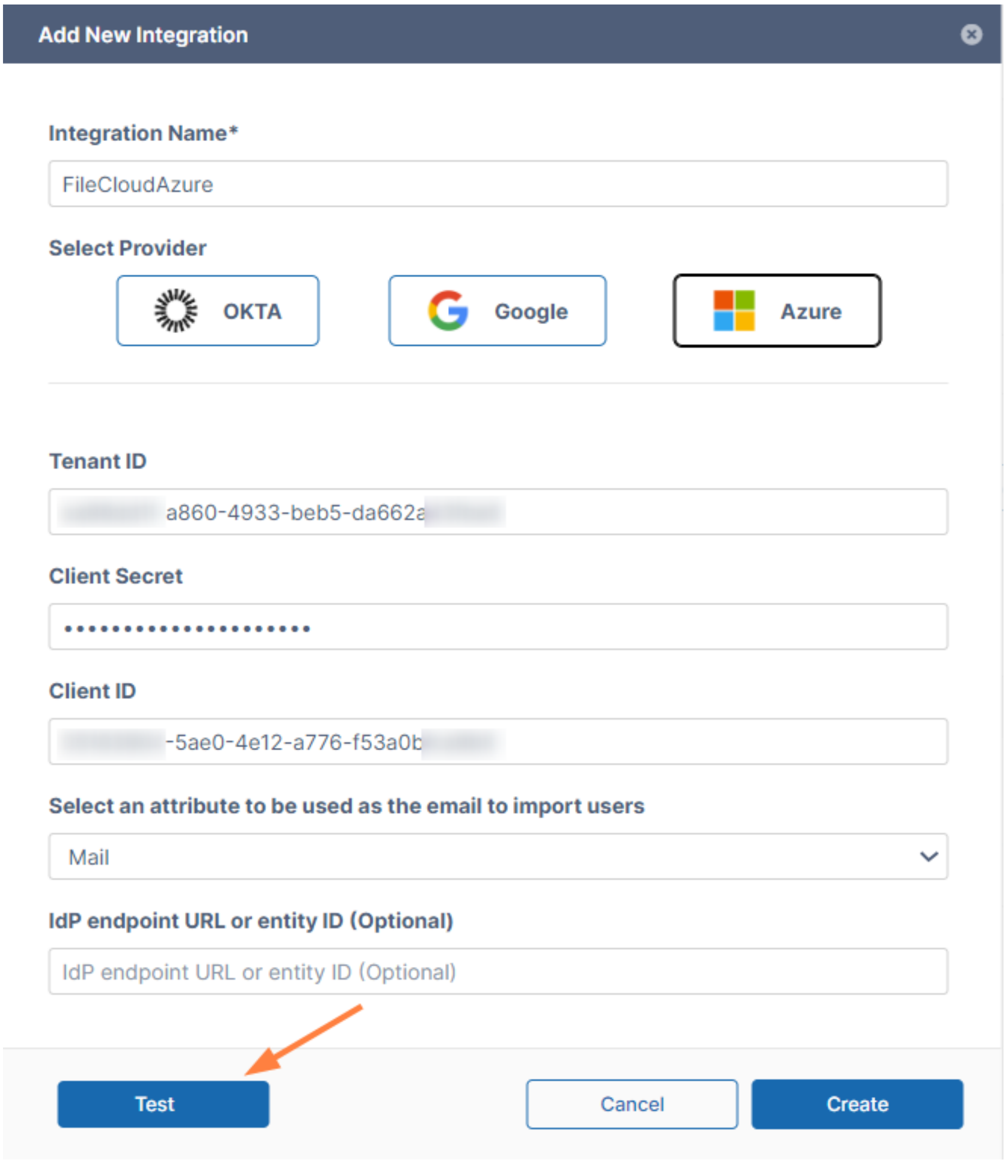
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
AzureFileCloud	12/20/2025	5uw******************	[redacted]-1498-402a[redacted]..

Copy the value here and paste it into Client Secret.

2. Once you have filled in the fields, click **Test** to make sure your integration works.



Add New Integration

Integration Name*: FileCloudAzure

Select Provider: OKTA | Google | Azure

Tenant ID: [redacted]a860-4933-beb5-da662[redacted]

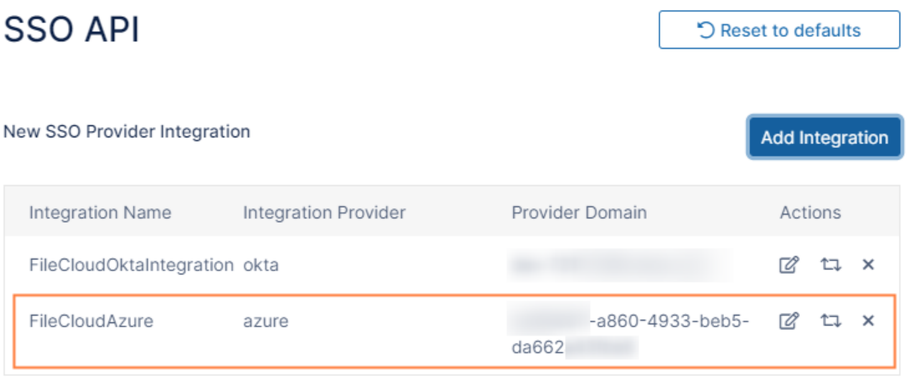
Client Secret: ••••••••••••••••••••••

Client ID: [redacted]-5ae0-4e12-a776-f53a0b[redacted]

Select an attribute to be used as the email to import users: Mail

IdP endpoint URL or entity ID (Optional): IdP endpoint URL or entity ID (Optional)

3. If the test is successful, click **Create**.
   The integration is added to the list of SSO integrations:



SSO API

New SSO Provider Integration

Integration Name	Integration Provider	Provider Domain	Actions
FileCloudOktaIntegration	okta	[redacted]	✎ ⟲ ×
FileCloudAzure	azure	[redacted]-a860-4933-beb5-da662[redacted]	✎ ⟲ ×

4. By default built-in Azure groups are not listed when you import groups from Azure SSO.

For help listing built-in Azure groups, please Contact FileCloud Support.

To list built-in Azure groups:

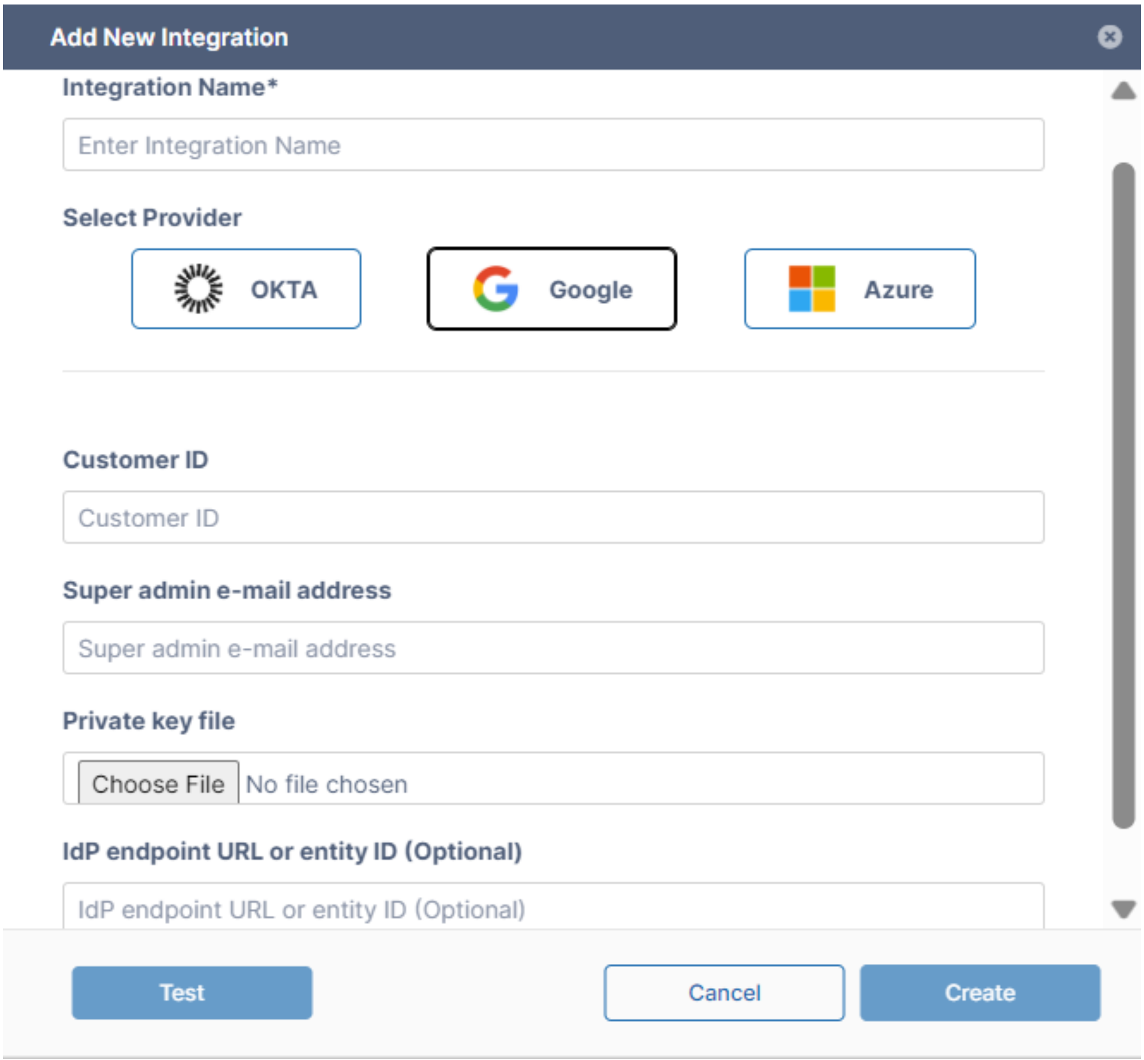
1. Open the configuration file at:
   Windows: **xampp/htdocs/config/cloudconfig.php**
   Linux: **/var/www/html/config/cloudconfig.php**
2. Add the setting:

```
define('TONIDOCLOUD_ADMIN_SSO_API_LIST_ALL_GROUPS',1);
```

Google

Enter integration values for Google

1. When you click the **Google** button under **Select Provider**, the following settings appear. Enter the value for each as indicated in the table below.



Integration Name

You may enter any name.

Customer ID

Find the value that you saved for EntityID in the Google admin portal and copy the value after **idpid=** at the end into **Customer ID**. For example, if the value you saved was: https://accounts.google.com/o/saml2?idpid=ABC123DEF[1], enter **ABC123DEF** into **Customer ID**. The image below shows where it appears in the Google admin portal.

Super admin e-mail address

The e-mail address of the superadmin who added the integration of FileCloud and Google SSO in the Google admin portal and the Google Cloud Console.

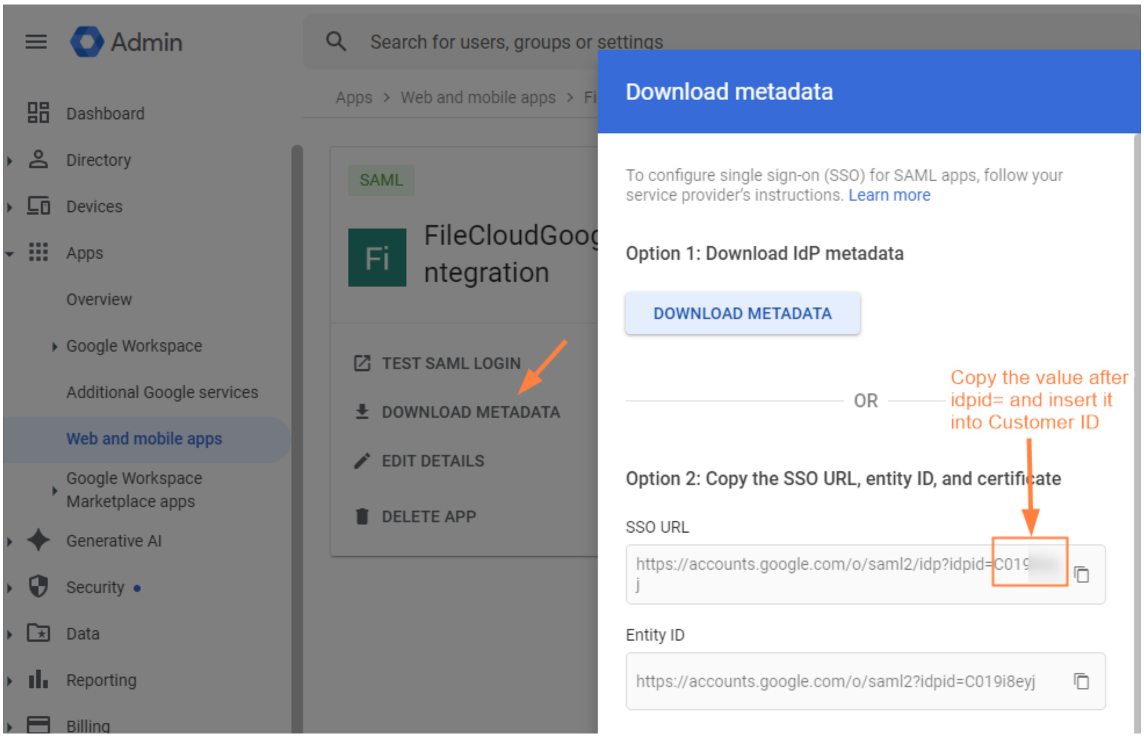
Private key file

The json file that was created in the Google Cloud Console.

[1] https://accounts.google.com/o/saml2?idpid=C019i8eyj

IdP endpoint URL or entity ID

If you are using multiple IdP's, enter the IdP endpoint URL or entity ID from the FileCloud SSO settings.



To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more

Option 1: Download IdP metadata

Option 2: Copy the SSO URL, entity ID, and certificate

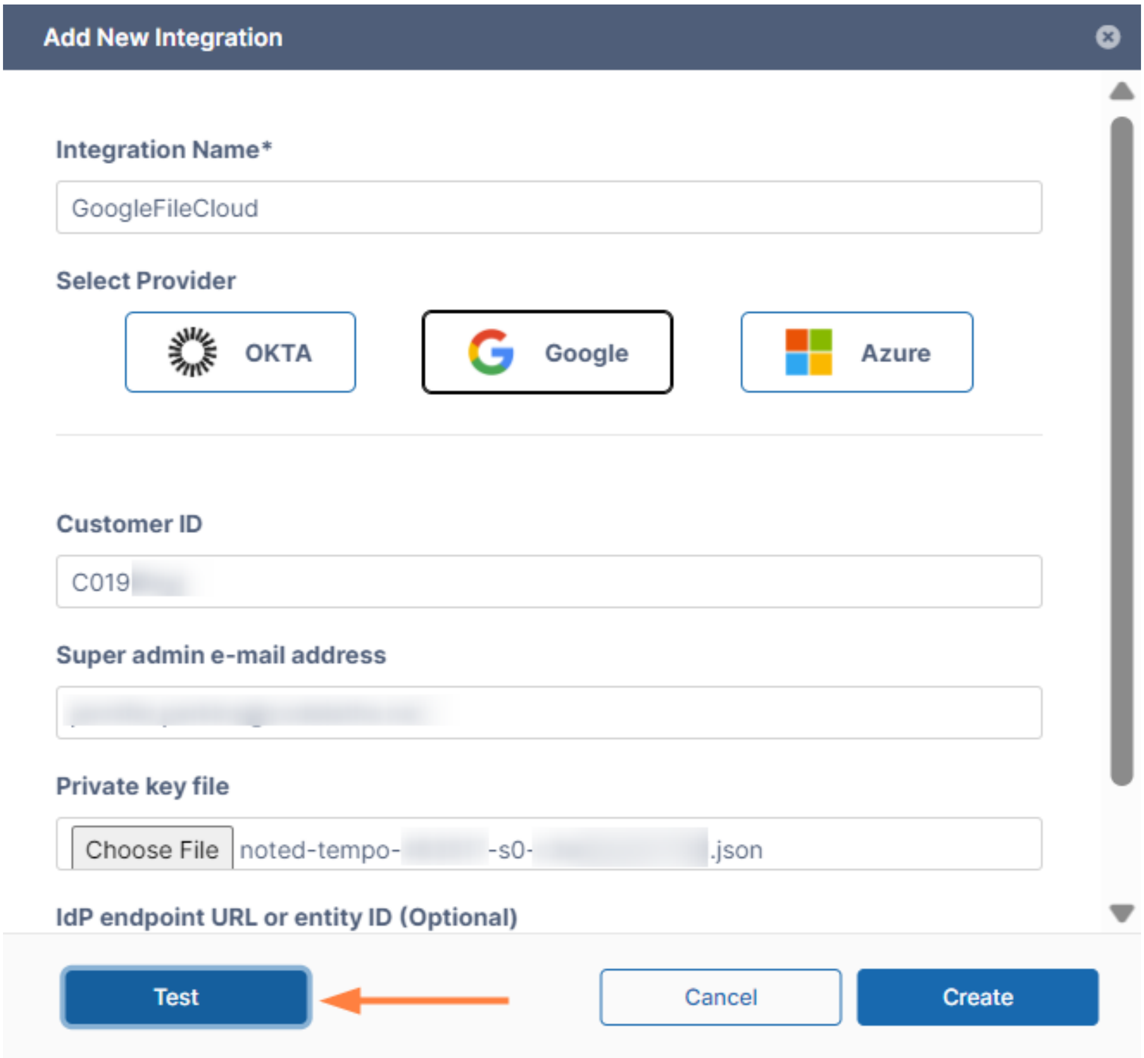
SSO URL: https://accounts.google.com/o/saml2/idp?idpid=C019[redacted]j

Entity ID: https://accounts.google.com/o/saml2?idpid=C019i8eyj

Copy the value after idpid= and insert it into Customer ID

Location of the **Customer ID** value in the Google Admin Portal.

2. Once you have filled in the fields, click **Test** to make sure your integration works.



Add New Integration

Integration Name*

GoogleFileCloud

Select Provider

Customer ID

C019[redacted]

Super admin e-mail address

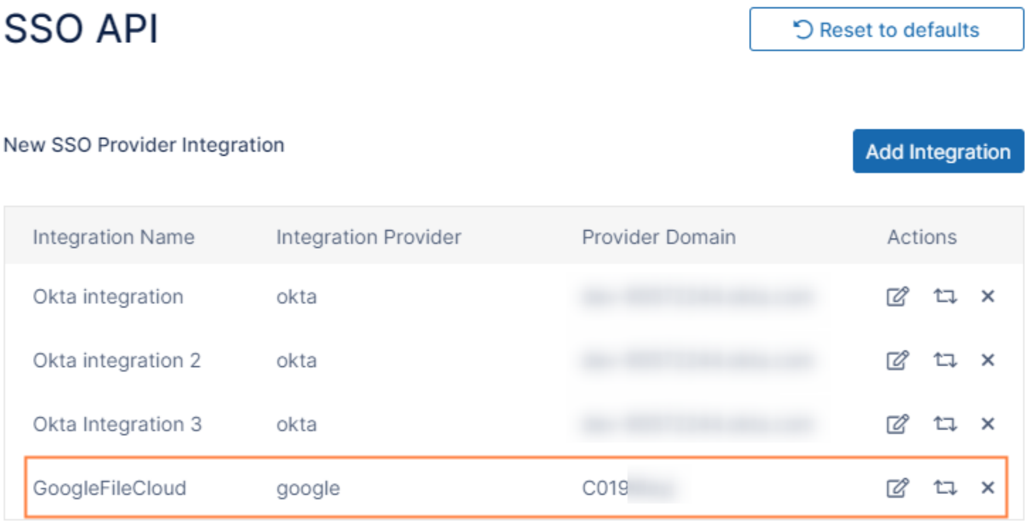
[redacted]

Private key file

Choose File noted-tempo-[redacted]-s0-[redacted].json

IdP endpoint URL or entity ID (Optional)

3. If the test is successful, click **Create**.
   The integration is added to the list of SSO integrations:



SSO API

New SSO Provider Integration

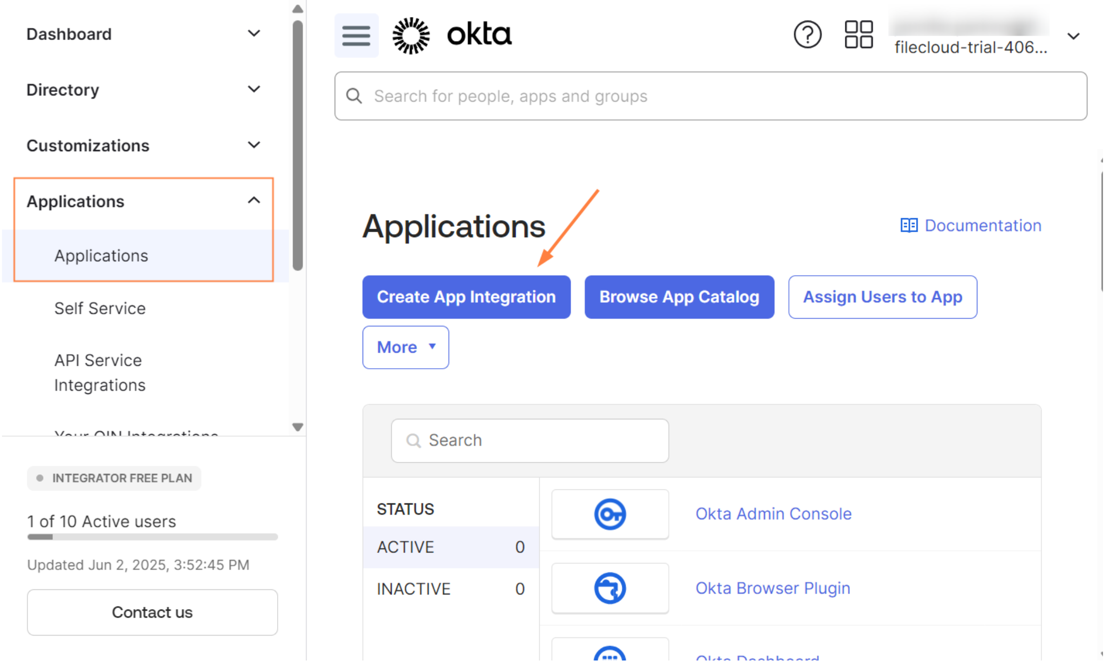
Integration Name	Integration Provider	Provider Domain	Actions
Okta integration	okta	[redacted]	
Okta integration 2	okta	[redacted]	
Okta Integration 3	okta	[redacted]	
GoogleFileCloud	google	C019[redacted]	

6. Now import groups and users through your SSO integration on the Managed Groups page.

Okta: Set Up FileCloud Integration for SSO Group/User Import

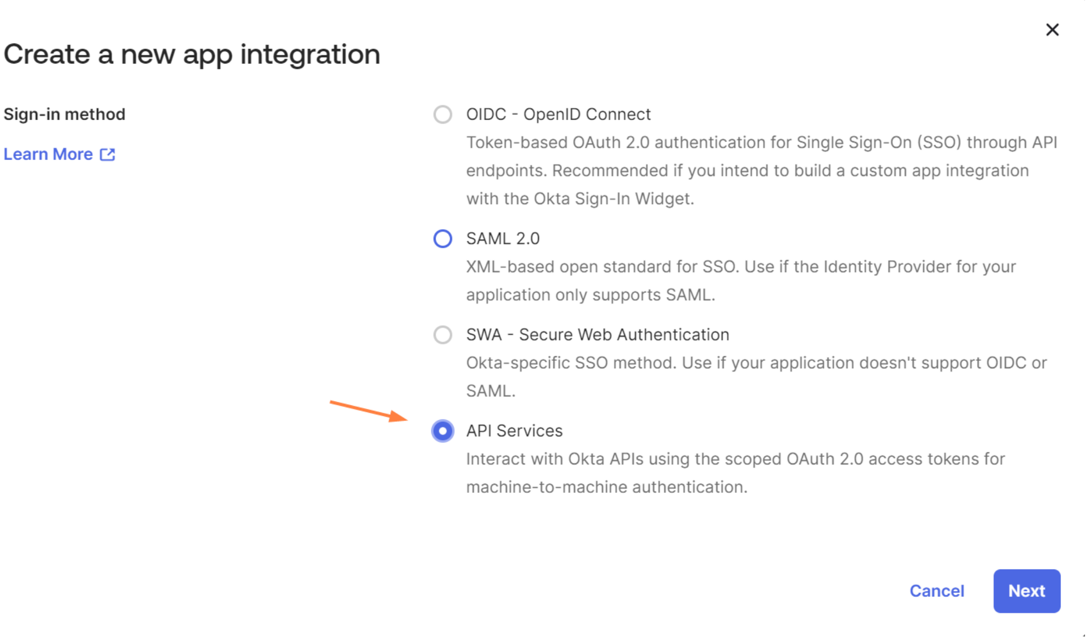
To configure FileCloud/Okta integration in Okta for SSO group/user import:

1. Log in to the Okta admin portal, and navigate to **Applications > Applications.**
2. Click **Create App Integration**.



A list of sign-in methods opens.

3. Choose **API Services**, and click **Next**.



Create a new app integration

Sign-in method

Learn More

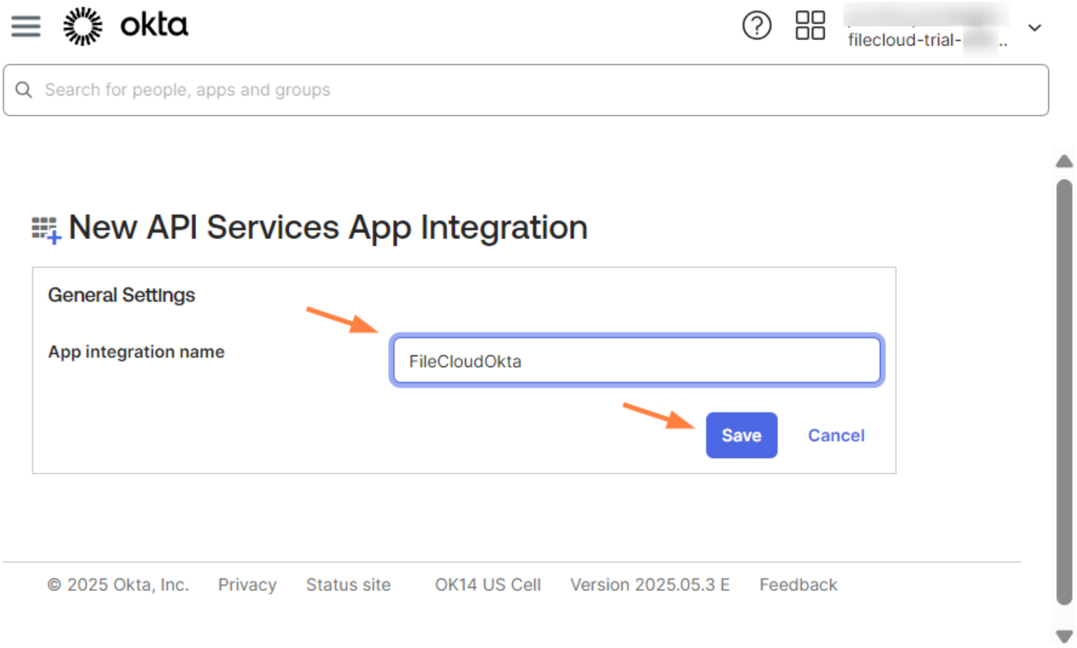
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

● API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

4. Enter a name for the app integration and click **Save**.

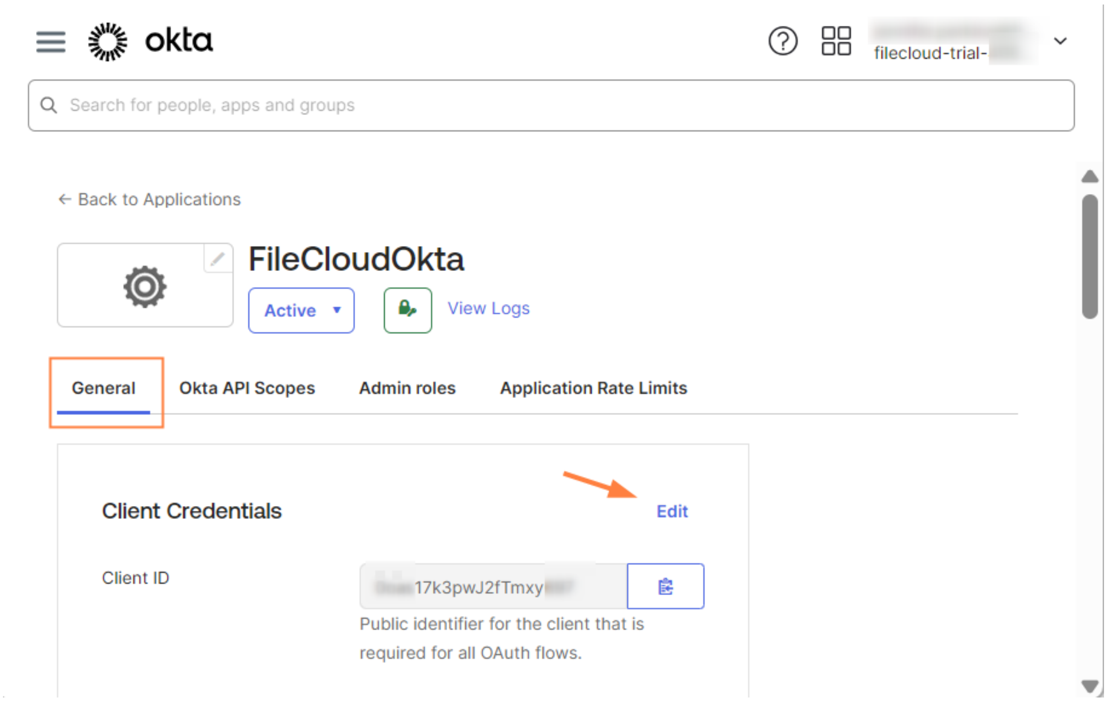


New API Services App Integration

General Settings

App integration name: FileCloudOkta

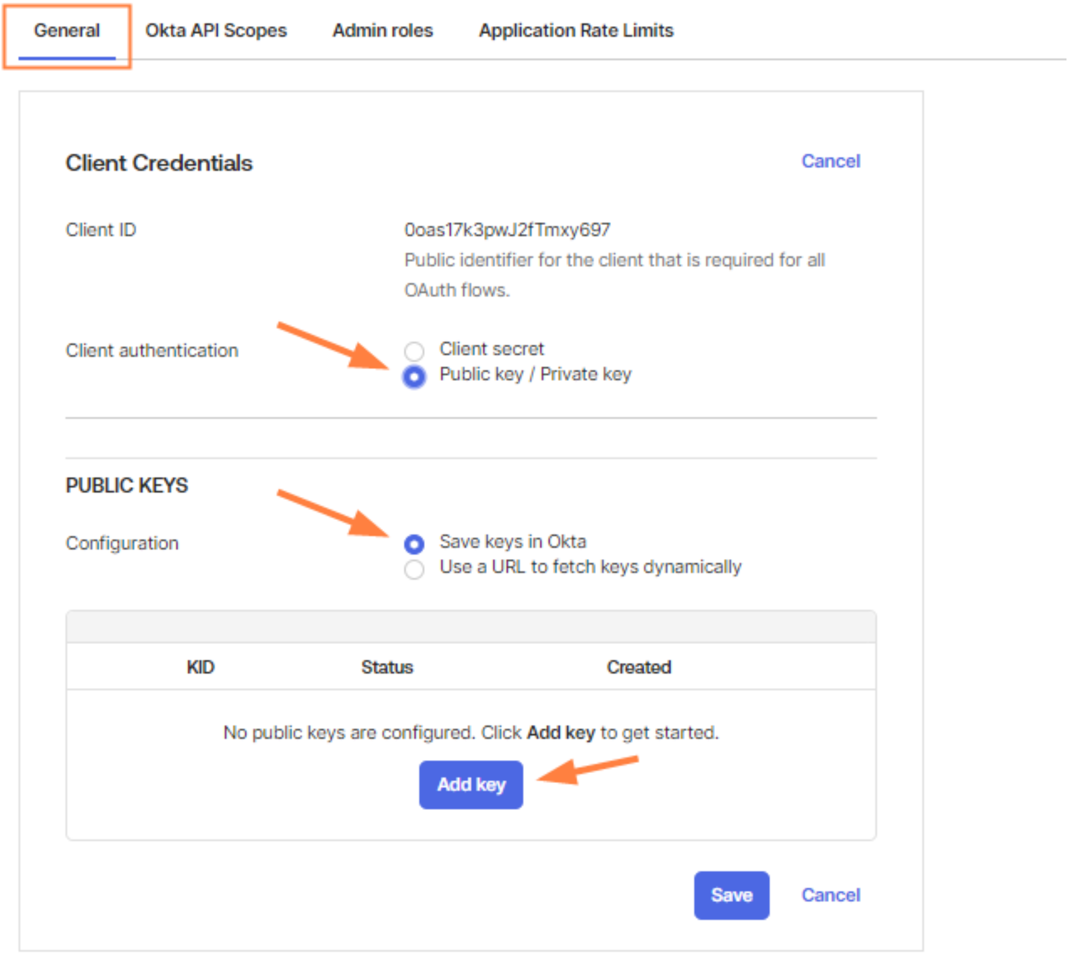
5. Your new app opens to the General tab. Click **Edit**.



Client ID: [redacted]17k3pwJ2fTmxy[redacted]

Public identifier for the client that is required for all OAuth flows.

6. For **Client authentication**, select **Public key / Private key**.
7. For **Configuration**, choose **Save keys in Okta**.
8. Click **Add key**.



Client Credentials

Client ID: 0oas17k3pwJ2fTmxy697

Public identifier for the client that is required for all OAuth flows.

Client authentication: ○ Client secret ● Public key / Private key

PUBLIC KEYS

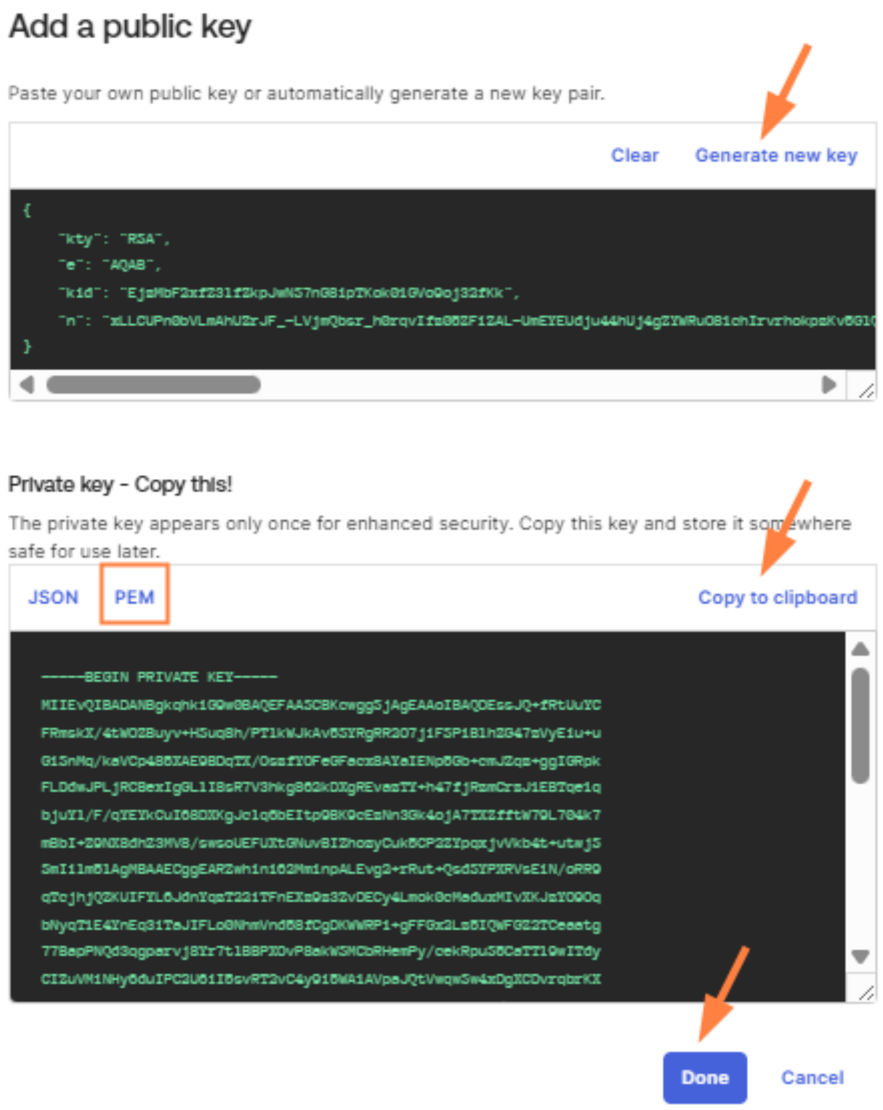
Configuration: ● Save keys in Okta ○ Use a URL to fetch keys dynamically

KID	Status	Created

No public keys are configured. Click **Add key** to get started.

The **Add a public key** window opens.

9. Paste in your own key or click **Generate new key**.
10. If you click **Generate new key**, under **Private key - Copy this!** click **PEM**, and then click **Copy to clipboard**, and save the copied key to a text file with a **.pem** extension so you can upload it to FileCloud.
    If you do not save as a **.pem** file, you will not be able to upload the private key to FileCloud.



Add a public key

Paste your own public key or automatically generate a new key pair.

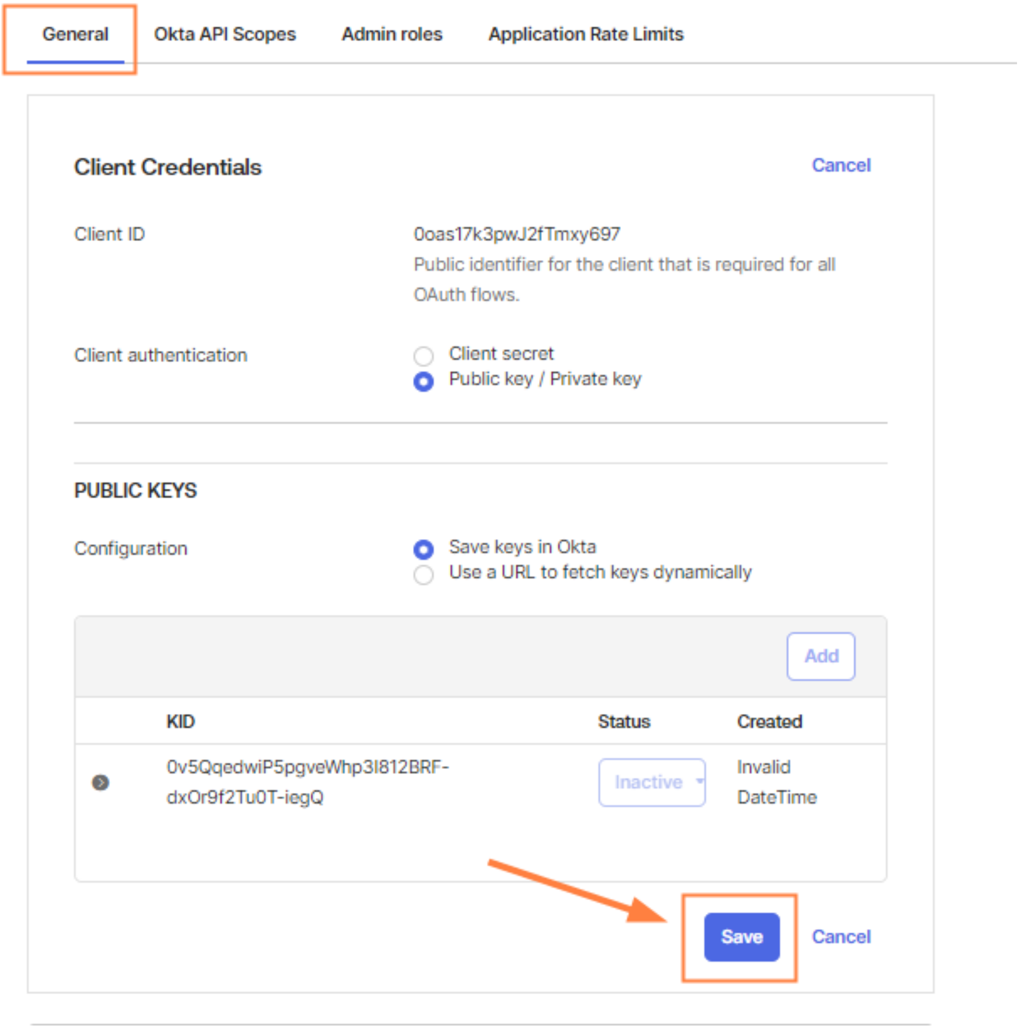
```
{
    "kty": "RSA",
    "e": "AQAB",
    "kid": "EjsMbF2xfZ31fZkpJwN57nG81pTKok01GVo9oj32fKk",
    "n": "xLLCUPn0bVLmAhUZrJF_-LVjmQbsr_h0rqvIfs00ZF1ZAL-UmEYEUdju44hUj4gZYWRuO81chIrvrhokpsKv0G1(
}
```

Private key - Copy this!

The private key appears only once for enhanced security. Copy this key and store it somewhere safe for use later.

```
------BEGIN PRIVATE KEY------
MIIEvQIBADANBgkqhk1G9w0BAQEFAASCBKcwgg5jAgEAAoIBAQDEssJQ+fRtUuYC
FRmskX/4tWO2Buyv+H5uq8h/PT1kWJkAv65YRgRR2O7j1F5P1B1h2G47sVyE1u+u
G13nMq/keVCp486XAE9BDqTX/OszfYOFeGFacx8AYaIENp6Gb+cmJZqs+ggIGRpk
FLDdwJPLjRCBexIgGL1IBsR7V3hkg862kDXgREvazTY+h47fjRsmCrsJ1EBTqe1q
bjuY1/F/qYEYkCuI68DXKgJc1q6bEItp9BK9cEsNn3Gk4ojA7TXZfftW79L704k7
mBbI+Z9NXBdhZ3MV8/swsoUEFUXtGNuv8IZhozyCuk6CP2ZYpqxjvVkb4t+utwj5
3mI1lm61AgMBAAECggEARZwhin162MmInpALEvg2+rRut+Qsd5YPXRVsE1N/oRR9
qTcjhjQZKUIFYL6JdnYqsT221TFnEXs9s32vDECy4LmokGcMaduxMIvXKJzYO9Oq
bNyqT1E4YnEq31TaJIFLoGNhmVnd68fCgDKWWRP1+gFFGx2Ls6IQWFGZ2TCeaatg
77BapPNQd3qgparvj8Yr7tlBBPXOvP8akW3MCbRHemPy/cekRpu36CaTT19wITdy
CIZuVM1NHy6duIPC2U61I6svRT2vC4y916WA1AVpaJQtVwqw5w4xDgXCDvrqbrKX
```

11. Click **Done**.
12. Click **Save**, or your public key will not be saved.



Client Credentials

Client ID: 0oas17k3pwJ2fTmxy697
Public identifier for the client that is required for all OAuth flows.

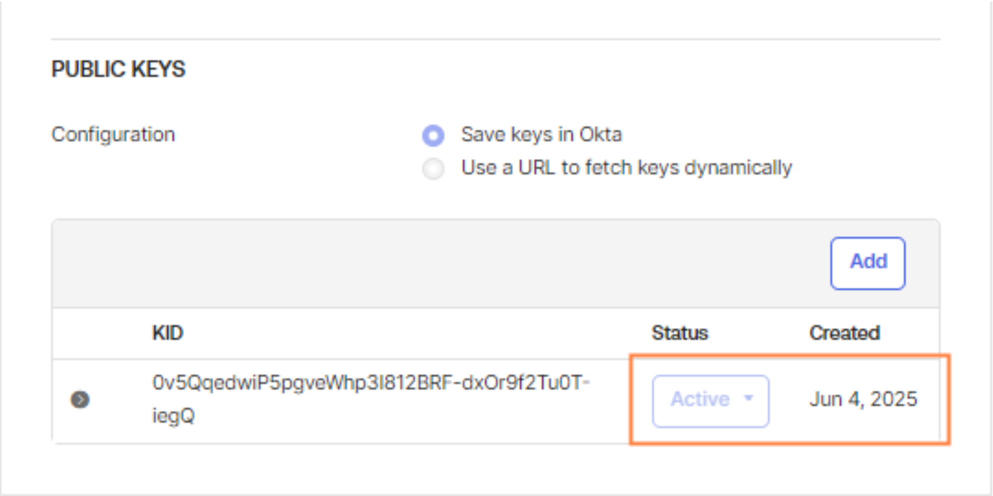
Client authentication: ○ Client secret ● Public key / Private key

PUBLIC KEYS

Configuration: ● Save keys in Okta ○ Use a URL to fetch keys dynamically

	KID	Status	Created
	0v5QqedwiP5pgveWhp3I812BRF-dxOr9f2Tu0T-iegQ	Inactive	Invalid DateTime

Once you click **Save**, your key should show a **Status** of **Active** and a **Created** date.

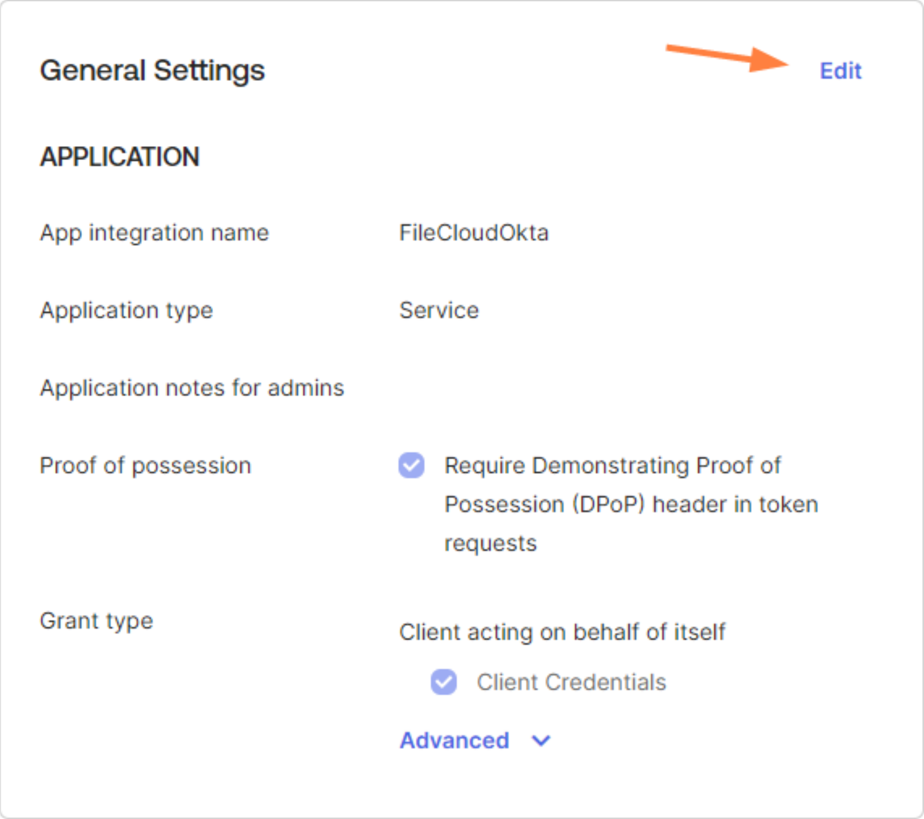


PUBLIC KEYS

Configuration: ● Save keys in Okta ○ Use a URL to fetch keys dynamically

	KID	Status	Created
	0v5QqedwiP5pgveWhp3I812BRF-dxOr9f2Tu0T-iegQ	Active	Jun 4, 2025

13. Remain on the General tab. Scroll down to **General Settings**, and click **Edit**



General Settings

Edit

APPLICATION

App integration name: FileCloudOkta

Application type: Service

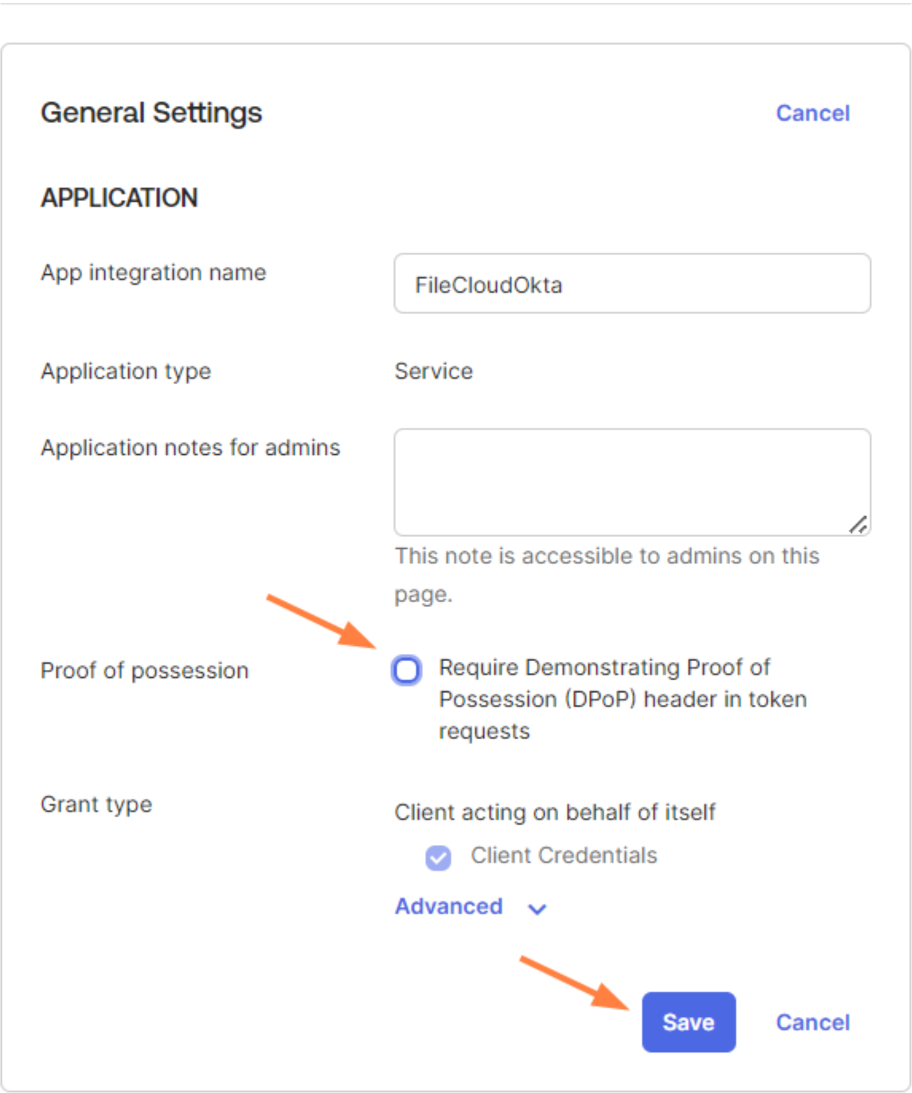
Application notes for admins

Proof of possession: ☑ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type: Client acting on behalf of itself

☑ Client Credentials

14. Uncheck **Proof of possession**, and click **Save**.



General Settings

APPLICATION

App integration name: FileCloudOkta

Application type: Service

Application notes for admins:

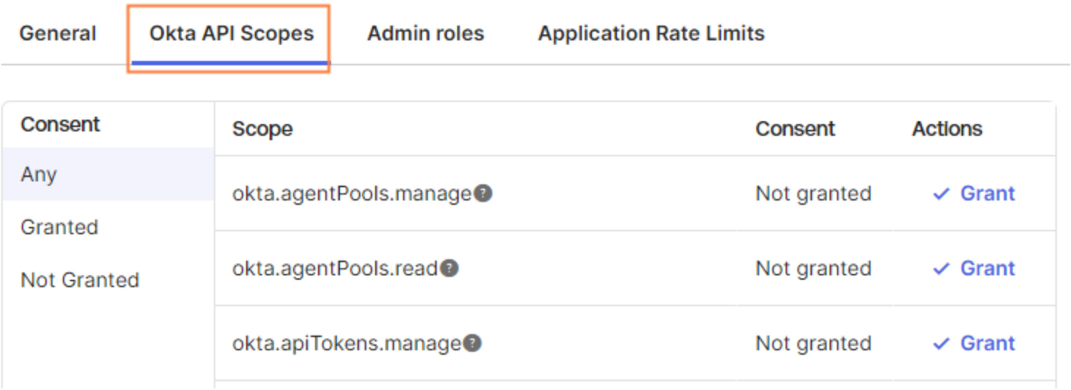
This note is accessible to admins on this page.

Proof of possession: ○ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type: Client acting on behalf of itself

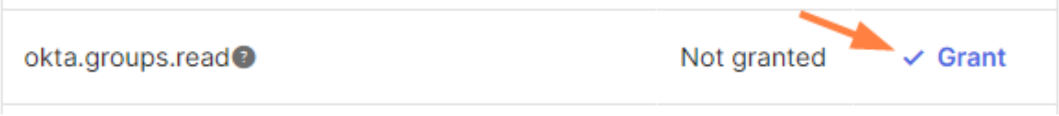
☑ Client Credentials

Click the **Okta API Scopes** tab.



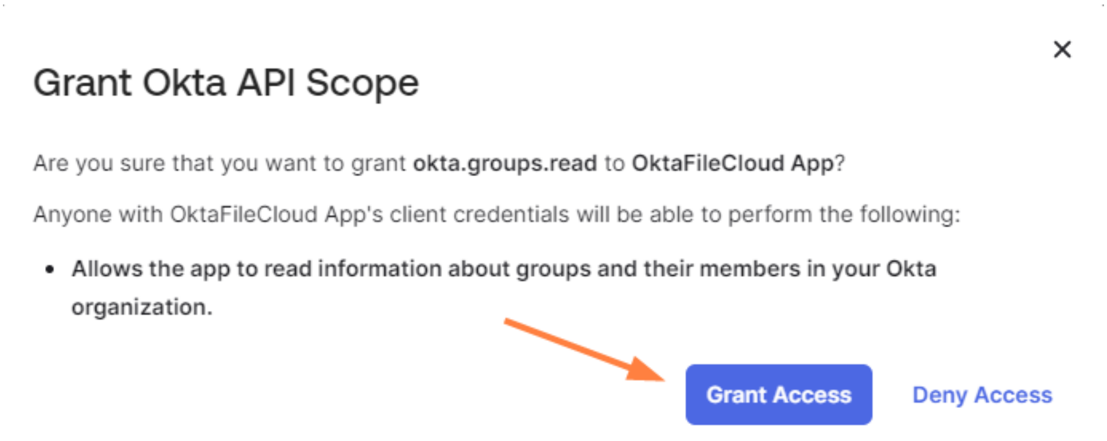
Scope	Consent	Actions
okta.agentPools.manage	Not granted	✓ Grant
okta.agentPools.read	Not granted	✓ Grant
okta.apiTokens.manage	Not granted	✓ Grant

15. Scroll down to **okta.groups.read** and click **Grant** to enable FileCloud to read Okta groups.



You are prompted to grant **okta.groups.read** scope to the app.

16. Click **Grant Access**.



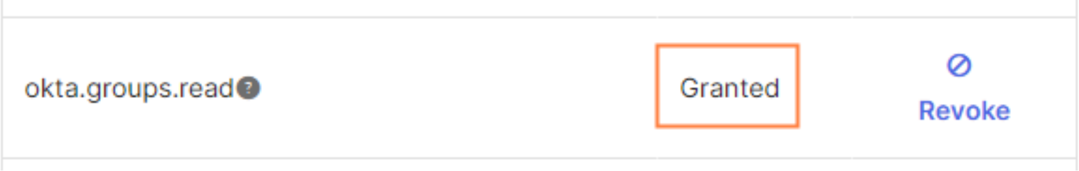
Grant Okta API Scope

Are you sure that you want to grant **okta.groups.read** to **OktaFileCloud App**?

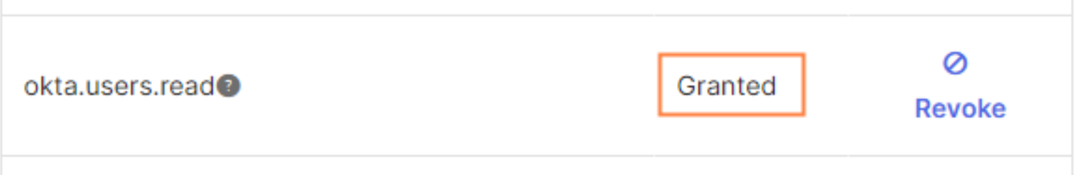
Anyone with OktaFileCloud App's client credentials will be able to perform the following:

- **Allows the app to read information about groups and their members in your Okta organization.**

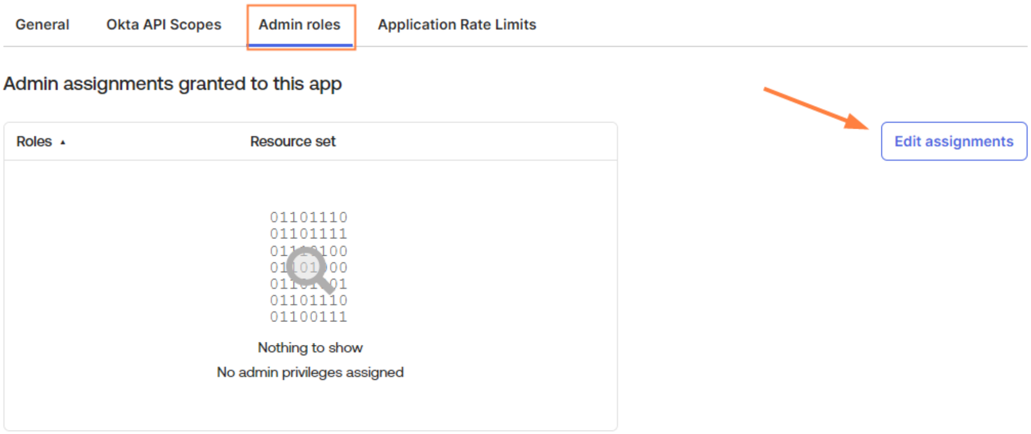
Now the row for **okta.groups.read** should appear as:



17. Scroll down to **okta.users.read** and click **Grant Access** to enable FileCloud to read Okta users. The **Grant Okta API Scope** notification does not appear again.



18. Click the **Admin roles** tab.
19. Click **Edit assignments**.



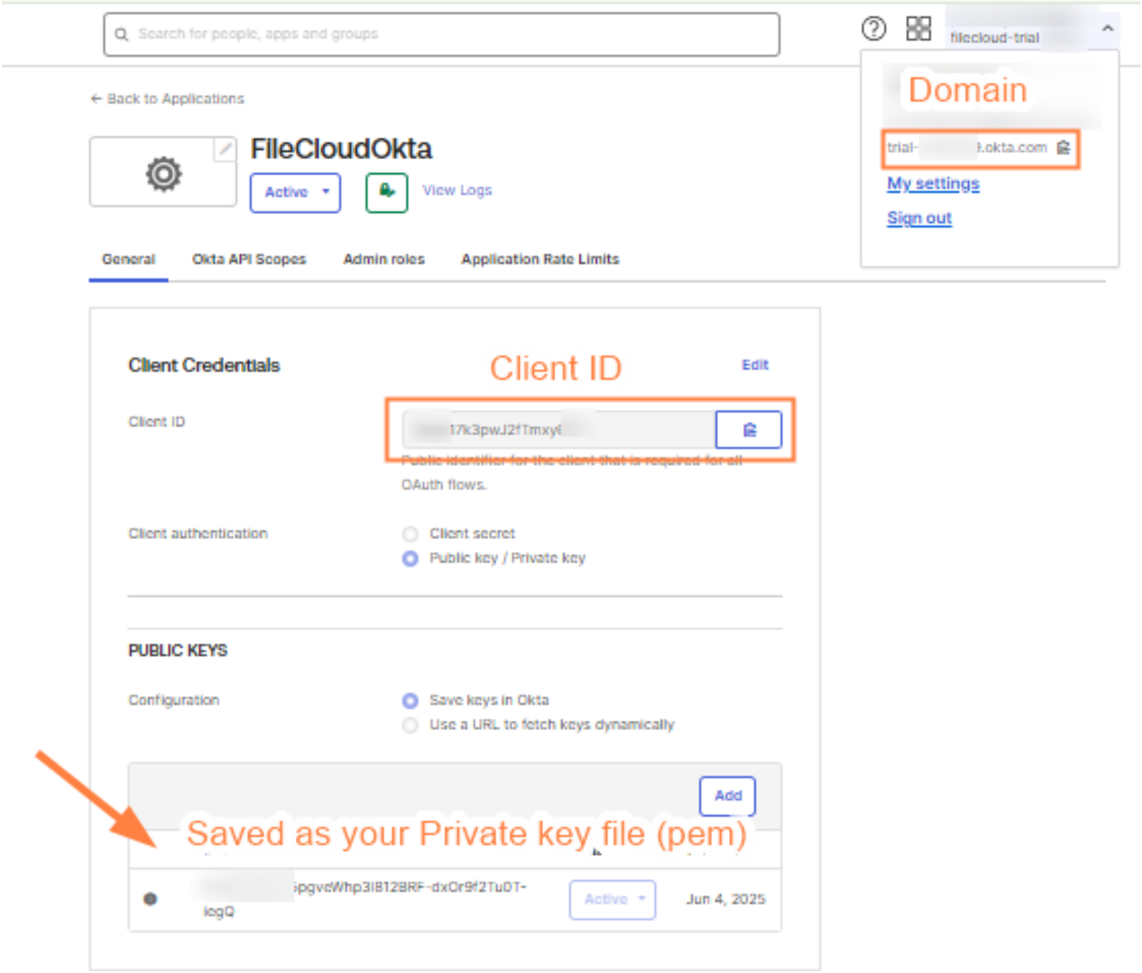
Admin assignments granted to this app

Nothing to show

No admin privileges assigned

20. In **Role**, choose a role that should have access to Okta groups and users, or choose **Read-only Administrator**.
21. Click **Save Changes**.

    You have finished setting up integration on the Okta side.
    Now you have the values you need to set up integration on the FileCloud side: the domain in the user drop-down box, the **Client ID** on the General tab, and the .pem keyfile that you saved.



Domain

trial-[redacted].okta.com

FileCloudOkta

Client Credentials

Client ID

Client ID: [redacted]17k3pwJ2fTmxy[redacted]

Public identifier for the client that is required for all OAuth flows.

Client authentication: ○ Client secret ● Public key / Private key

PUBLIC KEYS

Configuration: ● Save keys in Okta ○ Use a URL to fetch keys dynamically

Saved as your Private key file (pem)

● [redacted]pgvcWhp3I812BRF-dxOr9f2TuOT-kcgQ Active Jun 4, 2025

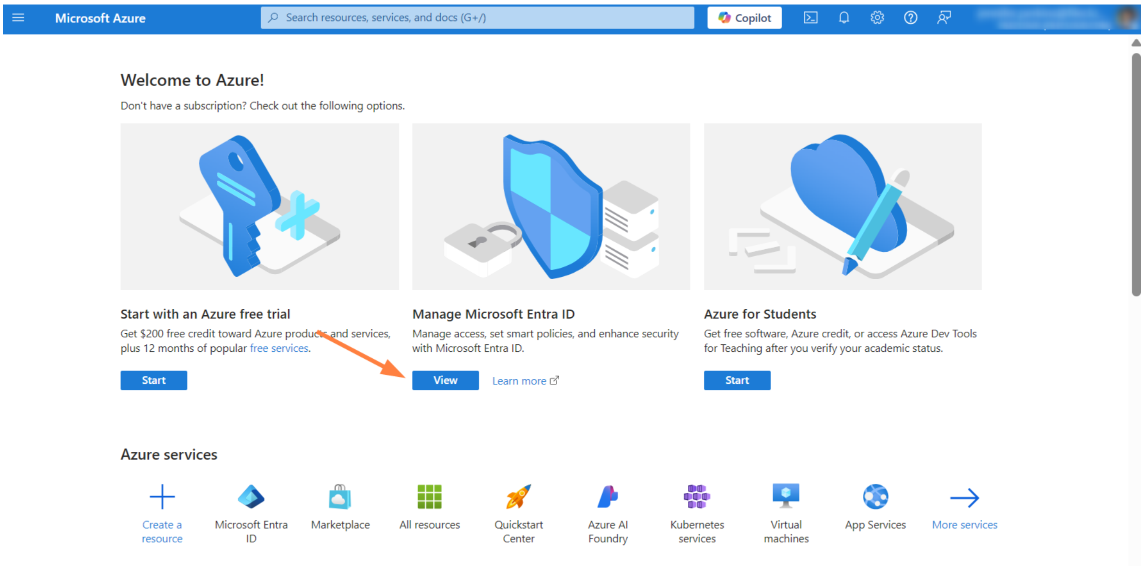
To enter the values into the FileCloud side, see SSO API: Configure Import of SSO Groups and Users.

Azure: Set up FileCloud Integration for SSO Group/User Import

To configure FileCloud/Azure integration in Azure for SSO group/user import:

1. Log into portal.azure.com[2], and go to Microsoft Entra ID (https://entra.microsoft.com/) .

[2] https://portal.azure.com/



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

Manage Microsoft Entra ID

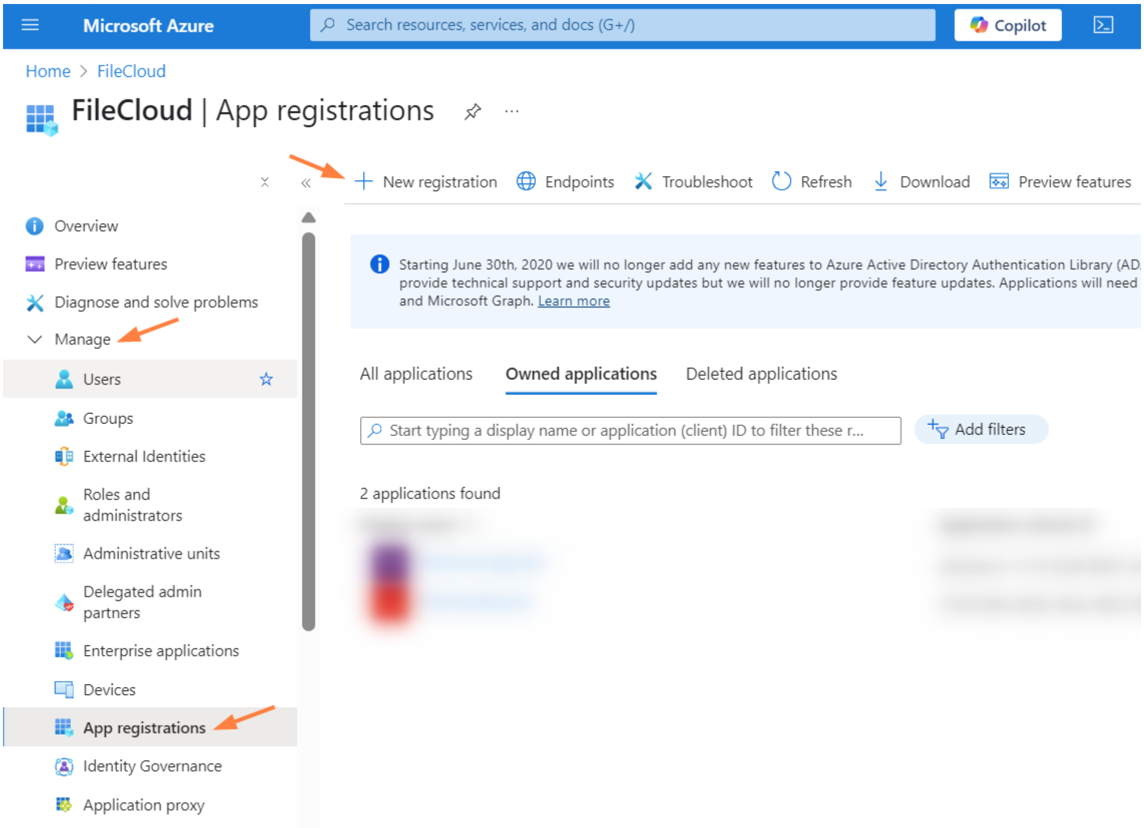
Manage access, set smart policies, and enhance security with Microsoft Entra ID.

Azure for Students

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

Azure services

2. In the left navigation pane, go to Manage > App registrations, and at the top of the page, click **New registration**.



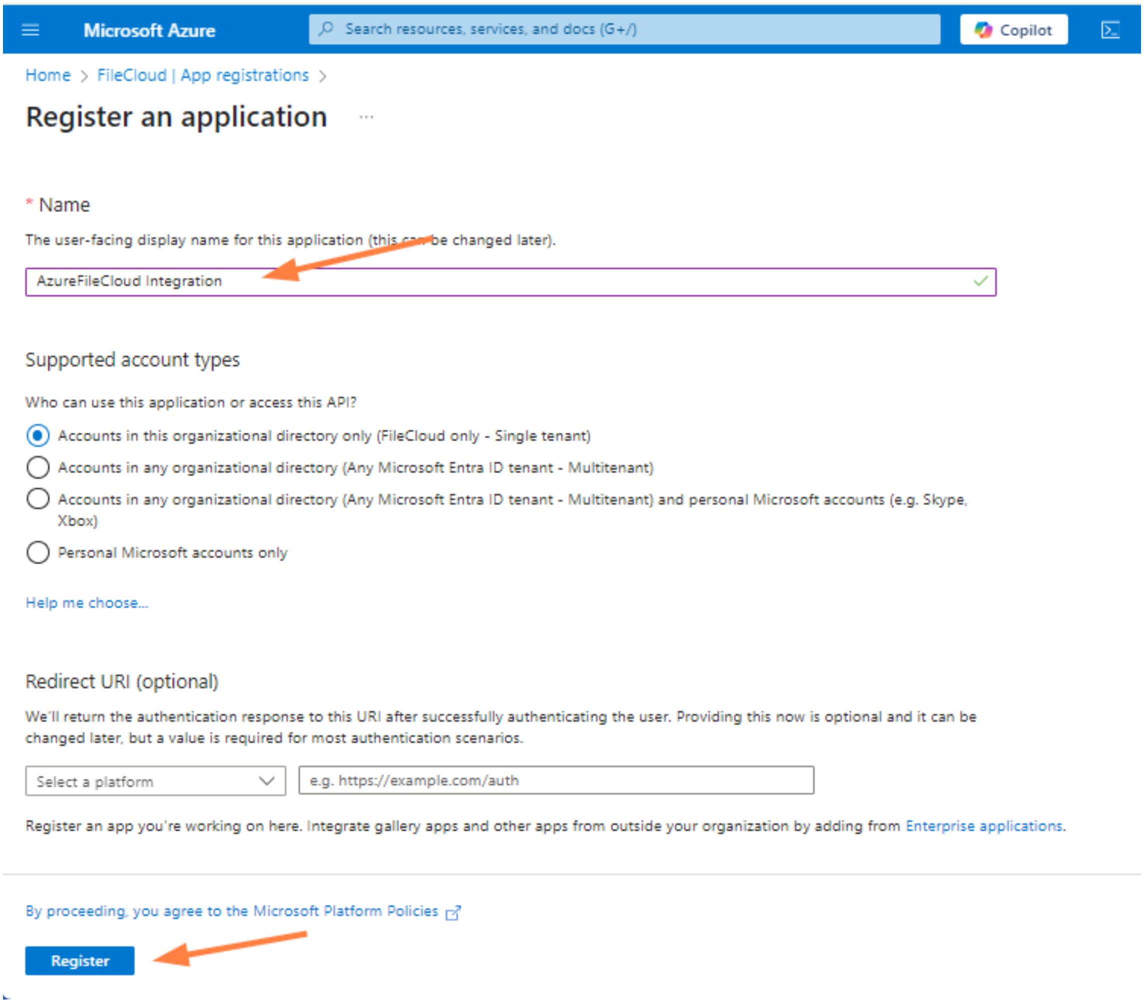
FileCloud | App registrations

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (AD provide technical support and security updates but we will no longer provide feature updates. Applications will need and Microsoft Graph. Learn more

All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters

2 applications found

3. Enter a name for the application, and then click **Register**.



Home > FileCloud | App registrations >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

AzureFileCloud Integration

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (FileCloud only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

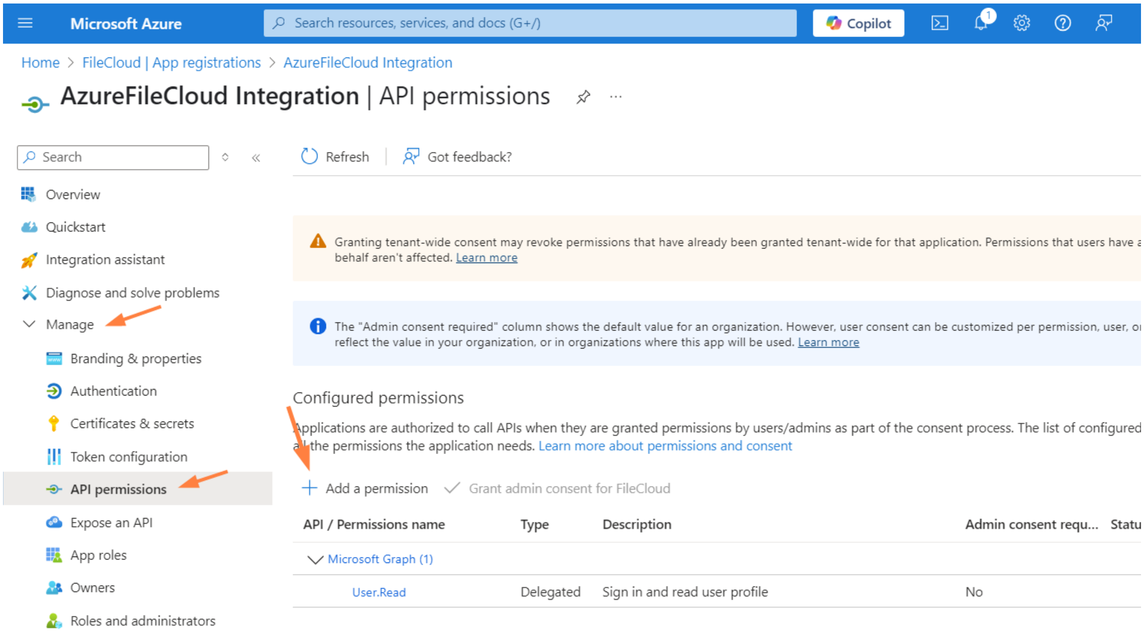
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

4. In the left navigation pane, go to **Manage > API permissions**, and then click **Add a permission**.



Home > FileCloud | App registrations > AzureFileCloud Integration

AzureFileCloud Integration | API permissions

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have a behalf aren't affected. Learn more

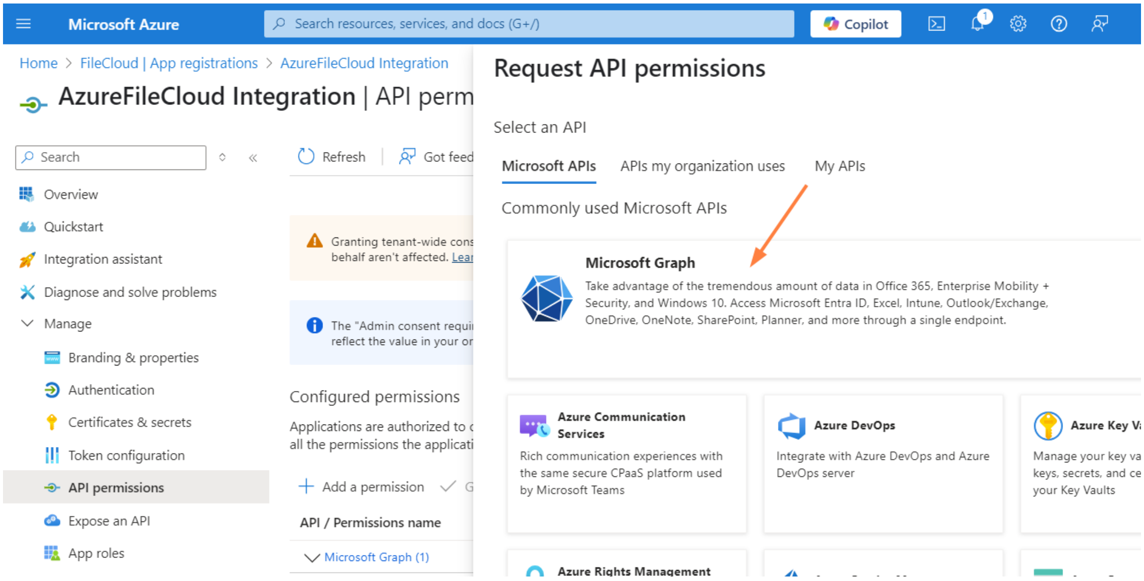
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, o reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Statu
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

5. In the **Request API permissions** box, click **Microsoft Graph**.



Granting tenant-wide cons behalf aren't affected. Lear

The "Admin consent requi reflect the value in your or

Configured permissions

Applications are authorized to c all the permissions the applicati

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

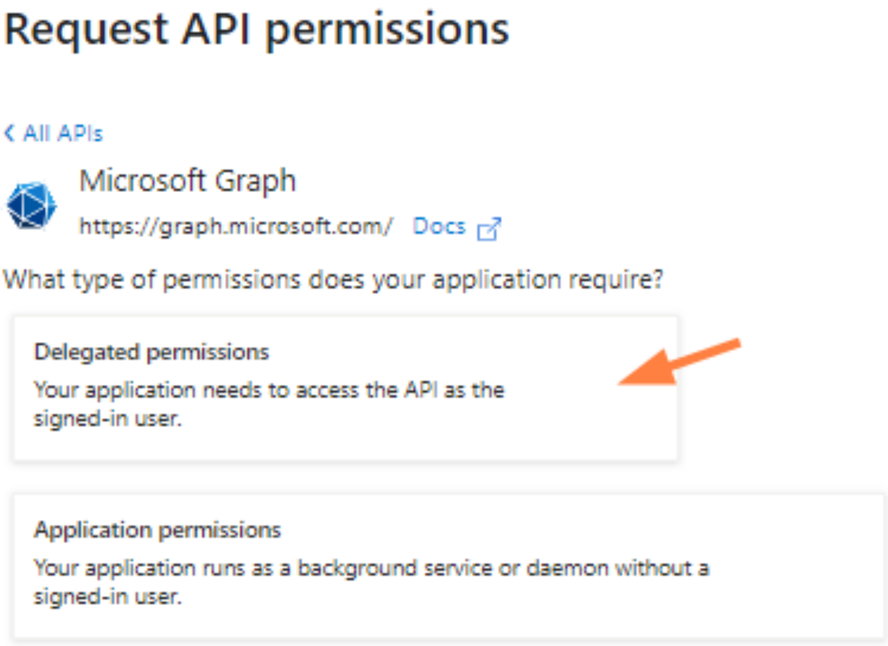
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Integrate with Azure DevOps and Azure DevOps server

Manage your key va keys, secrets, and ce your Key Vaults

In the **Request API Permissions** box, you are prompted to choose a type of permission.

6. First, select **Delegated permissions**, and request the permissions specified below.



What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

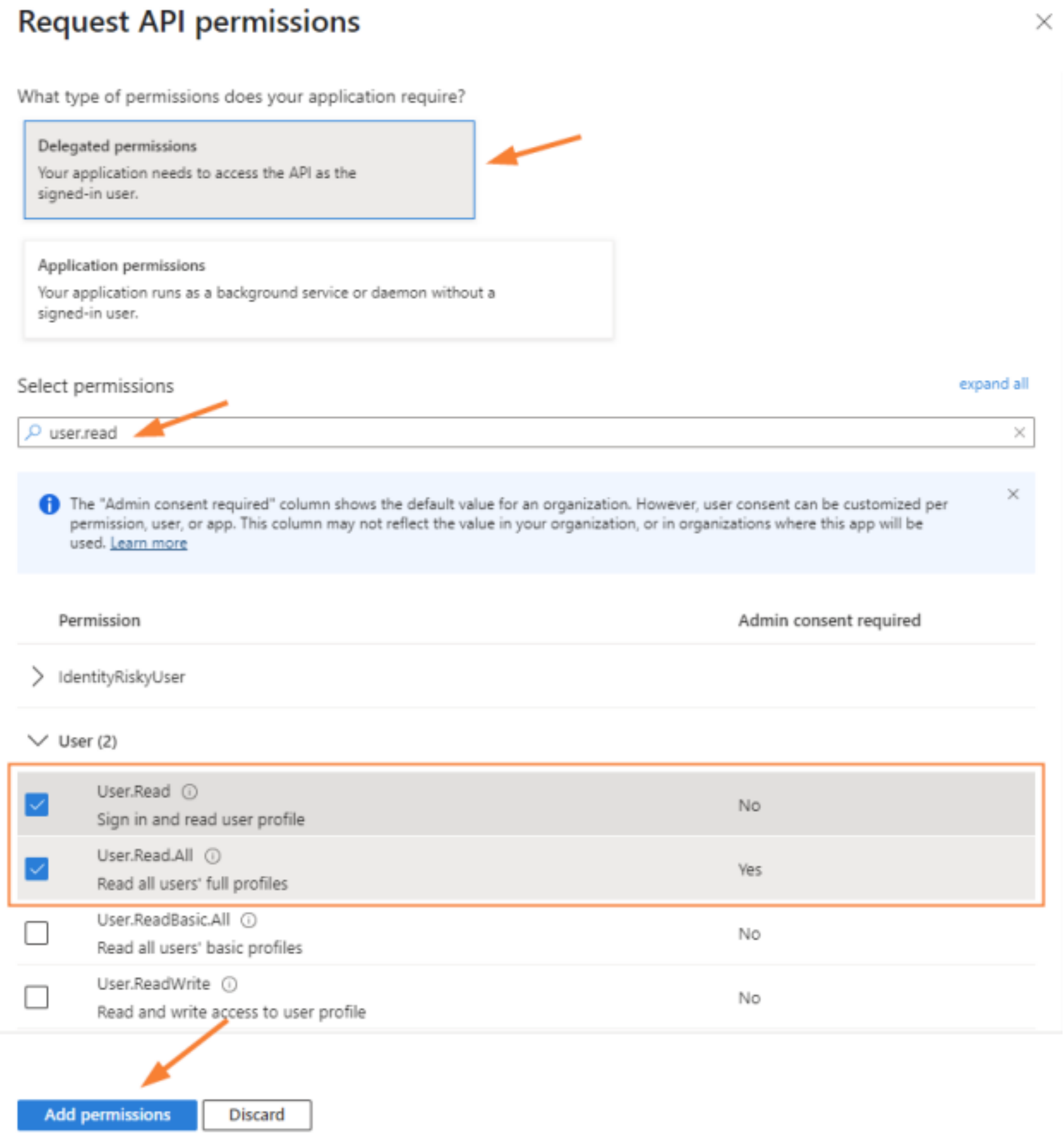
Your application runs as a background service or daemon without a signed-in user.

Delegated permissions to request:

- Directory.Read.All
- Group.Read.All
- GroupMember.Read.All

- User.Read
- User.Read.All

7. Search for the permission type in the Select permissions search bar to find it more quickly, and then check the permissions.
8. When you are done checking all of the above permissions, click **Add permissions**.



Request API permissions

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

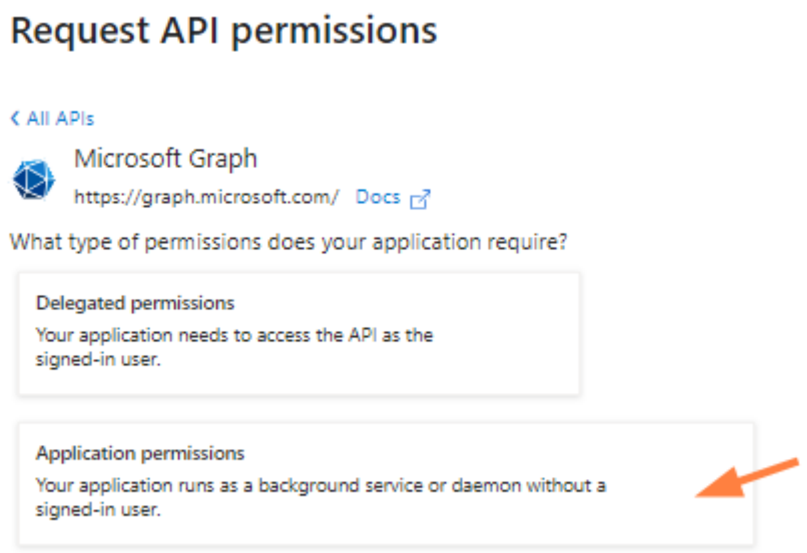
Select permissions

user.read

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

	Permission	Admin consent required
	> IdentityRiskyUser	
	∨ User (2)	
☑	User.Read ⓘ Sign in and read user profile	No
☑	User.Read.All ⓘ Read all users' full profiles	Yes
□	User.ReadBasic.All ⓘ Read all users' basic profiles	No
□	User.ReadWrite ⓘ Read and write access to user profile	No

Now, in the Request API permissions box, choose Application permissions, and request the permissions specified below:



Request API permissions

‹ All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

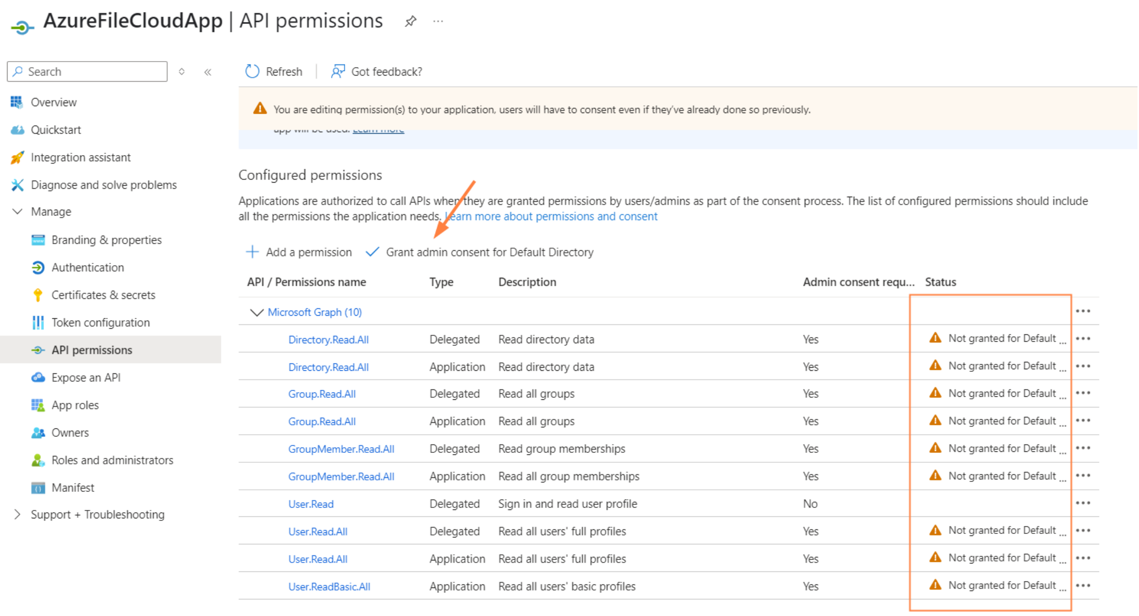
Application permissions to request:

- Directory.Read.All
- Group.Read.All
- GroupMember.Read.All
- User.Read.All
- User.ReadBasic.All

9. Repeat steps 7 and 8 to request the Application permissions.

   Initially, most of the permissions show that permission has not been granted.

10. Above the list, click **Grant admin consent for [Tenant name]**, and when prompted, click **Yes.**
    Note: If you are not a global admin, you must ask your global admin to grant the API permissions for you.



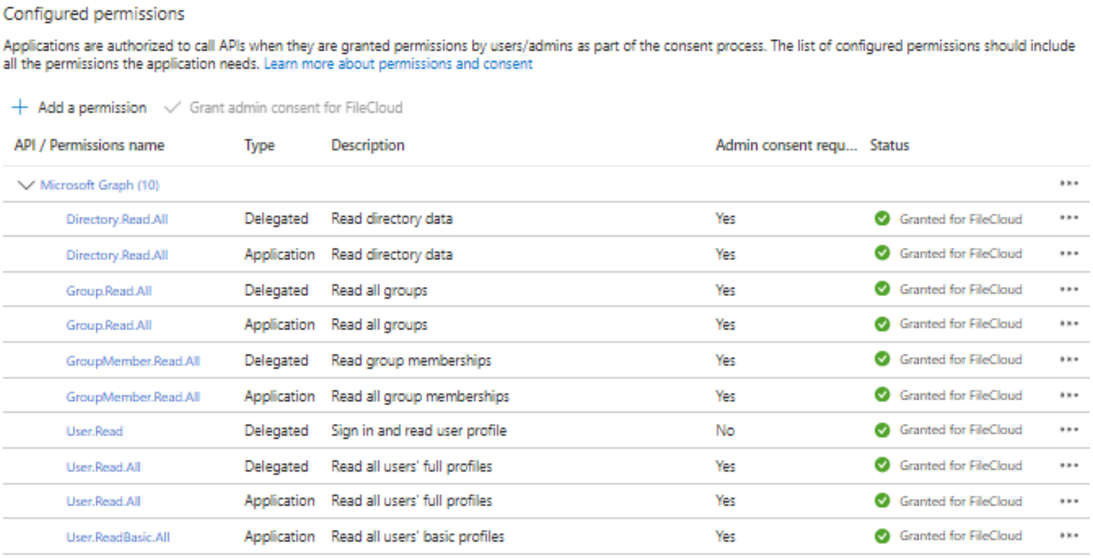
You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (10)				
Directory.Read.All	Delegated	Read directory data	Yes	Not granted for Default ...
Directory.Read.All	Application	Read directory data	Yes	Not granted for Default ...
Group.Read.All	Delegated	Read all groups	Yes	Not granted for Default ...
Group.Read.All	Application	Read all groups	Yes	Not granted for Default ...
GroupMember.Read.All	Delegated	Read group memberships	Yes	Not granted for Default ...
GroupMember.Read.All	Application	Read all group memberships	Yes	Not granted for Default ...
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Delegated	Read all users' full profiles	Yes	Not granted for Default ...
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for Default ...
User.ReadBasic.All	Application	Read all users' basic profiles	Yes	Not granted for Default ...

When all of your permissions have been granted, your list of permissions should appear similar to:

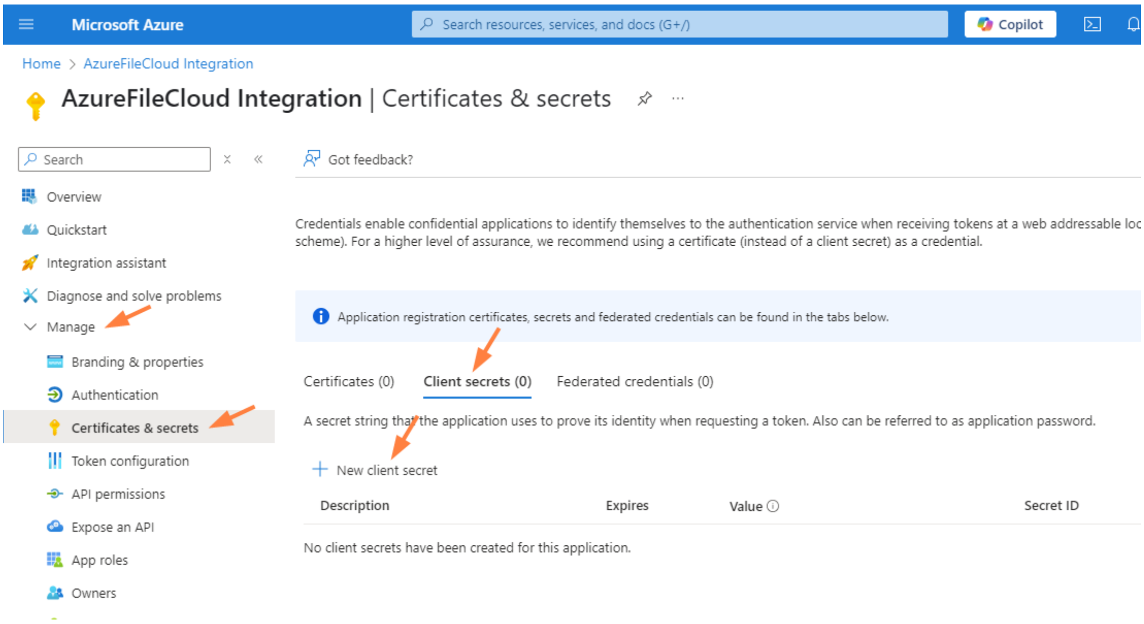


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (10)				
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for FileCloud
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for FileCloud
Group.Read.All	Delegated	Read all groups	Yes	✓ Granted for FileCloud
Group.Read.All	Application	Read all groups	Yes	✓ Granted for FileCloud
GroupMember.Read.All	Delegated	Read group memberships	Yes	✓ Granted for FileCloud
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for FileCloud
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for FileCloud
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for FileCloud
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for FileCloud
User.ReadBasic.All	Application	Read all users' basic profiles	Yes	✓ Granted for FileCloud

11. Now, in the left navigation pane, go to **Manage > Certificates & secrets**, and click the **Client secrets** tab.
12. Click **New client secret**.



Home > AzureFileCloud Integration

AzureFileCloud Integration | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable loc scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | Client secrets (0) | Federated credentials (0)

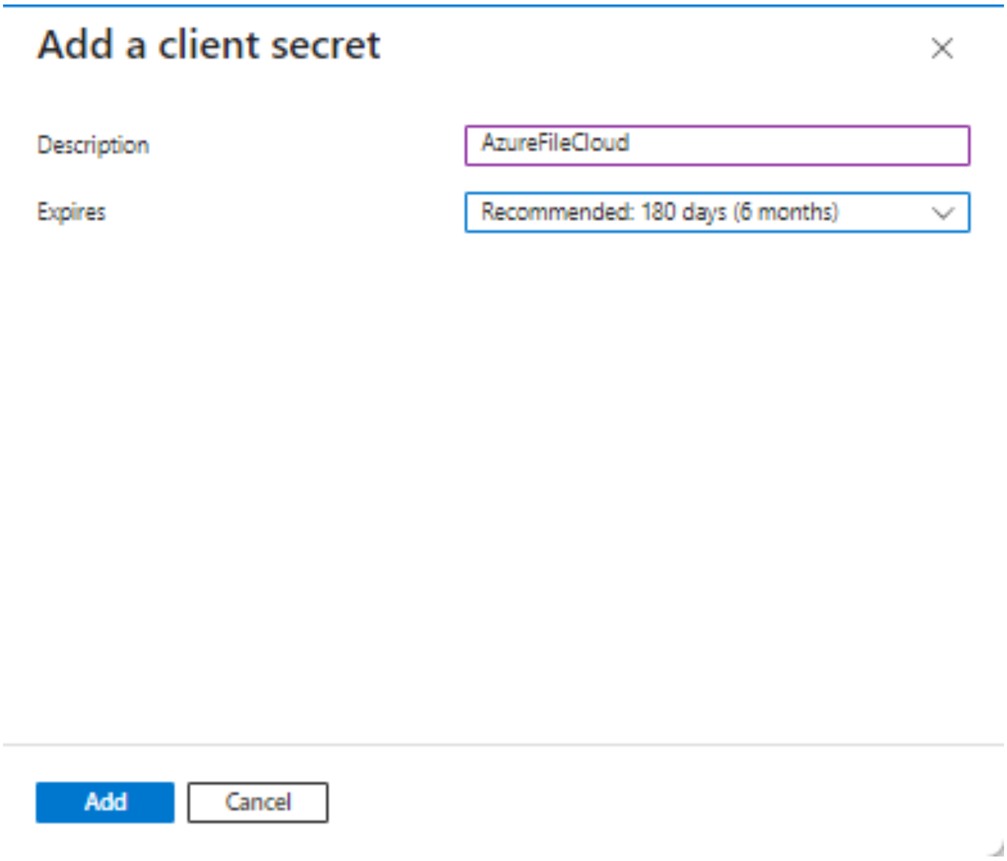
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

13. In the **Add a client secret** box, enter a description for the client secret, and choose an expiration date, then click **Add**.

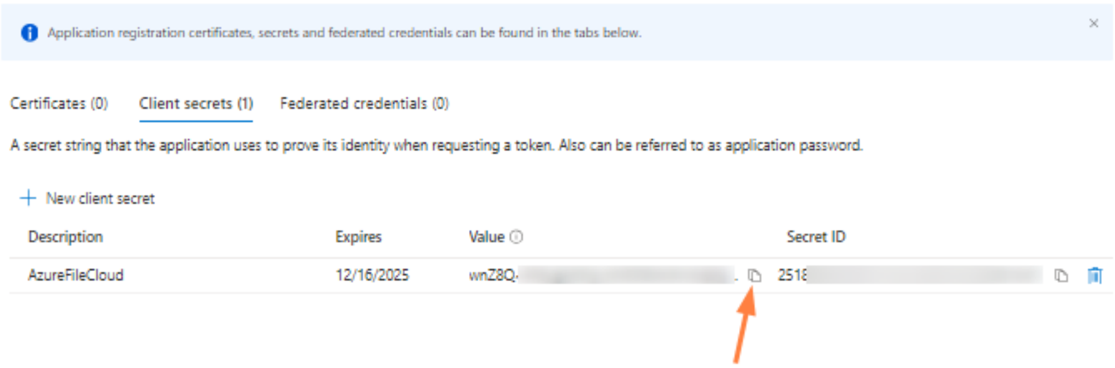


Add a client secret

Description: AzureFileCloud

Expires: Recommended: 180 days (6 months)

14. Click the copy icon next to **Value** and save it. You will use it to fill in the **Client Secret** field in FileCloud.



Application registration certificates, secrets and federated credentials can be found in the tabs below.

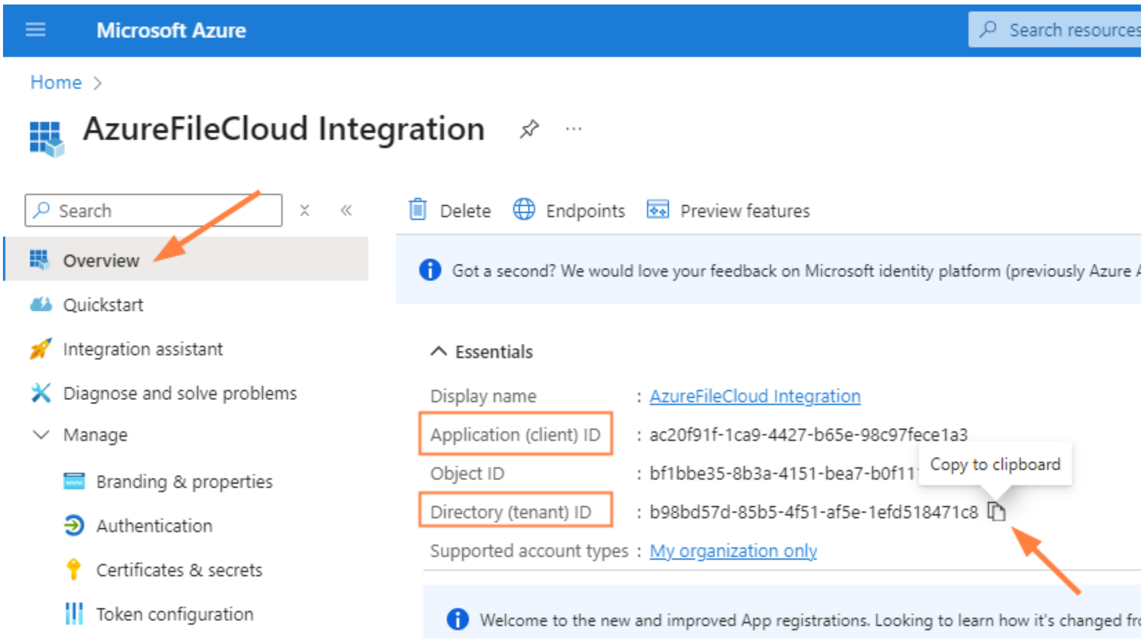
Certificates (0) | Client secrets (1) | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
AzureFileCloud	12/16/2025	wnZ8Q[redacted]	2518[redacted]

15. In the left navigation pane, click **Overview**.
16. Hover over **Directory (tenant) ID** and click the copy icon. Save the **Directory (tenant) ID**. You will use it to fill in the **Tenant ID** field in FileCloud.
17. Hover over **Application (client) ID** and click the copy icon. Save the **Application (client) ID**. You will use it to fill in the **Client ID** field in FileCloud



Got a second? We would love your feedback on Microsoft identity platform (previously Azure

Essentials

Display name : AzureFileCloud Integration
Application (client) ID : ac20f91f-1ca9-4427-b65e-98c97fece1a3
Object ID : bf1bbe35-8b3a-4151-bea7-b0f11
Directory (tenant) ID : b98bd57d-85b5-4f51-af5e-1efd518471c8
Supported account types : My organization only

Welcome to the new and improved App registrations. Looking to learn how it's changed fr

To enter the integration values into the FileCloud side, see SSO API: Configure Import of SSO Groups and Users (see page 38).

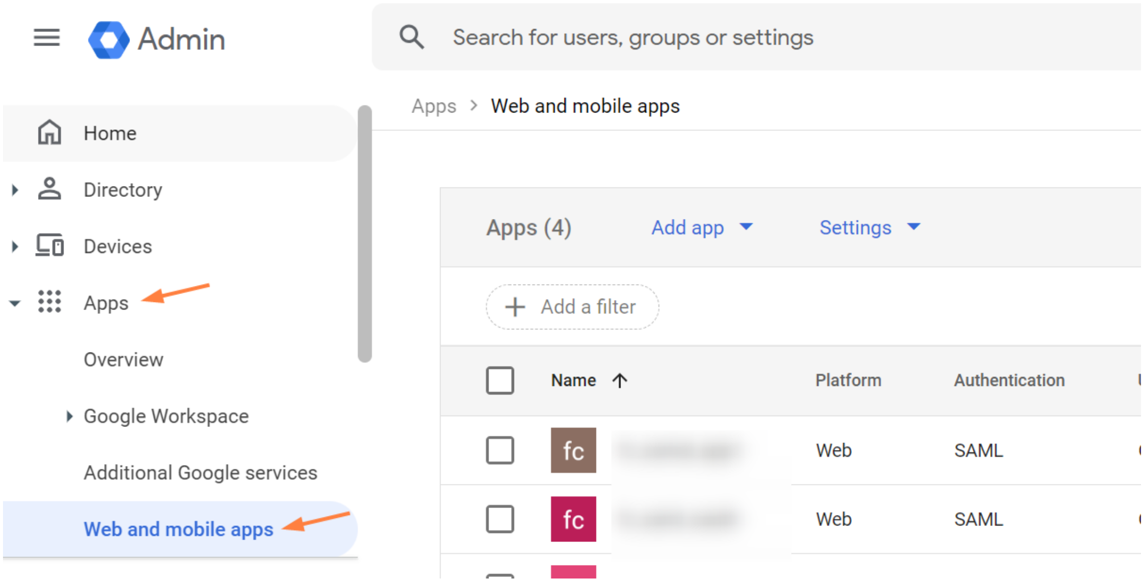
Google: Set up FileCloud Integration for SSO Group/User Import

To configure FileCloud/Google integration in Google for SSO group/user import:

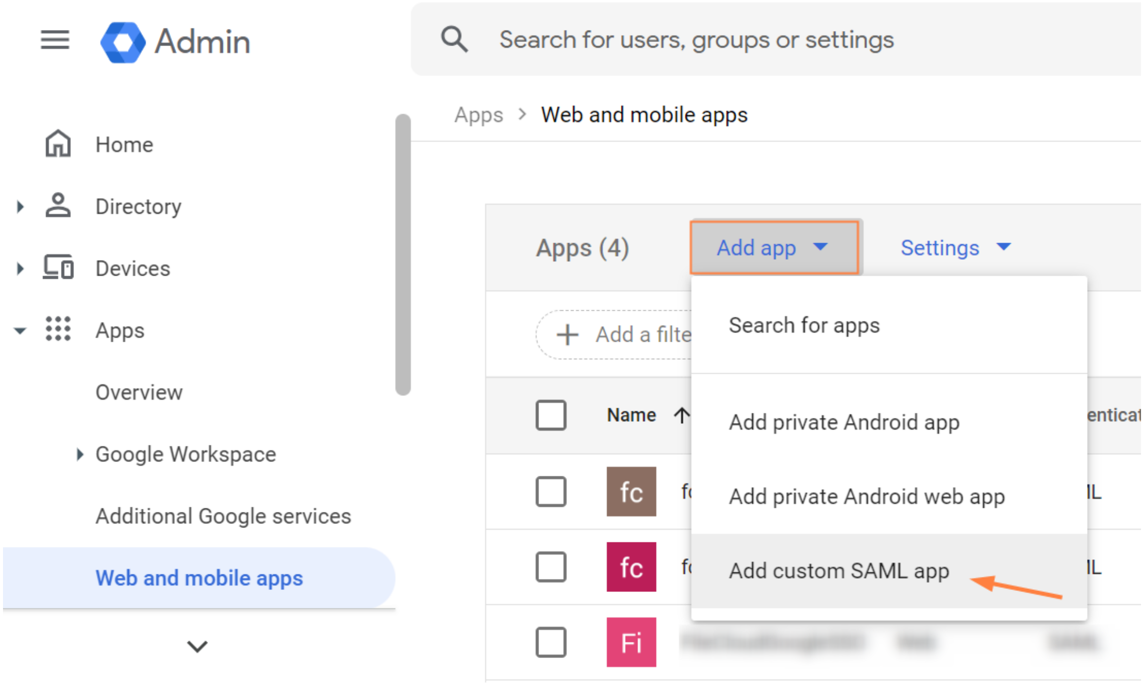
1. Log in to the Google Workspace Admin Center at admin.google.com[3].

[3] http://admin.google.com

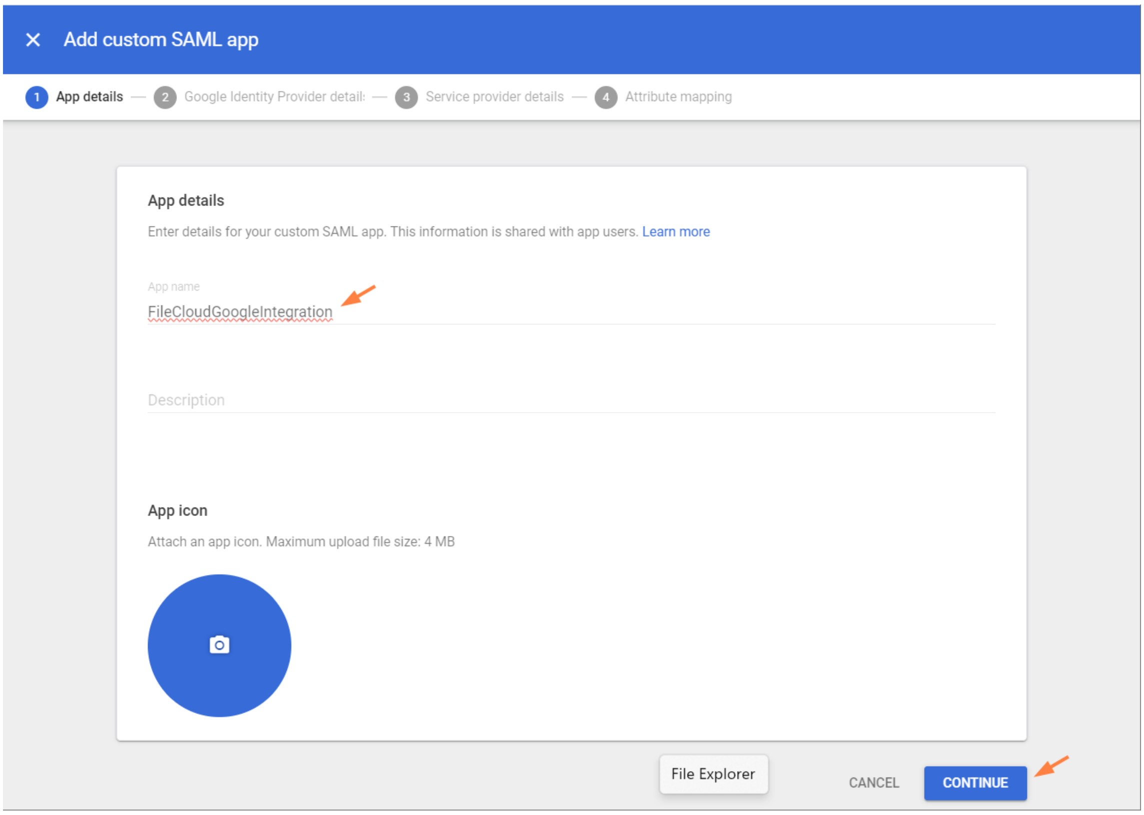
2. In the left navigation pane, go to **Apps > Web and mobile apps**.



3. Click **Add app** and choose **Add custom SAML** app.



4. Enter an **App name**, and click **CONTINUE**.



Add custom SAML app
1 App details — 2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

App details

Enter details for your custom SAML app. This information is shared with app users. Learn more

App name: FileCloudGoogleIntegration

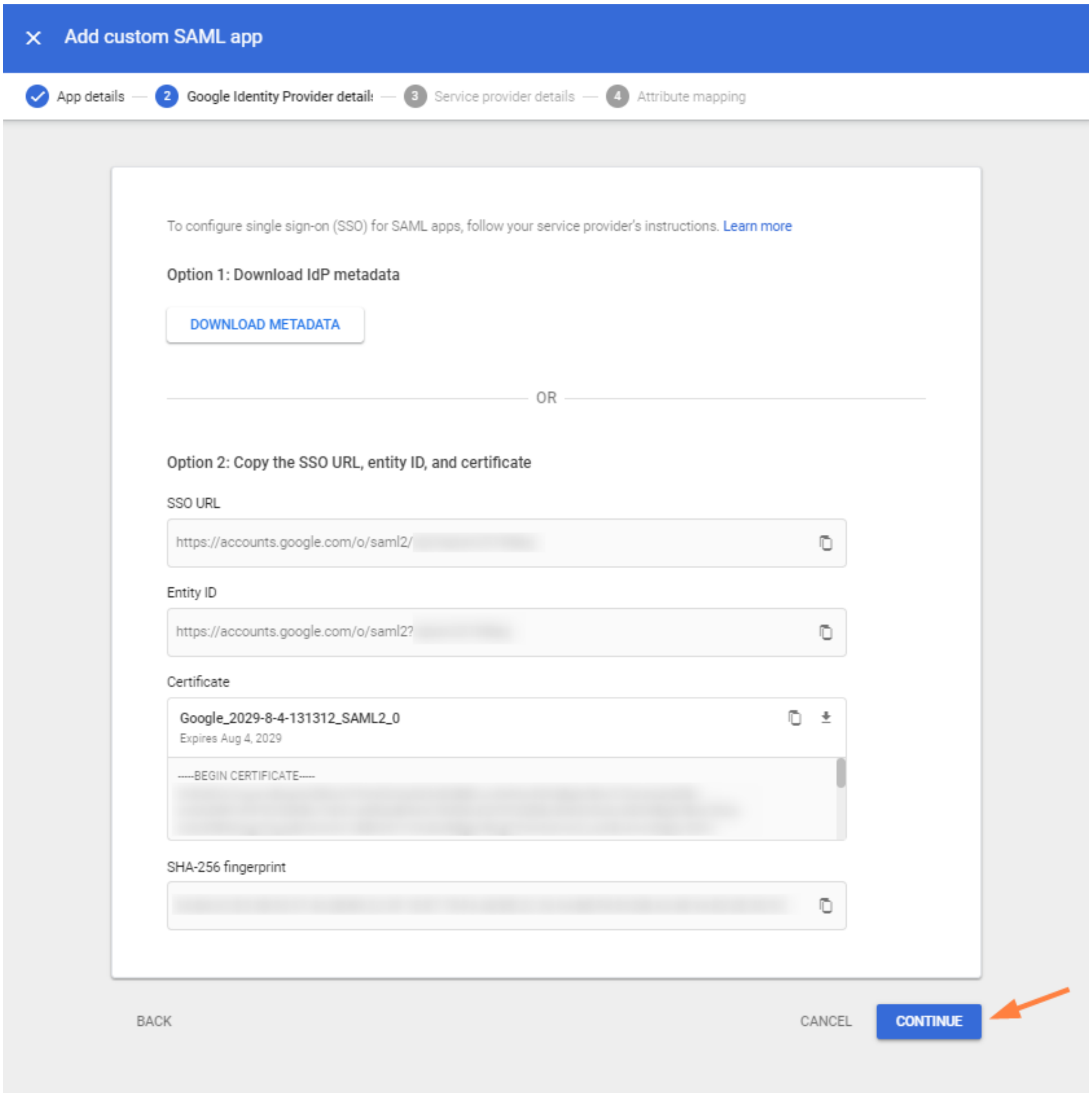
Description

App icon

Attach an app icon. Maximum upload file size: 4 MB

File Explorer
CANCEL
CONTINUE

5. Click **CONTINUE**.



Add custom SAML app

App details — 2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more

Option 1: Download IdP metadata

DOWNLOAD METADATA

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

https://accounts.google.com/o/saml2/[redacted]

Entity ID

https://accounts.google.com/o/saml2?[redacted]

Certificate

Google_2029-8-4-131312_SAML2_0
Expires Aug 4, 2029

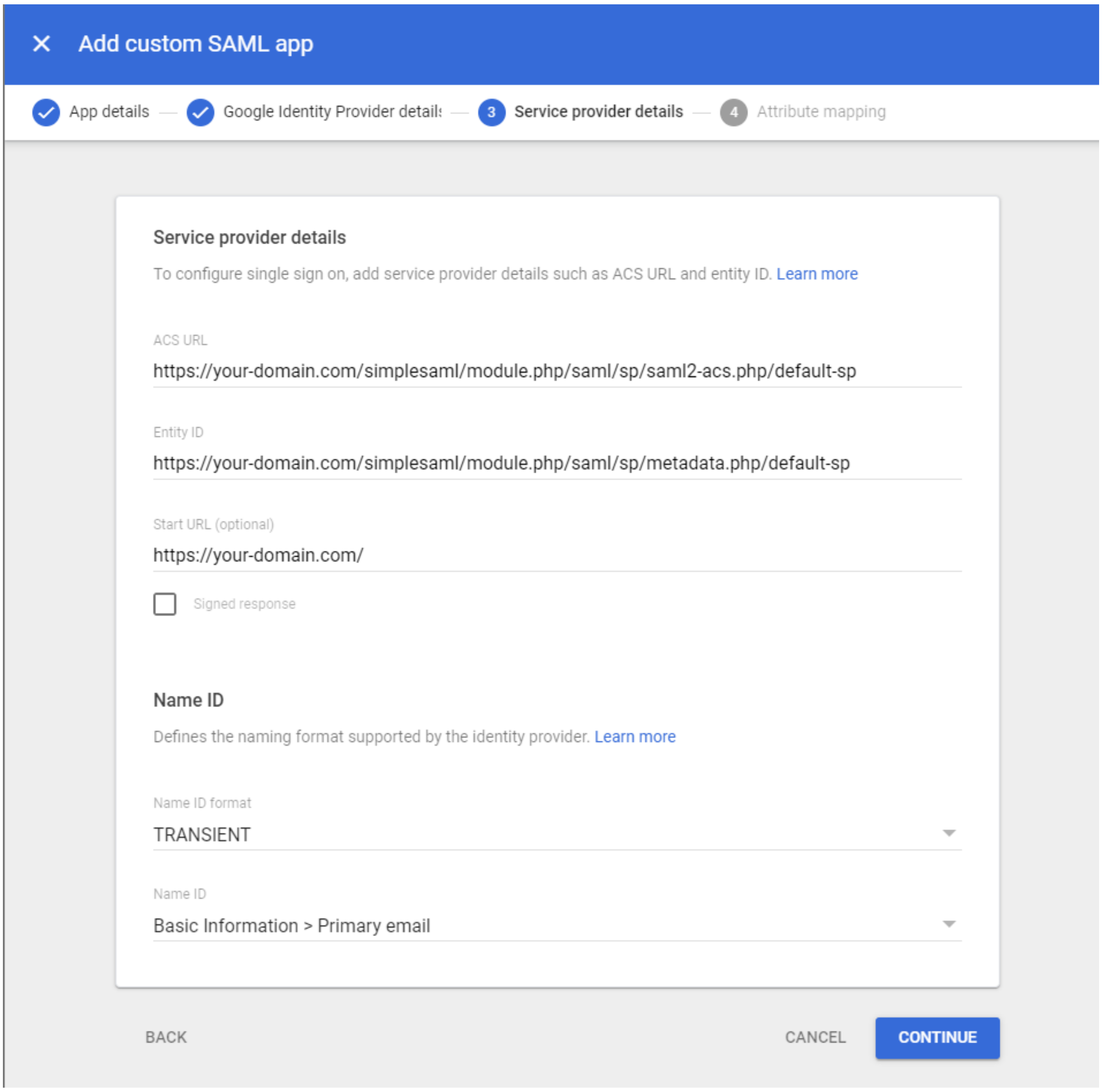
-----BEGIN CERTIFICATE-----
[redacted]

SHA-256 fingerprint

[redacted]

6. Fill in the fields as follows, replacing **your-domain.com**[4]with your FileCloud domain. Click **CONTINUE**.
ACS URL: https://your-domain/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
Entity ID: https://your-domain/simplesaml/module.php/saml/sp/metadata.php/default-sp
Start URL: https://your-domain/
Name ID Format: **TRANSIENT**
NameID: **Basic Information > Primary Email**

[4] http://your-domain.com


× Add custom SAML app
App details — Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL
https://your-domain.com/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp

Entity ID
https://your-domain.com/simplesaml/module.php/saml/sp/metadata.php/default-sp

Start URL (optional)
https://your-domain.com/

□ Signed response

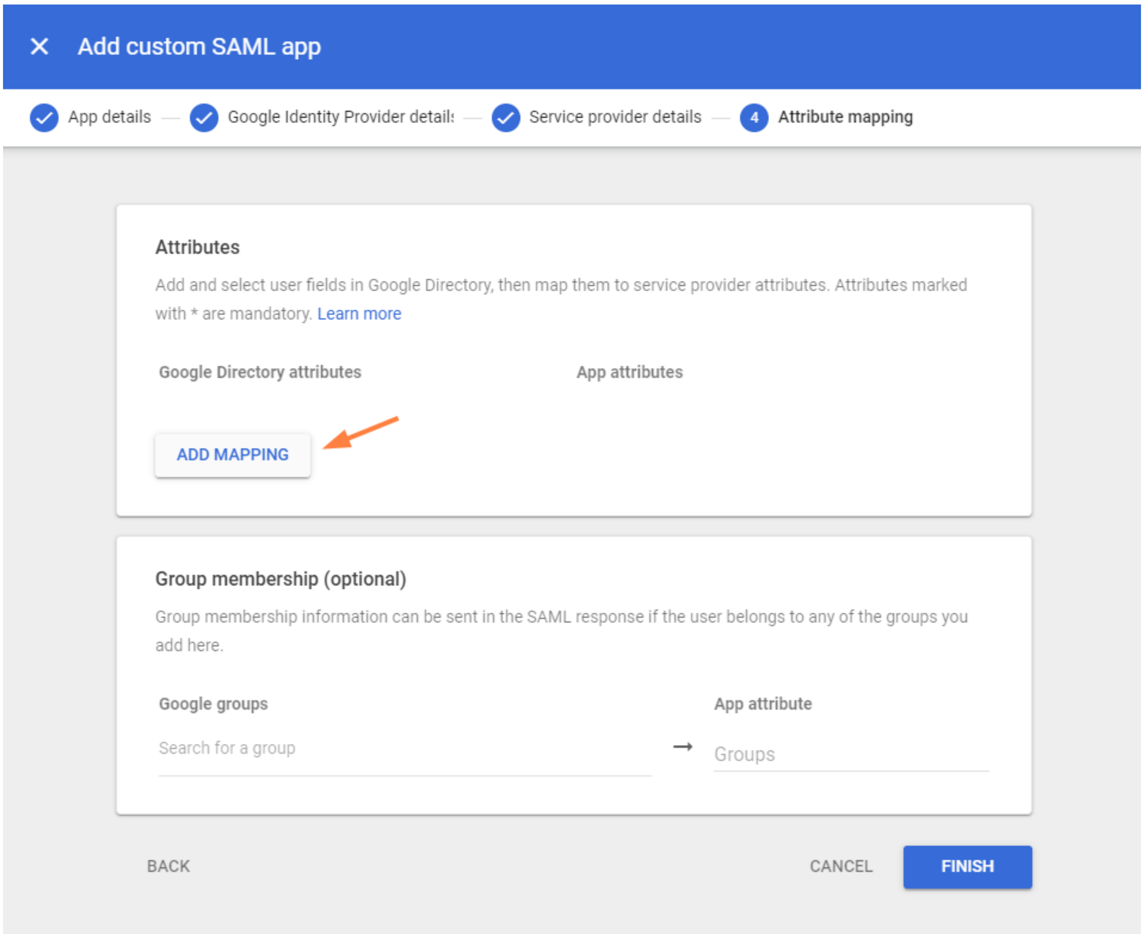
Name ID

Defines the naming format supported by the identity provider. Learn more

Name ID format
TRANSIENT

Name ID
Basic Information > Primary email

7. Click **ADD MAPPING**.



Add custom SAML app

App details — Google Identity Provider detail: — Service provider details — 4 Attribute mapping

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. Learn more

Google Directory attributes

App attributes

ADD MAPPING

Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups

Search for a group

App attribute

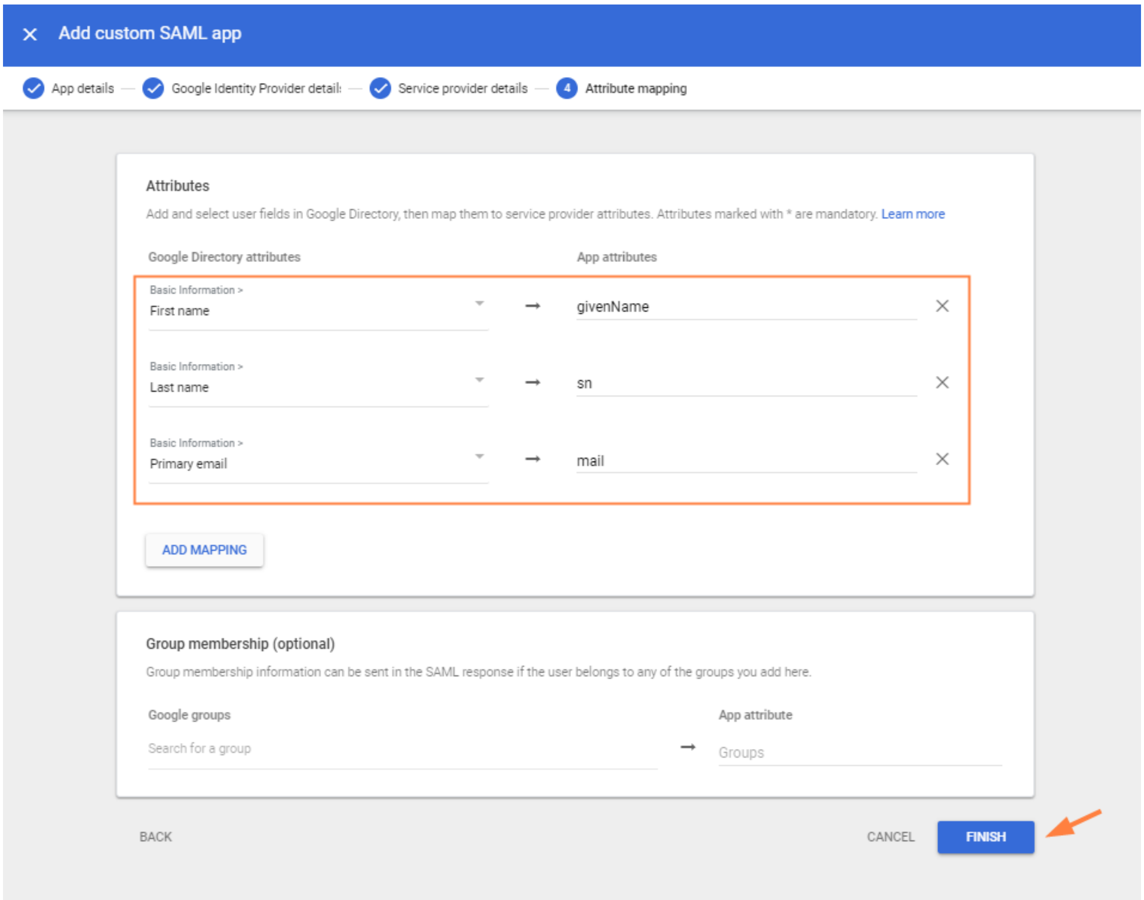
Groups

BACK

CANCEL

FINISH

8. Choose the **Google Directory attributes** below, and add the specific values shown to **App attributes**. Then click **FINISH**.



Add custom SAML app

App details — Google Identity Provider detail: — Service provider details — 4 Attribute mapping

Attributes

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. Learn more

Google Directory attributes		App attributes
Basic Information > First name	→	givenName
Basic Information > Last name	→	sn
Basic Information > Primary email	→	mail

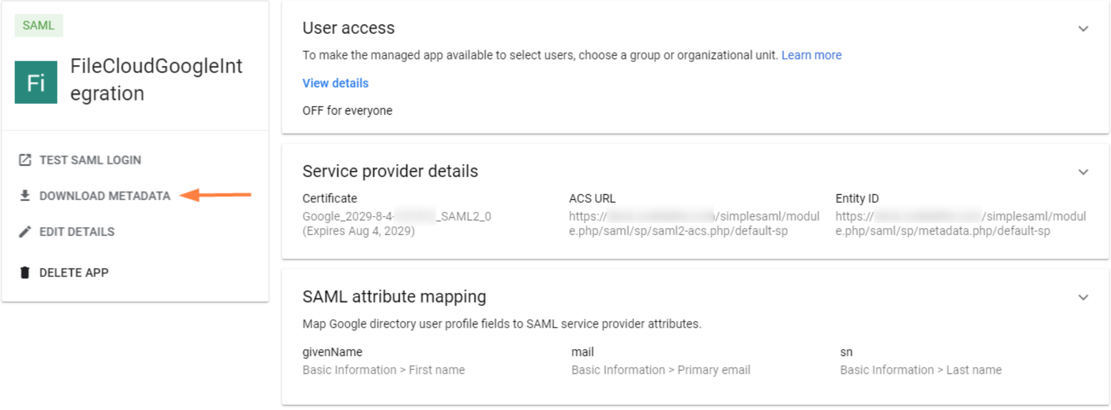
Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.

Google groups		App attribute
Search for a group	→	Groups

You should see a screen similar to the following.

9. Click **DOWNLOAD METADATA**.



FileCloudGoogleIntegration

User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

OFF for everyone

Service provider details

Certificate	ACS URL	Entity ID
Google_2029-8-4-[redacted]_SAML2_0 (Expires Aug 4, 2029)	https://[redacted]/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp	https://[redacted]/simplesaml/module.php/saml/sp/metadata.php/default-sp

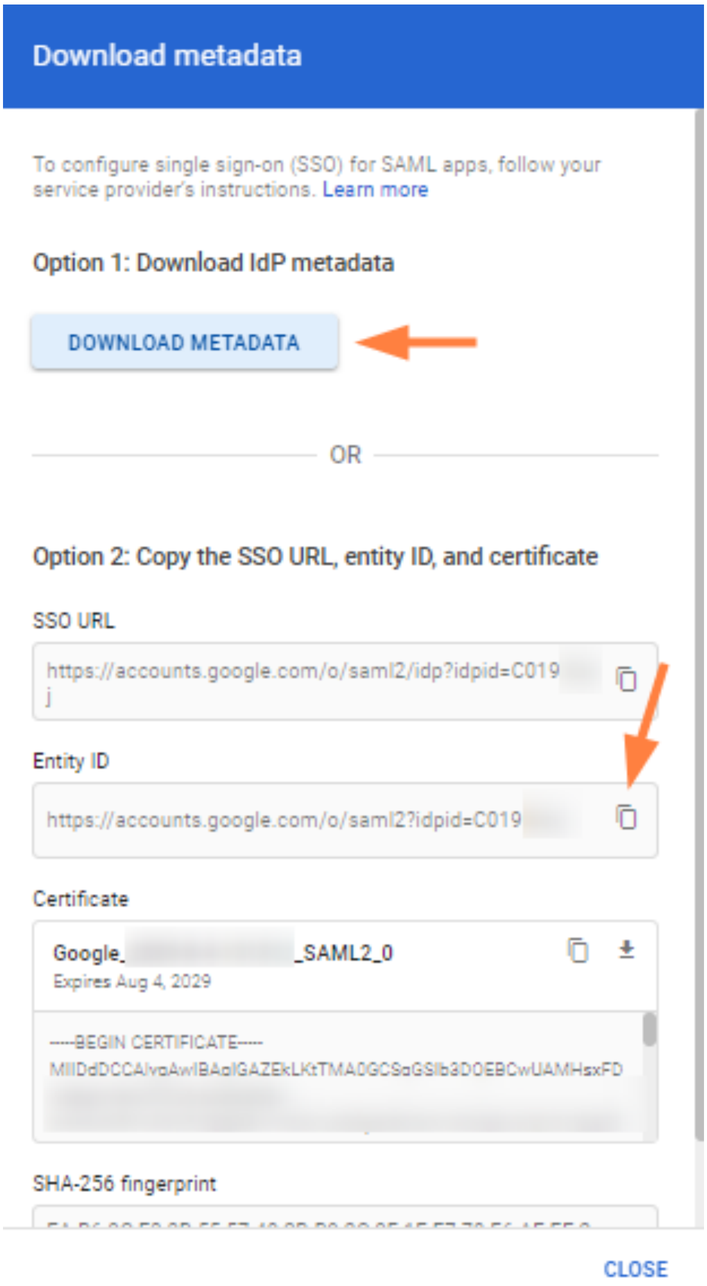
SAML attribute mapping

Map Google directory user profile fields to SAML service provider attributes.

givenName	mail	sn
Basic Information > First name	Basic Information > Primary email	Basic Information > Last name

10. In the **Download metadata** popup, click **DOWNLOAD METADATA**.
    The file **GoogleIDPMetadata.xml** is automatically downloaded.

11. Click the copy icon next to **Entity ID**, and save it. You will need it to complete your configuration in FileCloud.



Download metadata

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more

Option 1: Download IdP metadata

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL: https://accounts.google.com/o/saml2/idp?idpid=C019[redacted]j

Entity ID: https://accounts.google.com/o/saml2?idpid=C019[redacted]

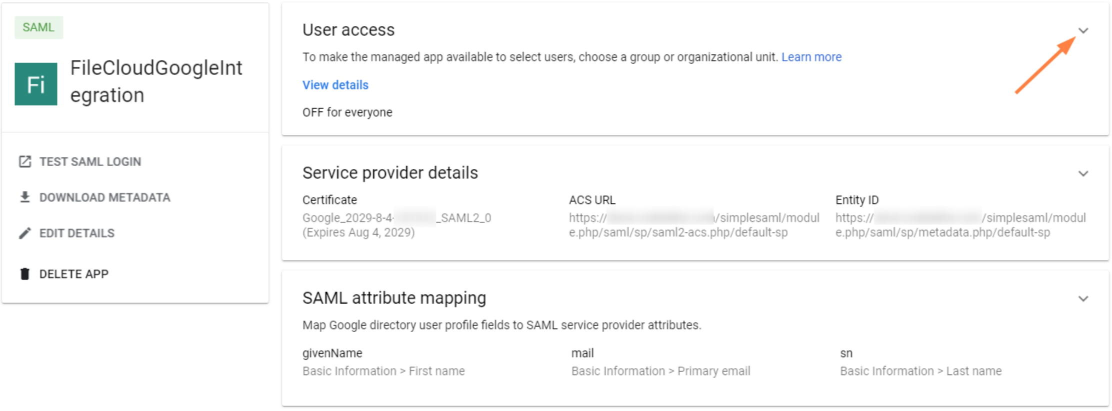
Certificate: Google_[redacted]_SAML2_0
Expires Aug 4, 2029

```
-----BEGIN CERTIFICATE-----
MIIDdDCCAlygAwIBAgIGAZEkLKtTMA0GCSqGSIb3DQEBCwUAMHsxFD
```

[redacted]

SHA-256 fingerprint

12. Click **CLOSE**.
13. Click the down arrow in the User access box.



User access

To make the managed app available to select users, choose a group or organizational unit. Learn more

View details

OFF for everyone

Service provider details

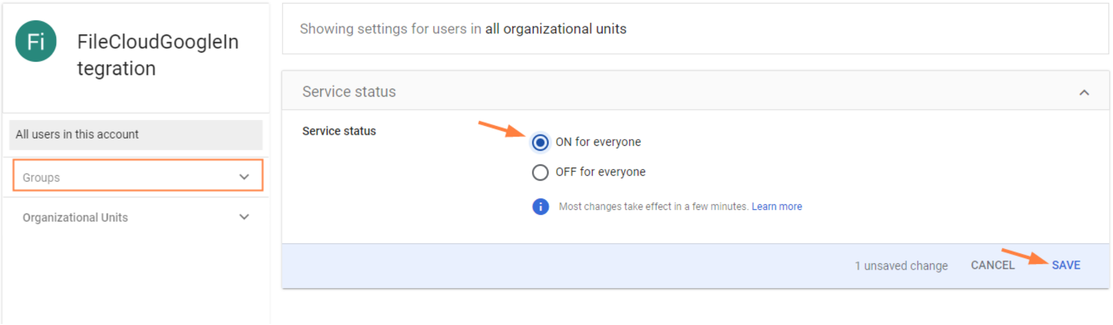
Certificate	ACS URL	Entity ID
Google_2029-8-4-[redacted]_SAML2_0 (Expires Aug 4, 2029)	https://[redacted]/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp	https://[redacted]/simplesaml/module.php/saml/sp/metadata.php/default-sp

SAML attribute mapping

Map Google directory user profile fields to SAML service provider attributes.

givenName	mail	sn
Basic Information > First name	Basic Information > Primary email	Basic Information > Last name

14. Select **ON for everyone**.
    If you want to only enable this for certain groups, click the **Groups** down arrow and add the groups.



Showing settings for users in all organizational units

Service status

Service status ● ON for everyone ○ OFF for everyone

Most changes take effect in a few minutes. Learn more

1 unsaved change

15. Click **SAVE.**

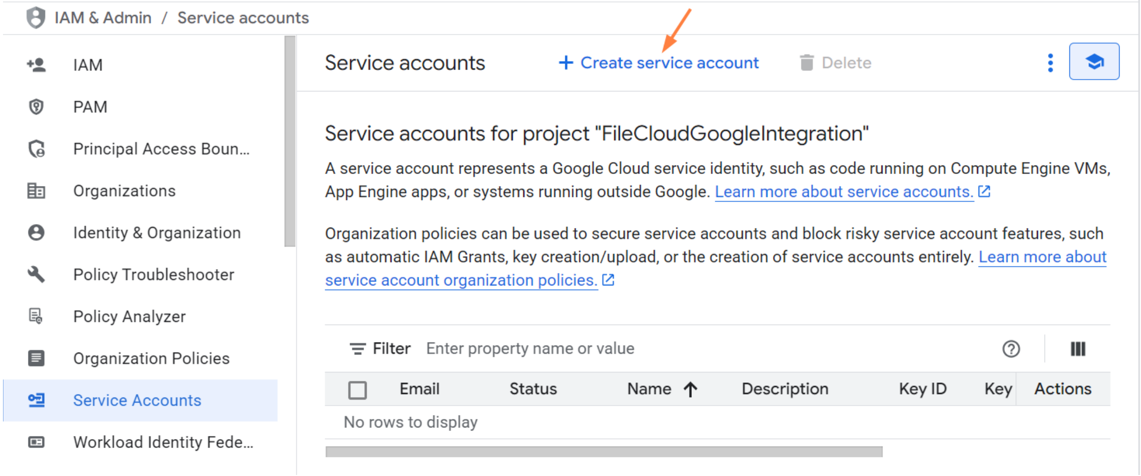
Now, create a key file and grant OAuth scopes.

Create a key file and grant FileCloud access to Google

Using your superadmin account, create a service account that grants FileCloud the necessary access to the Google api for SSO authentication. If you do not have a superadmin account, have a superadmin perform the following steps for you.

To create the service account:

1. Log in to https://console.cloud.google.com/iam-admin/serviceaccounts.
2. Select your project, or create a new one.
3. Click **Create service account**.



Service accounts for project "FileCloudGoogleIntegration"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

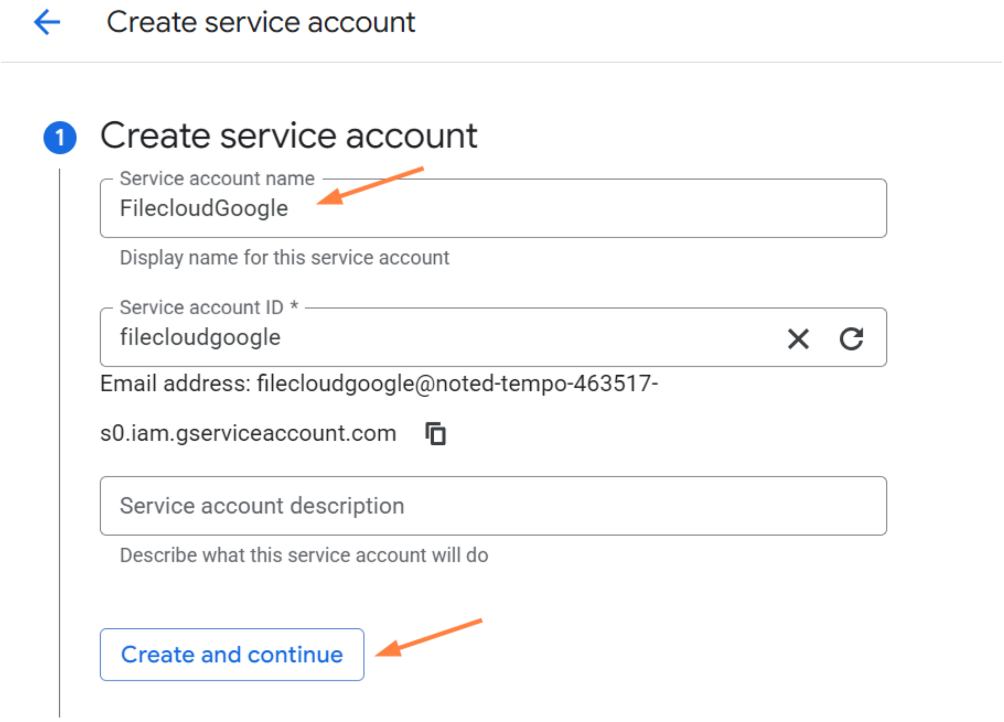
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

Filter Enter property name or value

□	Email	Status	Name ↑	Description	Key ID	Key	Actions

No rows to display

4. Enter a **Service account name** and click **Create and continue**.



Service account name: FilecloudGoogle

Display name for this service account

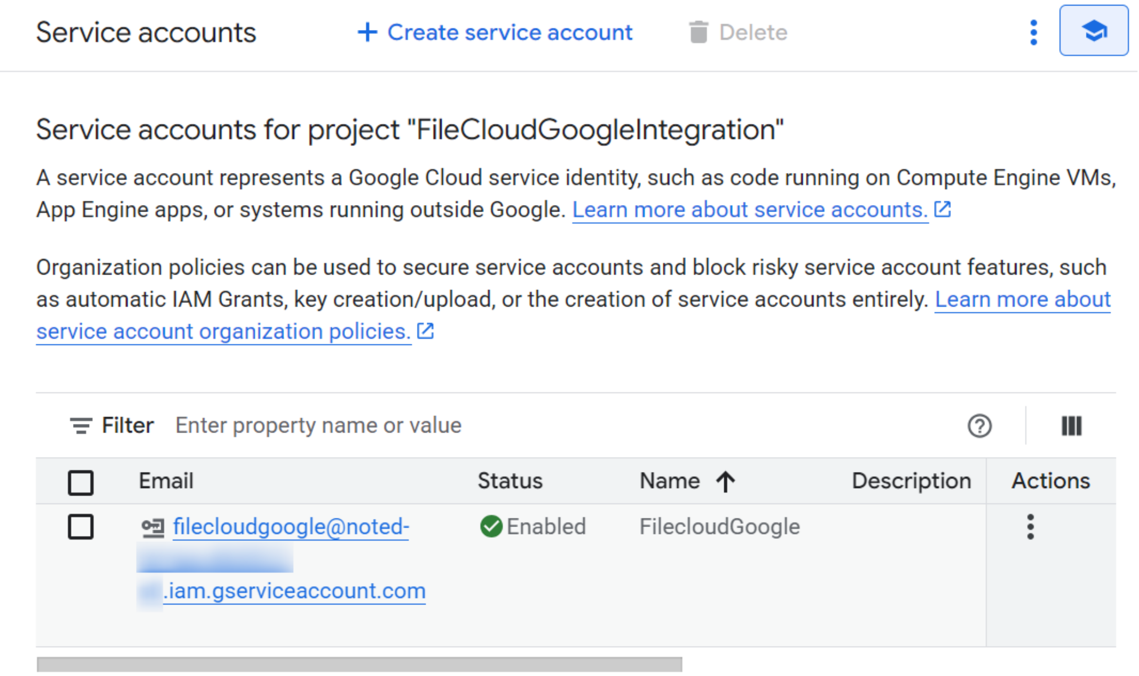
Service account ID *: filecloudgoogle

Email address: filecloudgoogle@noted-tempo-463517-s0.iam.gserviceaccount.com

Service account description

Describe what this service account will do

5. Continue through the **Permissions** and the **Principals with access** sections without entering any values, and click **Done**.
   The service account is saved.



Service accounts for project "FileCloudGoogleIntegration"

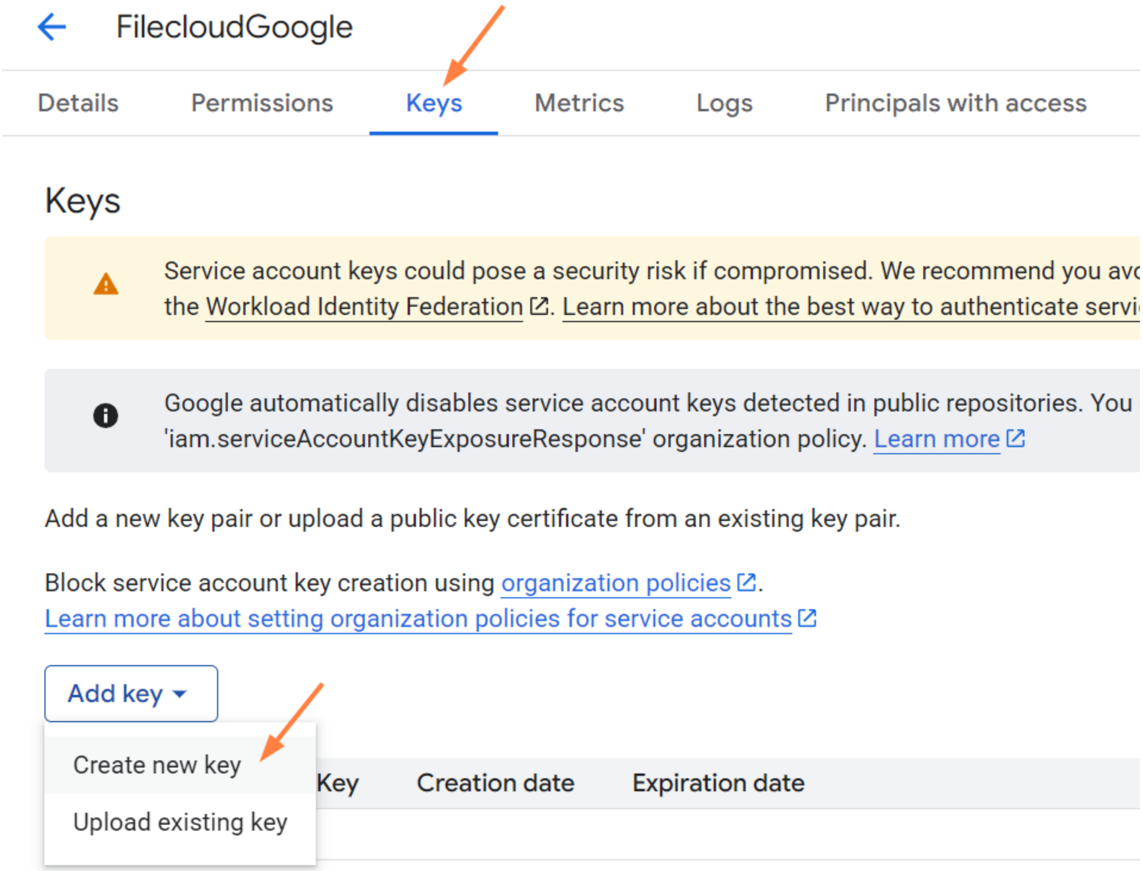
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

□	Email	Status	Name ↑	Description	Actions
□	filecloudgoogle@noted-[redacted].iam.gserviceaccount.com	✓ Enabled	FilecloudGoogle		⋮

Create and download the private key file

1. On the Service accounts page, click the service account you created.
2. Click the **Keys** tab, and then click **Add key** and choose **Create new key**.



FilecloudGoogle

Keys

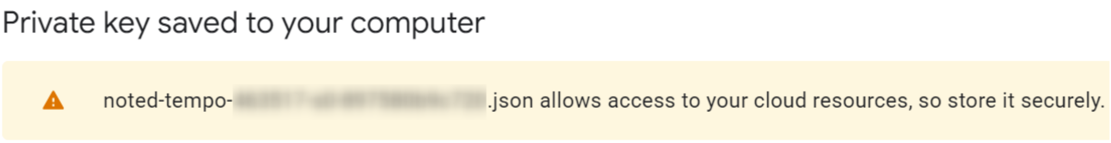
Service account keys could pose a security risk if compromised. We recommend you avo
the Workload Identity Federation. Learn more about the best way to authenticate servi

Google automatically disables service account keys detected in public repositories. You
'iam.serviceAccountKeyExposureResponse' organization policy. Learn more

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

3. Select **JSON**, and click **Create**.
   The private key file is saved in a json file. Note its name so you are able to upload it later when you set up Google/FileCloud SSO integration in FileCloud.



Private key saved to your computer

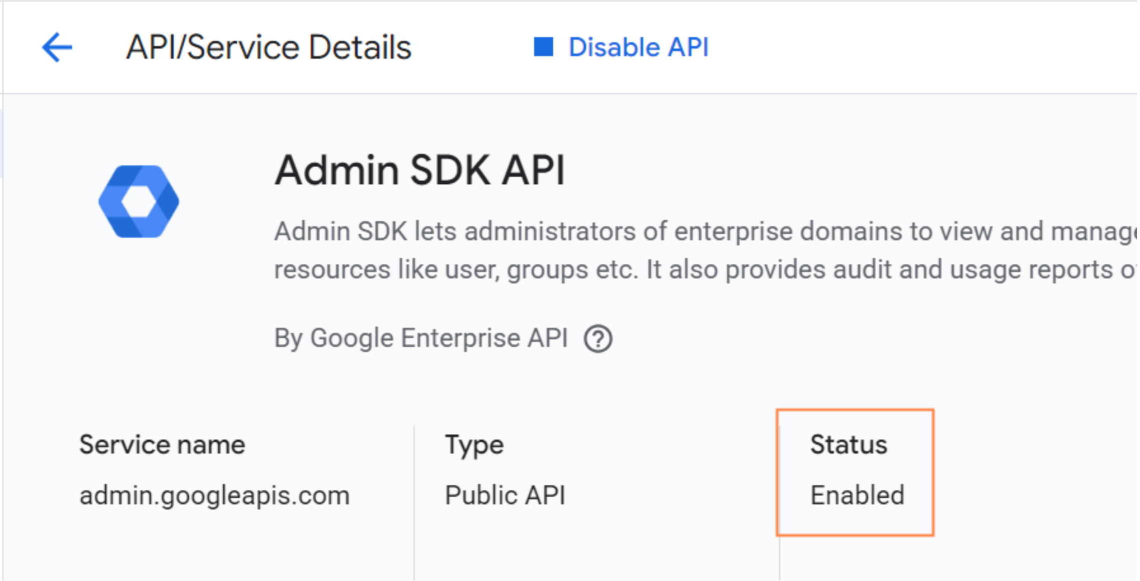
noted-tempo-[redacted].json allows access to your cloud resources, so store it securely.

To enter the values into the FileCloud side, see SSO API: Configure Import of SSO Groups and Users.

Enable the Admin SDK API library

1. Go to https://console.cloud.google.com/apis/library
2. Search for **Admin SDK**.

3. Click it, and then click **Enable**.
   Status should appear as **Enabled**.



← API/Service Details

Disable API

Admin SDK API

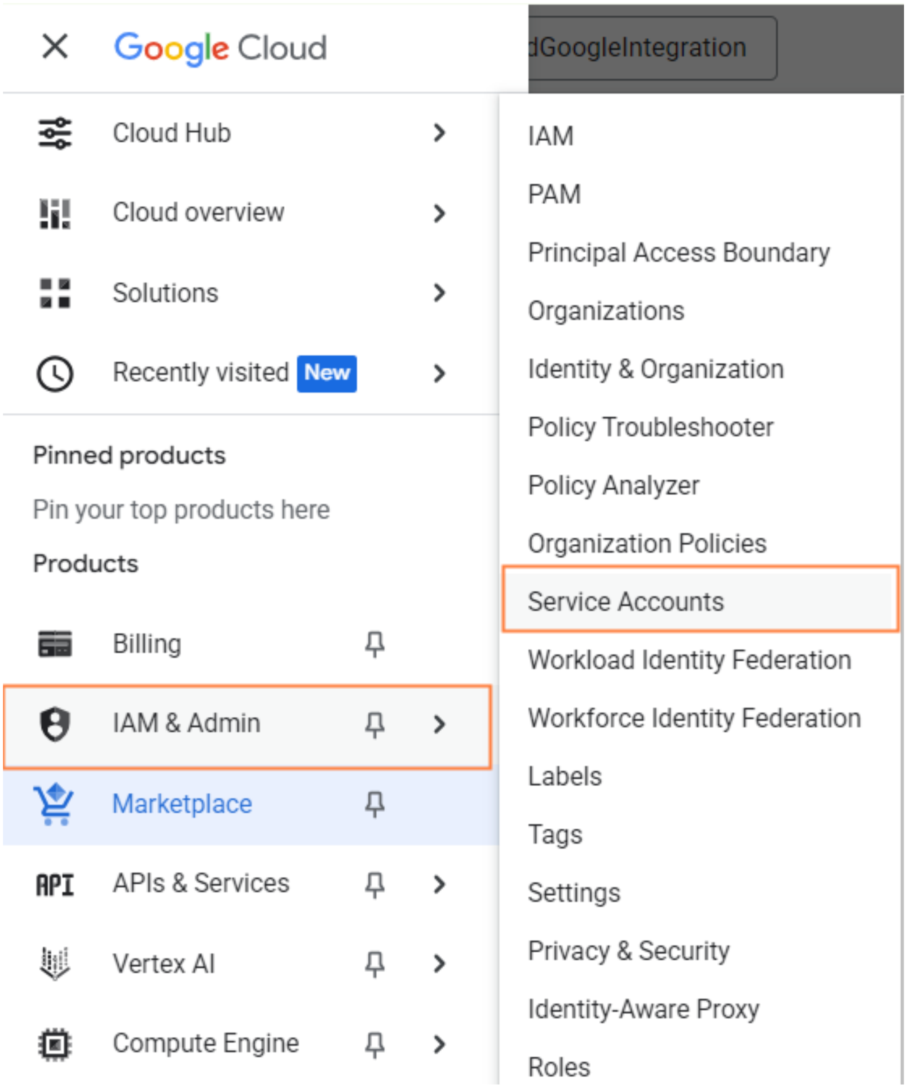
Admin SDK lets administrators of enterprise domains to view and manag resources like user, groups etc. It also provides audit and usage reports o

By Google Enterprise API

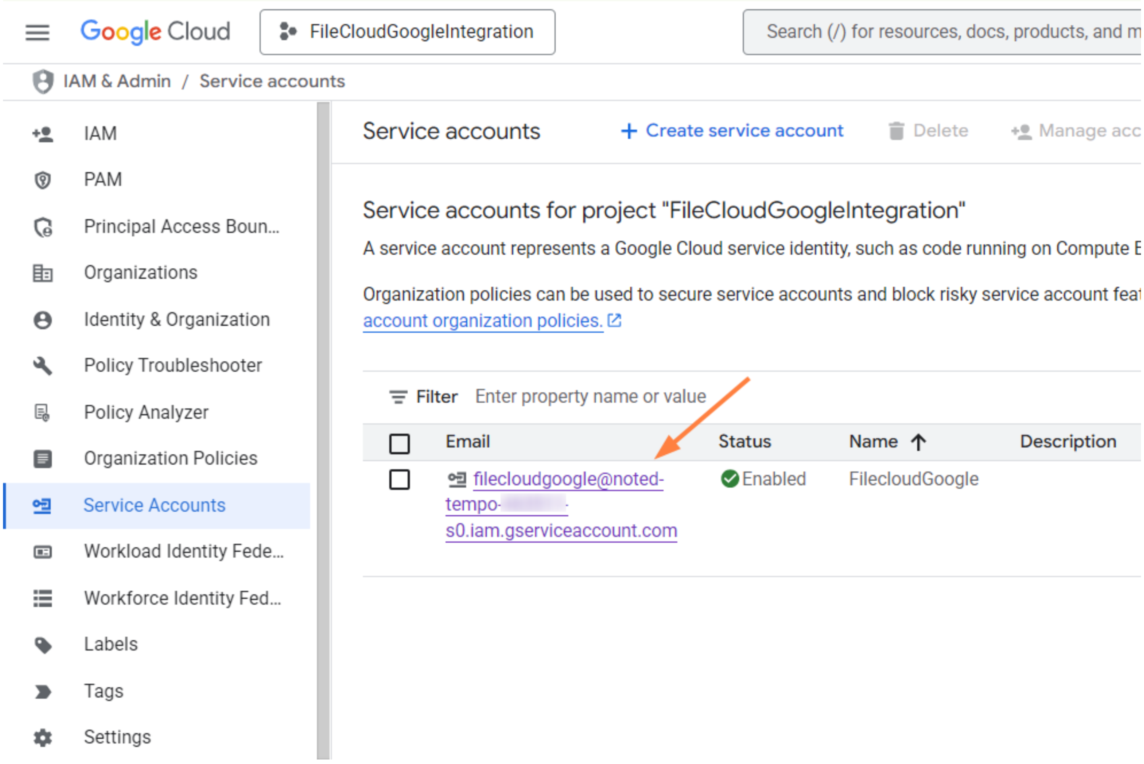
Service name	Type	Status
admin.googleapis.com	Public API	Enabled

Get the service account Client ID:

1. In the left navigation pane, go to **IAM & Admin > Service Accounts**.



2. Click your service account to open it.



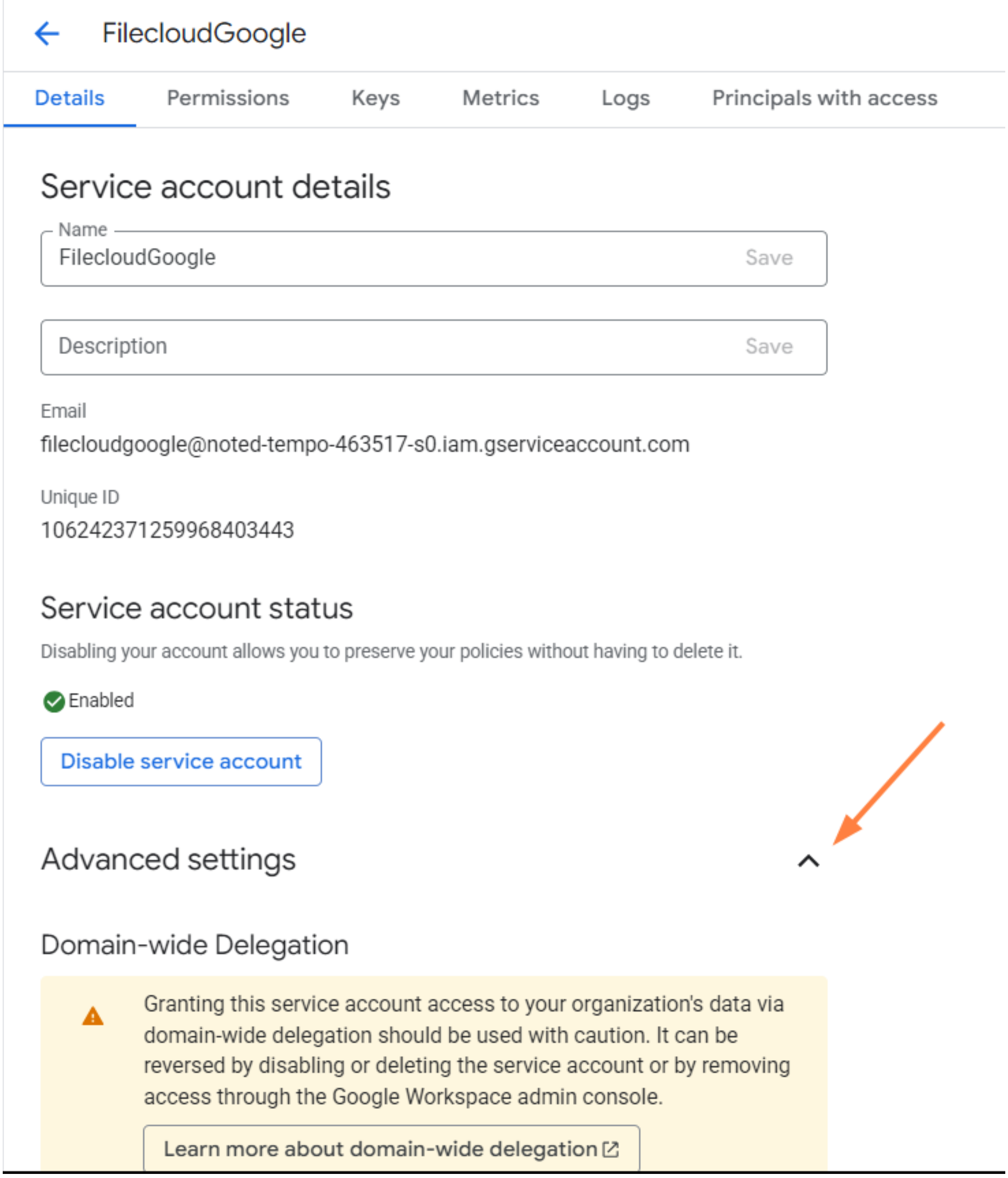
Service accounts for project "FileCloudGoogleIntegration"

A service account represents a Google Cloud service identity, such as code running on Compute E

Organization policies can be used to secure service accounts and block risky service account feat account organization policies.

☐	Email	Status	Name ↑	Description
☐	filecloudgoogle@noted-tempo-[redacted]-s0.iam.gserviceaccount.com	✓ Enabled	FilecloudGoogle	

3. At the bottom of the page, click **Advanced settings.**



Service account details

Name: FilecloudGoogle

Description

Email
filecloudgoogle@noted-tempo-463517-s0.iam.gserviceaccount.com

Unique ID
106242371259968403443

Service account status

Disabling your account allows you to preserve your policies without having to delete it.

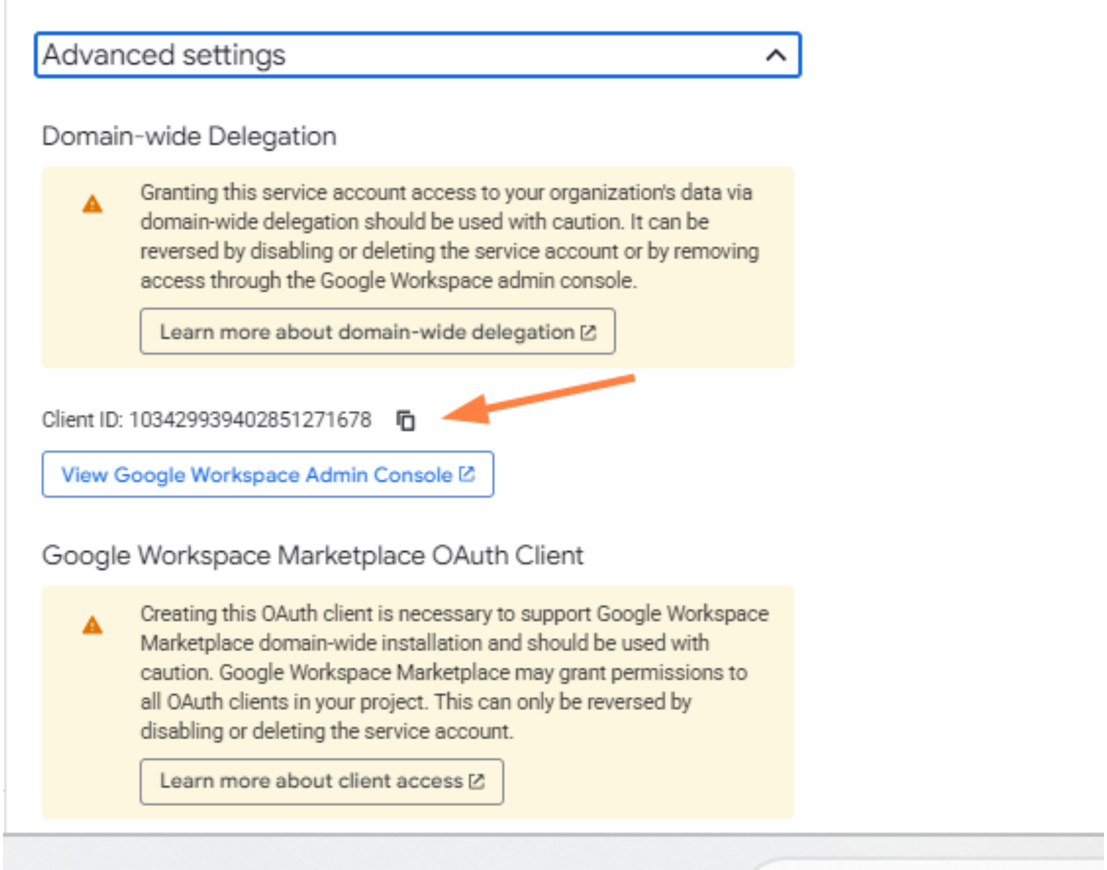
Enabled

Advanced settings

Domain-wide Delegation

Granting this service account access to your organization's data via domain-wide delegation should be used with caution. It can be reversed by disabling or deleting the service account or by removing access through the Google Workspace admin console.

4. Click the copy icon next to **Client ID**, and save it.



Advanced settings

Domain-wide Delegation

Granting this service account access to your organization's data via domain-wide delegation should be used with caution. It can be reversed by disabling or deleting the service account or by removing access through the Google Workspace admin console.

Learn more about domain-wide delegation

Client ID: 103429939402851271678

View Google Workspace Admin Console

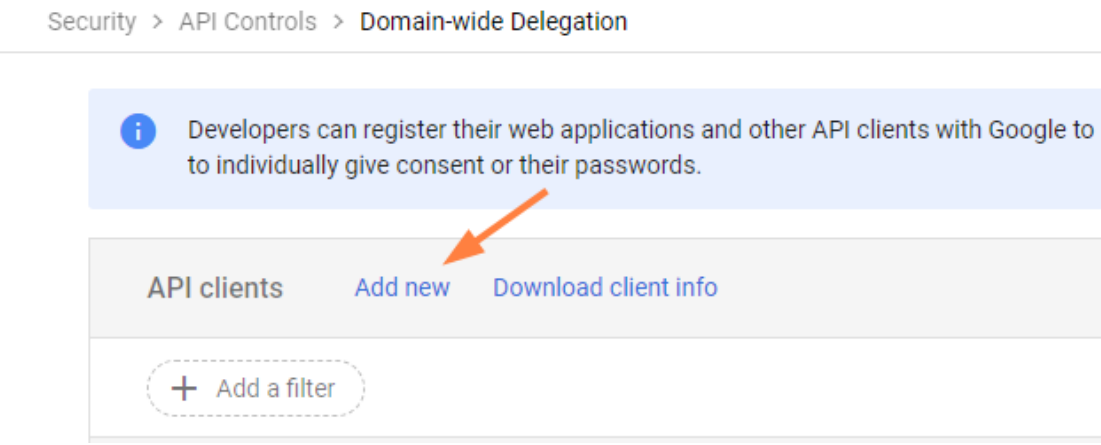
Google Workspace Marketplace OAuth Client

Creating this OAuth client is necessary to support Google Workspace Marketplace domain-wide installation and should be used with caution. Google Workspace Marketplace may grant permissions to all OAuth clients in your project. This can only be reversed by disabling or deleting the service account.

You will paste it into the **Client ID** field in the next section.

Grant OAuth Scopes via the Admin Console

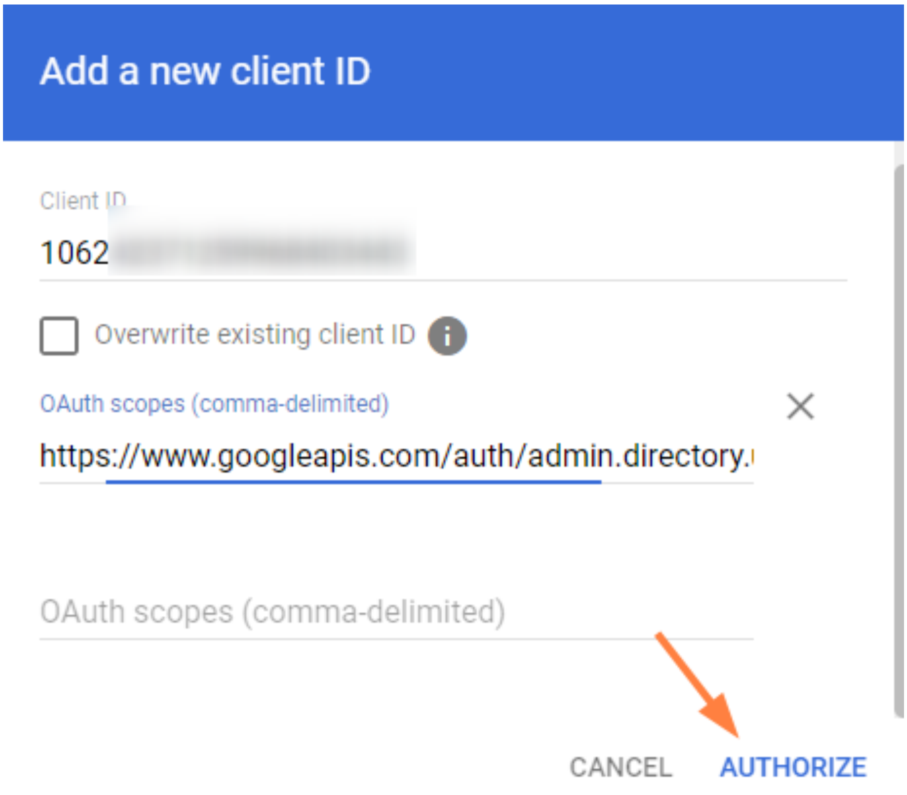
1. Log back into Google Workspace Admin Center and go to https://admin.google.com/ac/owl/domainwidedelegation.
2. Click **Add new**.



Security > API Controls > Domain-wide Delegation

Developers can register their web applications and other API clients with Google to to individually give consent or their passwords.

3. In the **Add a new client ID** dialog box, and enter the following values:
   Client ID - Enter the Client ID you saved in the previous section from https://console.cloud.google.com[5].
   OAuth scopes - Enter the following as a string with the commas included:
   https://www.googleapis.com/auth/admin.directory.user.readonly,
   https://www.googleapis.com/auth/admin.directory.group.readonly,
   https://www.googleapis.com/auth/admin.directory.group.member.readonly
4. Click **AUTHORIZE**.



Add a new client ID

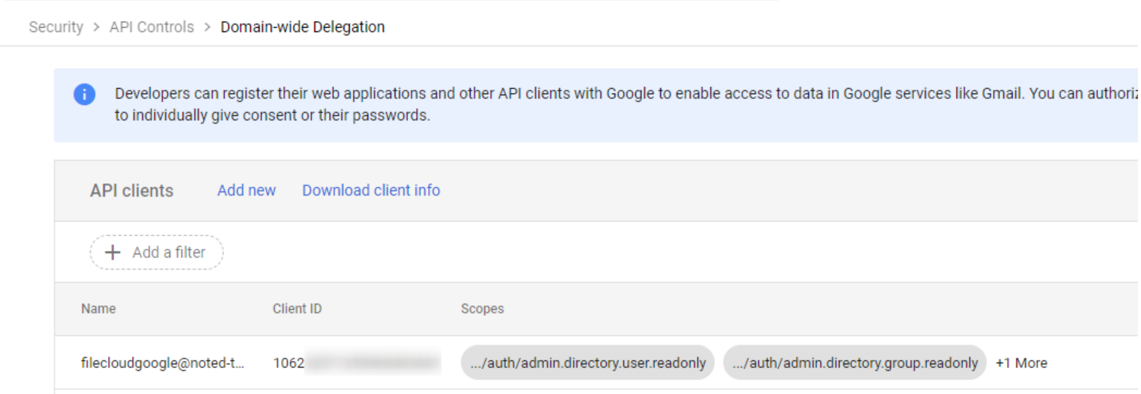
Client ID
1062[redacted]

☐ Overwrite existing client ID

OAuth scopes (comma-delimited)
https://www.googleapis.com/auth/admin.directory.

OAuth scopes (comma-delimited)

5. The OAuth scopes are now added to the Client ID.



Security > API Controls > Domain-wide Delegation

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authoriz
to individually give consent or their passwords.

Name	Client ID	Scopes
filecloudgoogle@noted-t...	1062[redacted]	.../auth/admin.directory.user.readonly .../auth/admin.directory.group.readonly +1 More

[5] https://console.cloud.google.com/iam-admin/serviceaccounts

To enter the integration values into the FileCloud side, see SSO API: Configure Import of SSO Groups and Users[6].

[6] https://www.filecloud.com/supportdocs/spaces/FCDOC/pages/288653318/.SSO+API+Configure+Import+of+SSO+Groups+and+Users+v23.251

CASB integration

> For security purposes, to initially access the API, you must now change the default API key. If you do not change it, when you enter a command to call the API, an error is returned.
> **Note**: You are only required to change the default API key initially; after that, you can continue to use the new key you entered.

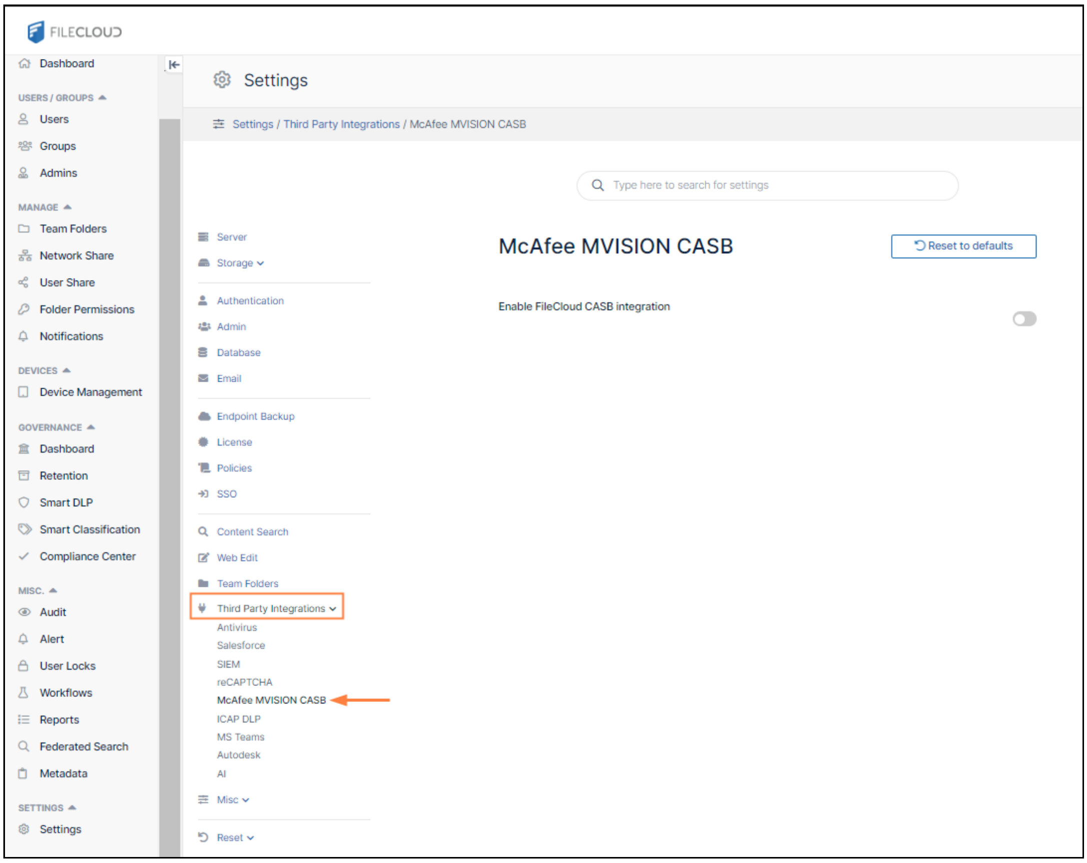
FileCloud includes a smart data leak prevention (DLP) functionality that monitors user actions and and prevents them if they pose a security risk.

In Version 20.2, FileCloud has added integration with external cloud access security broker (CASB) software to enable you to expand your DLP monitoring and risk prevention. This enables you to expand activity monitoring and measures taken when there is a possible security breach.

Currently, FileCloud supports integration with McAfee CASB software.

To enable CASB integration with FileCloud:

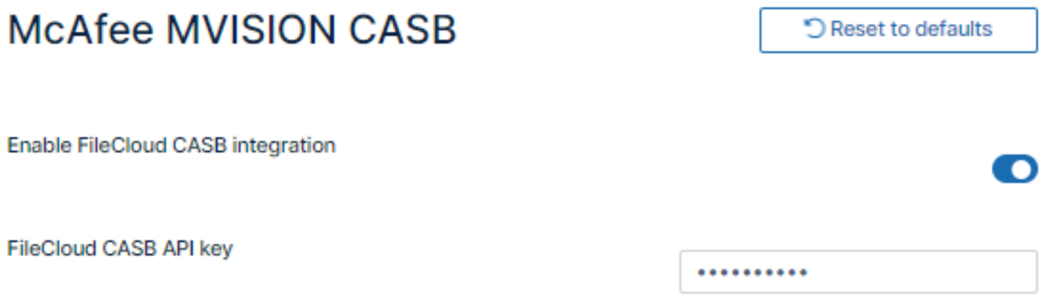
1. Open the McAfee MVISION CASB settings page.
   To go to the McAfee MVISION CASB settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the Settings navigation page, click Third Party Integrations 🧩.
   b. In the inner navigation bar on the left of the Third Party Integrations page, expand the **Third Party Integrations** menu, and click **McAfee MVISION CASB**, as shown below.



McAfee MVISION CASB

Enable FileCloud CASB integration ○

2. Check **Enable FileCloud CASB** Integration.
   The field **FileCloud CASB API Key** appears.



McAfee MVISION CASB

Enable FileCloud CASB integration ●

FileCloud CASB API key ••••••••••

3. Change the value of **FileCloud CASB API key** to any alphanumeric string.
4. Click **Save**.
5. Add the value of the **FileCloud CASB API key** to McAfee MVISION CASB. See McAfee's product documentation[7]for instructions.

McAfee CASB integration (see page 92)

[7] https://docs.mcafee.com/

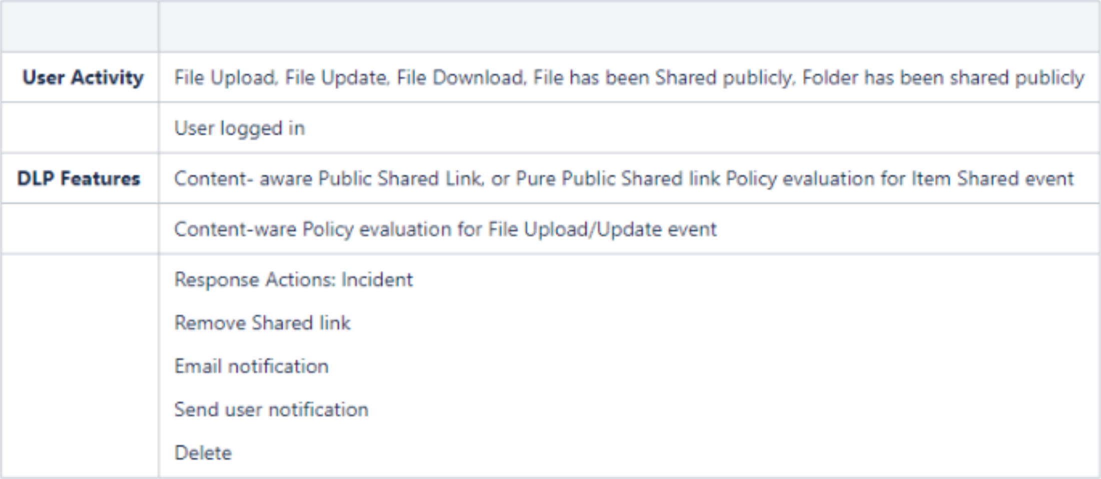
McAfee CASB integration

Beginning with version 20.2, FileCloud supports integration with McAfee CASB.

This enables you to use McAfee CASB to apply extensive DLP rules when monitoring user events such as actions on files and folders and logins to the system. If a CASB DLP rule is violated, McAfee takes actions such as notifying a user, deleting a file, or removing a share.

For example, you could set up McAfee CASB to monitor the content of files when they are shared in a public FileCloud folder.

McAfee CASB supported features



User Activity	File Upload, File Update, File Download, File has been Shared publicly, Folder has been shared publicly
	User logged in
DLP Features	Content- aware Public Shared Link, or Pure Public Shared link Policy evaluation for Item Shared event
	Content-ware Policy evaluation for File Upload/Update event
	Response Actions: Incident Remove Shared link Email notification Send user notification Delete

FileCloud events and McAfee responses

To receive information about events, McAfee registers a webhook with FileCloud, which enables FileCloud to push information about events as they occur to McAfee CASB.

FileCloud pushes information to McAfee when a user performs one of the following actions:

- adds a file
- updates a file
- adds an external file
- downloads a file
- logs in successfully
- creates a share
- creates an account
- deletes an account

McAfee responds to events that may compromise security using FileCloud's API. FileCloud's API includes the following endpoints:

- register
- deregister
- getwebhook
- downloadfile
- upload
- deletefile
- getshareinformation
- removeuserfromshare
- removegroupfromshare
- deleteshare
- getuserinformation

For more information about using these APIs, see the API documentation at https://fcapi.getfilecloud.com/

ICAP DLP

> The ability to configure ICAP DLP as a provider for FileCloud's CCE is available in Version 20.3 and higher.

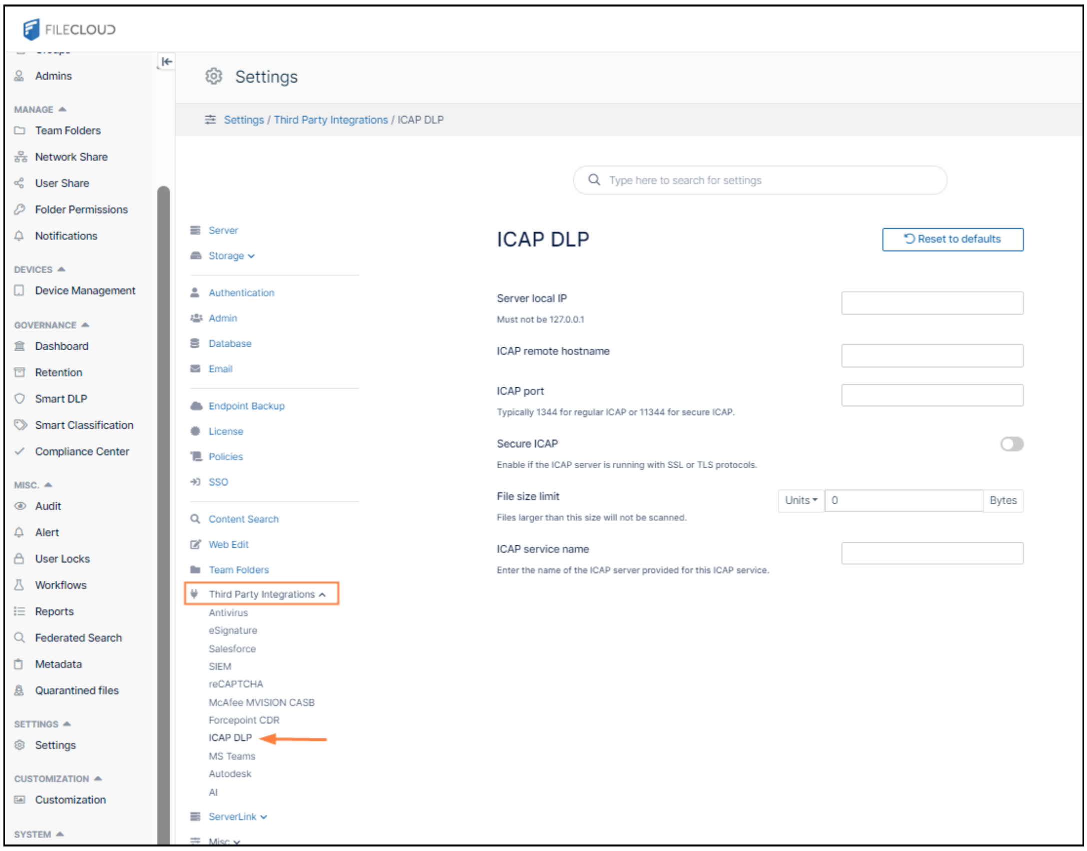
ICAP DLP has been added as a provider for FileCloud's Smart Classification (CCE), enabling you set up a content classification rule that flags files for blocking or deletion by DLP rules. You must configure it as a third-party provider in FileCloud to use it with the CCE.

What is ICAP?

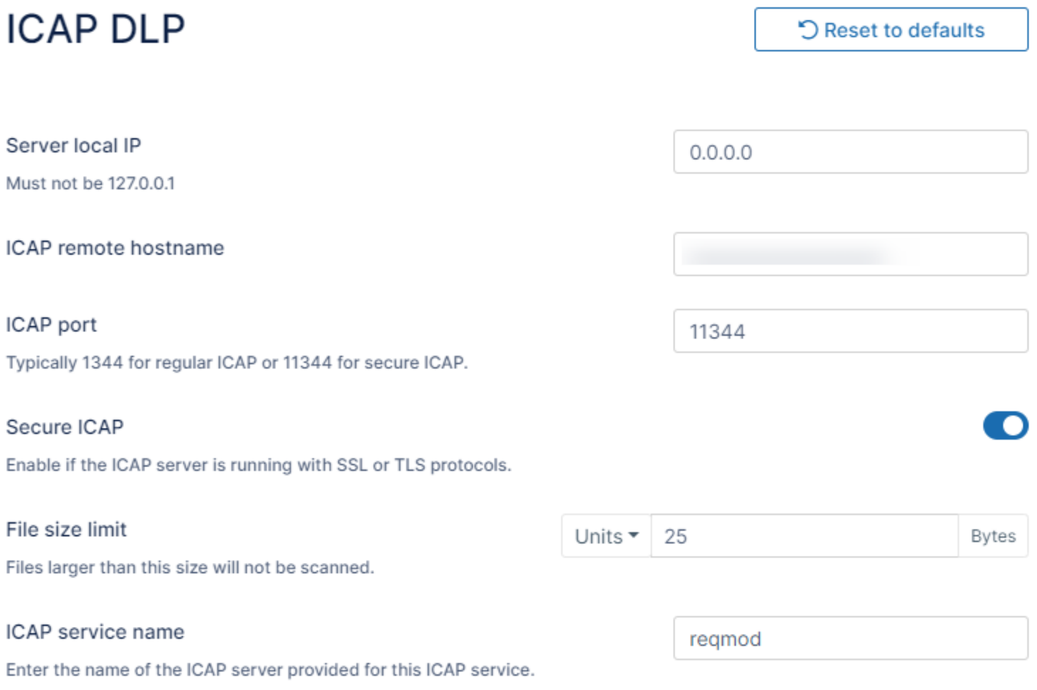
ICAP is a generic protocol that allows web servers to offload specialized tasks to custom-built servers. Examples of such specialized tasks include DLP (data loss prevention) based content scanning, URL filtering and antivirus scanning.

Integrating ICAP DLP with FileCloud

1. Open the ICAP DLP settings page.
   To go to the ICAP DLP settings page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the Settings navigation page, click Third Party Integrations 🧩.
   b. In the inner navigation bar on the left of the Third Party Integrations page, expand the **Third Party Integrations** menu, and click **ICAP DLP** as shown below.



2. Fill in the fields. See the table below for information.



ICAP DLP

Reset to defaults

Server local IP: 0.0.0.0

Must not be 127.0.0.1

ICAP remote hostname:

ICAP port: 11344

Typically 1344 for regular ICAP or 11344 for secure ICAP.

Secure ICAP: ●

Enable if the ICAP server is running with SSL or TLS protocols.

File size limit: Units 25 Bytes

Files larger than this size will not be scanned.

ICAP service name: reqmod

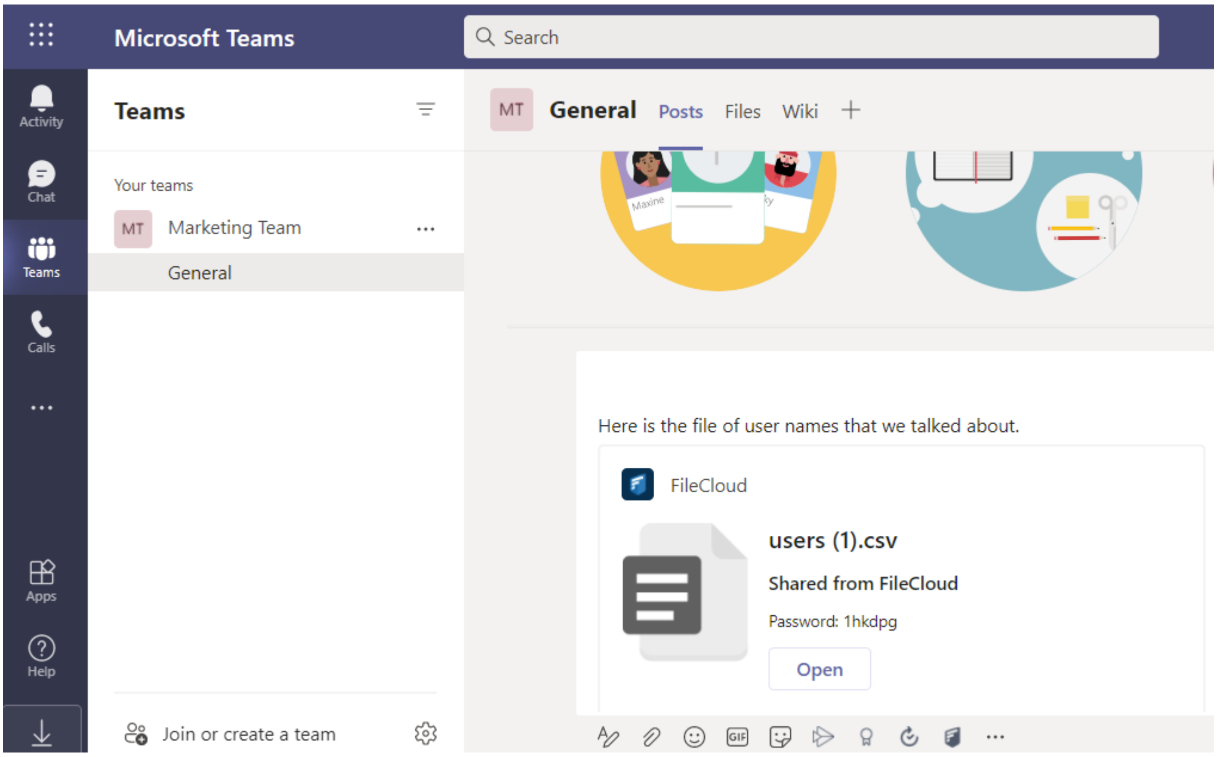
Enter the name of the ICAP server provided for this ICAP service.

Setting	Description
Server Local IP	In most cases, enter the value **0.0.0.0**. If you are using a separate FileCloud policy with ICAP, enter the Private (LAN) IP of the FileCloud server.
ICAP Remote Hostname	Enter the hostname or IP of the system where the ICAP DLP is deployed.
ICAP Port	Leave the default value of 1344 or use 11344 for secure ICAP. In rare cases, this might need to be changed to whatever port the ICAP DLP server is listening on.
Secure ICAP	Enable if the ICAP server is running with SSL or TLS protocols.
File Size Limit	To exclude very large files from scanning, specify the file size limit in bytes. Default value is 25MB.
ICAP Service Name	Consult the ICAP DLP server product documentation for this value. It must be set correctly; otherwise, integration won't work.

3. Click **Save**.
   After you have configured its settings in FileCloud, you can use ICAP DLP with FileCloud Smart Classification to set metadata values.

Microsoft Teams

FileCloud can be configured to function within MS Teams so users can share content in Team's chats and channels.



Here is the file of user names that we talked about.

FileCloud

users (1).csv

Shared from FileCloud

Password: 1hkdpg

Open

To set up integration:

1. The Teams administrator must create a FileCloud app.
2. The FileCloud administrator must enable Teams integration in FileCloud.
3. Then, FileCloud users can add the FileCloud app to their Teams installations in order to share FileCloud content in messages and view the FileCloud browser while working in Teams.

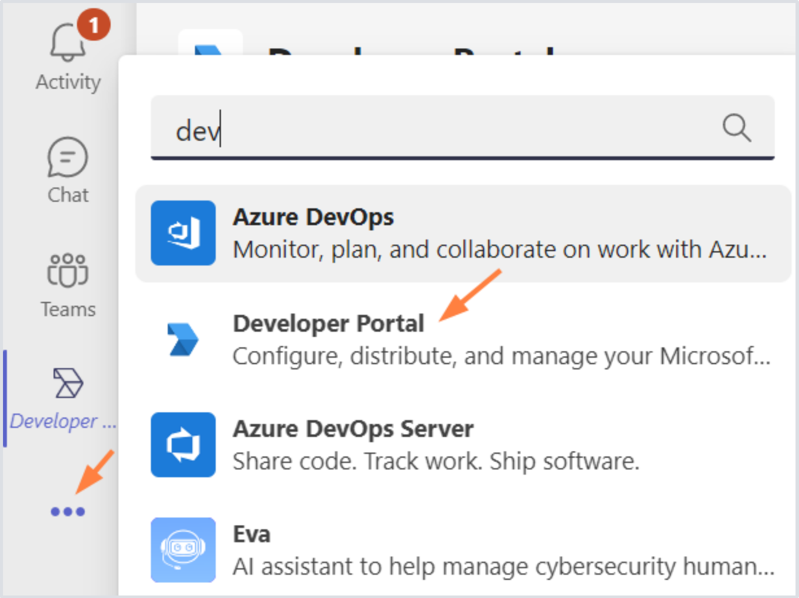
For MS Teams Admins: Configuring FileCloud in Teams

Before users can access FileCloud through MS Teams, the Teams administrator must perform the following configuration in Teams. After that, the FileCloud Admin must Enable FileCloud/Teams integration (see page 113) in the FileCloud Admin portal.

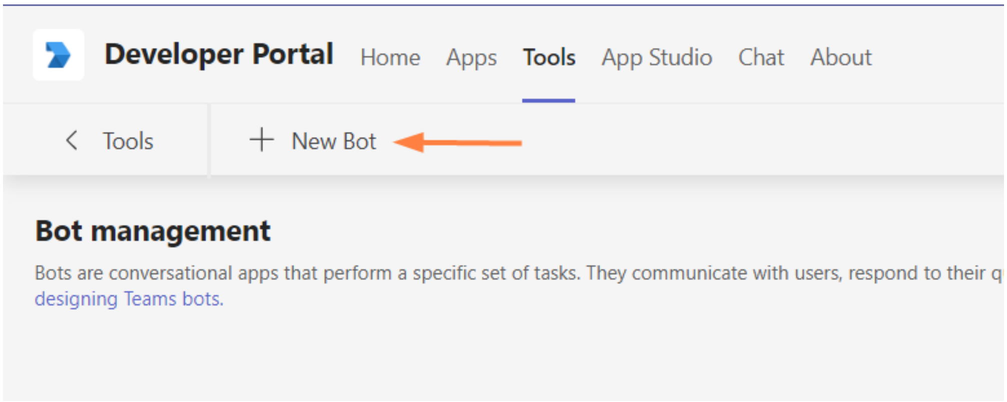
FileCloud integration with MS Teams is available beginning in FileCloud Version 21.2

1. Confirm that you have FileCloud Version 21.2 or higher installed.

2. Create an MS Teams bot in the Teams' **Developer Portal**:
   a. Open **MS Teams**.
   b. If you do not have the **Developer Portal** app installed already, click the **More** icon in the navigation pane, search for **Developer Portal**, and add it.


Activity
Chat
Teams
Developer ...
dev
Azure DevOps
Monitor, plan, and collaborate on work with Azu...
Developer Portal
Configure, distribute, and manage your Microsof...
Azure DevOps Server
Share code. Track work. Ship software.
Eva
AI assistant to help manage cybersecurity human...

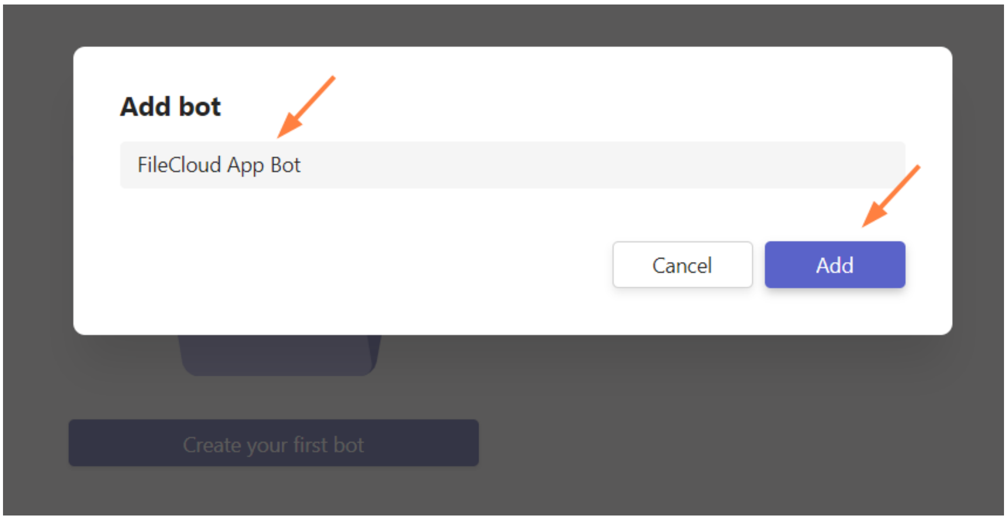
   c. Click the **Developer Portal** icon in the navigation pane, and go to **Tools > Bot Management**.
   d. Click **New Bot**.



Bot management

Bots are conversational apps that perform a specific set of tasks. They communicate with users, respond to their q
designing Teams bots.

   e. Name the bot ,and click **Add**.

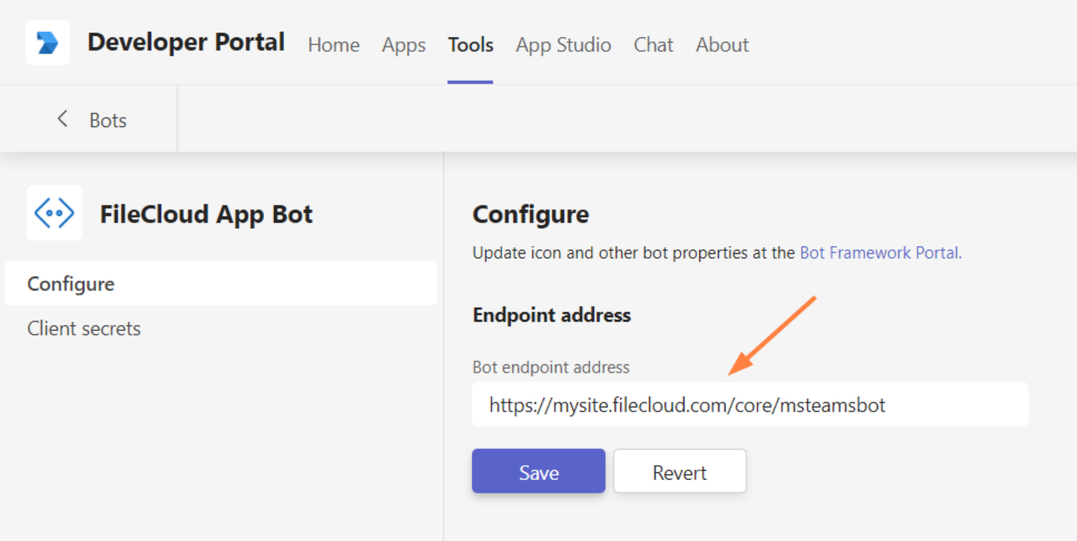


Add bot

FileCloud App Bot

The bot appears opened on the **Tools** screen.

f. Change the **Endpoint address** to point to the bot in your FileCloud server, and click Save. Use **https://[your** (see page 97) **FileCloud server]/core/msteamsbot**



Configure

Update icon and other bot properties at the Bot Framework Portal.

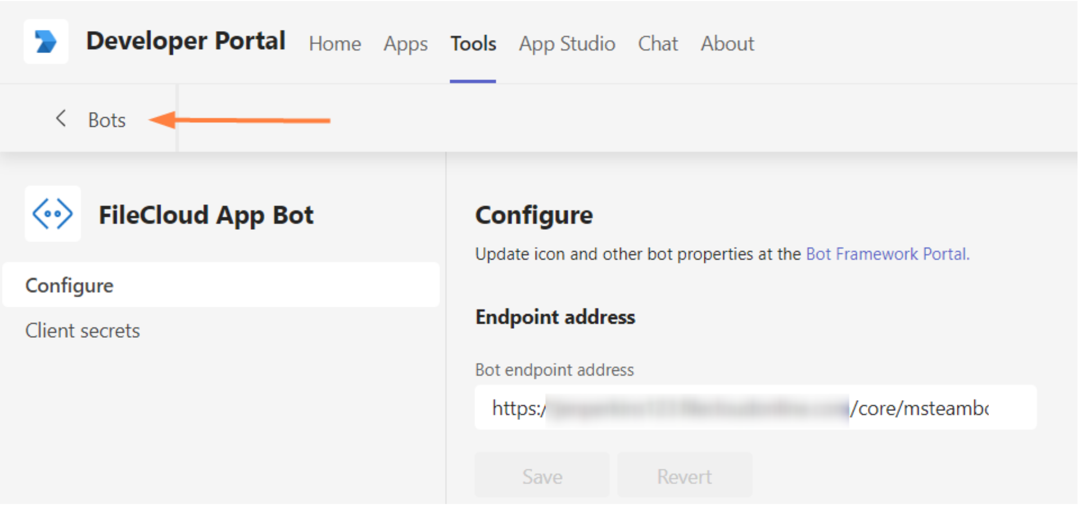
Endpoint address

Bot endpoint address

https://mysite.filecloud.com/core/msteamsbot

You are returned to the **Tools** screen.

g. Click **Bots**.



Configure

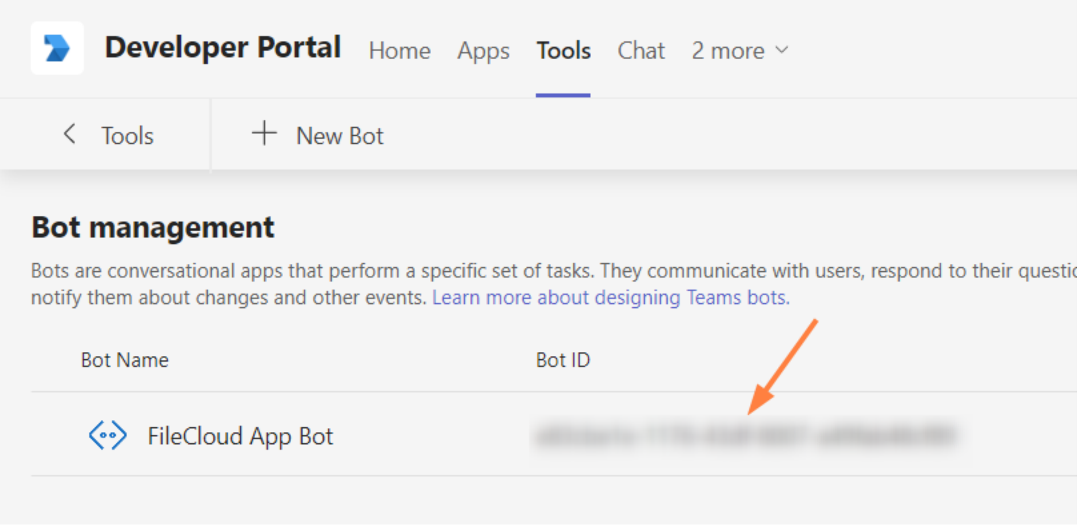
Update icon and other bot properties at the Bot Framework Portal.

Endpoint address

Bot endpoint address: https:/[redacted]/core/msteamb

You go back to the **Bots Management** screen.

h. Copy the **Bot ID**. You will need it to set up MS Teams integration in the FileCloud admin portal.

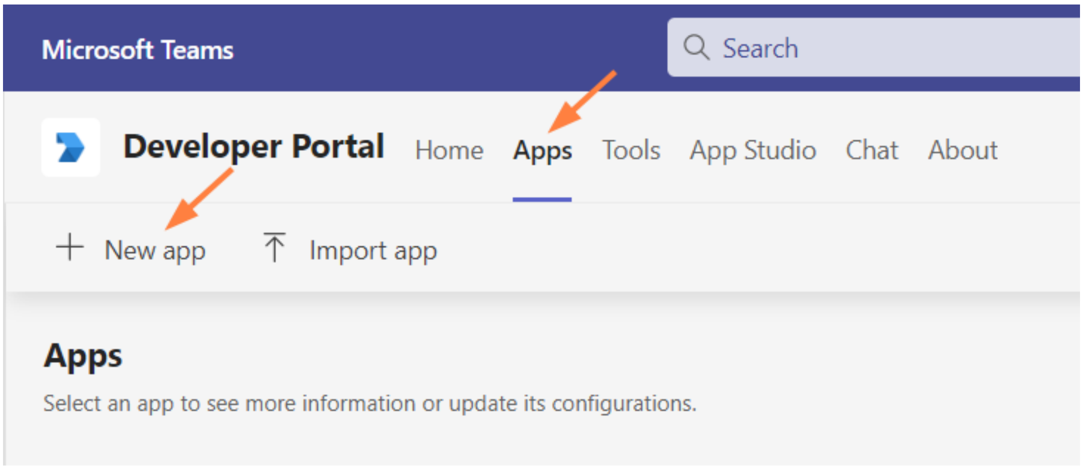


Bot management

Bots are conversational apps that perform a specific set of tasks. They communicate with users, respond to their questic notify them about changes and other events. Learn more about designing Teams bots.

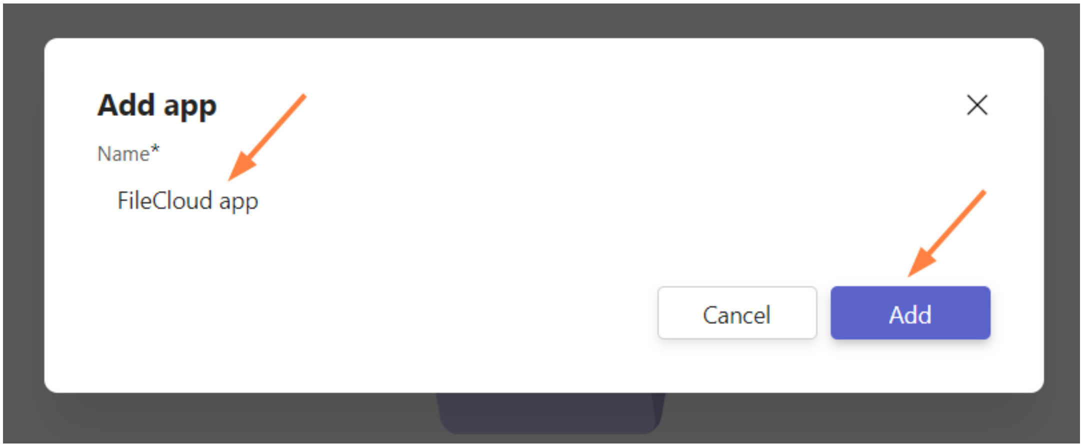
Bot Name	Bot ID
FileCloud App Bot	[redacted]

3. Create the MS Teams application in Teams' **Developer Portal**.
    a. In the **Developer Portal**, click the **Apps** tab, and then click **New App**.



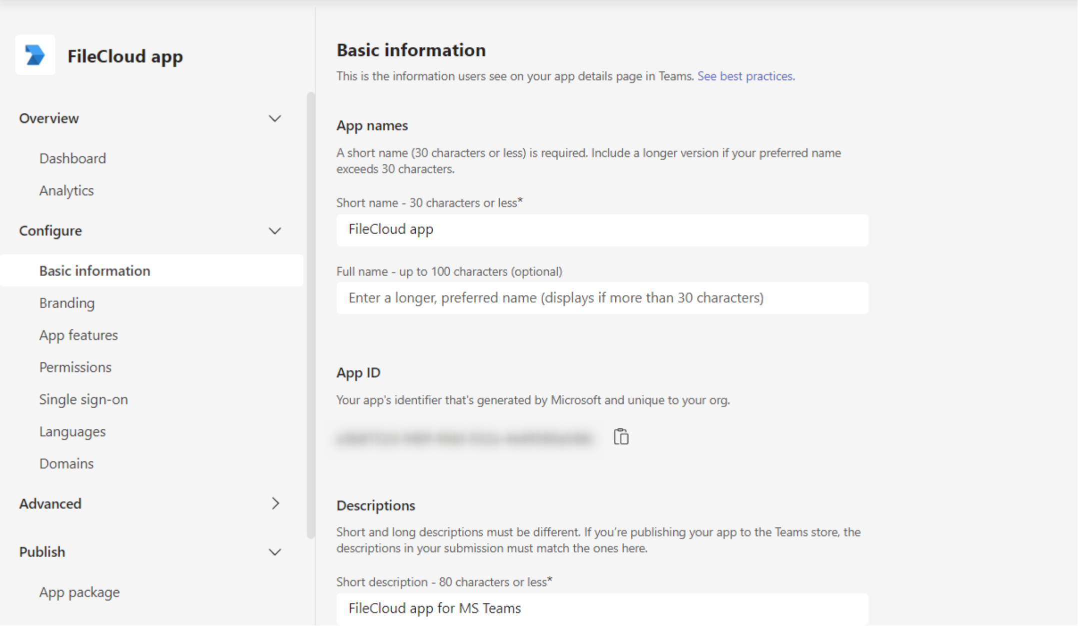
An **Add App** window opens.

b. Enter a name for your FileCloud app and click **Add**.



The **Basic Information** screen for the app opens.

c. Fill in the form, and click **Save**.
Depending on your MS Teams environment policies, you may not be required to enter a value for **Application (client) ID**.



Basic information

This is the information users see on your app details page in Teams. See best practices.

App names

A short name (30 characters or less) is required. Include a longer version if your preferred name exceeds 30 characters.

Short name - 30 characters or less*
FileCloud app

Full name - up to 100 characters (optional)
Enter a longer, preferred name (displays if more than 30 characters)

App ID

Your app's identifier that's generated by Microsoft and unique to your org.

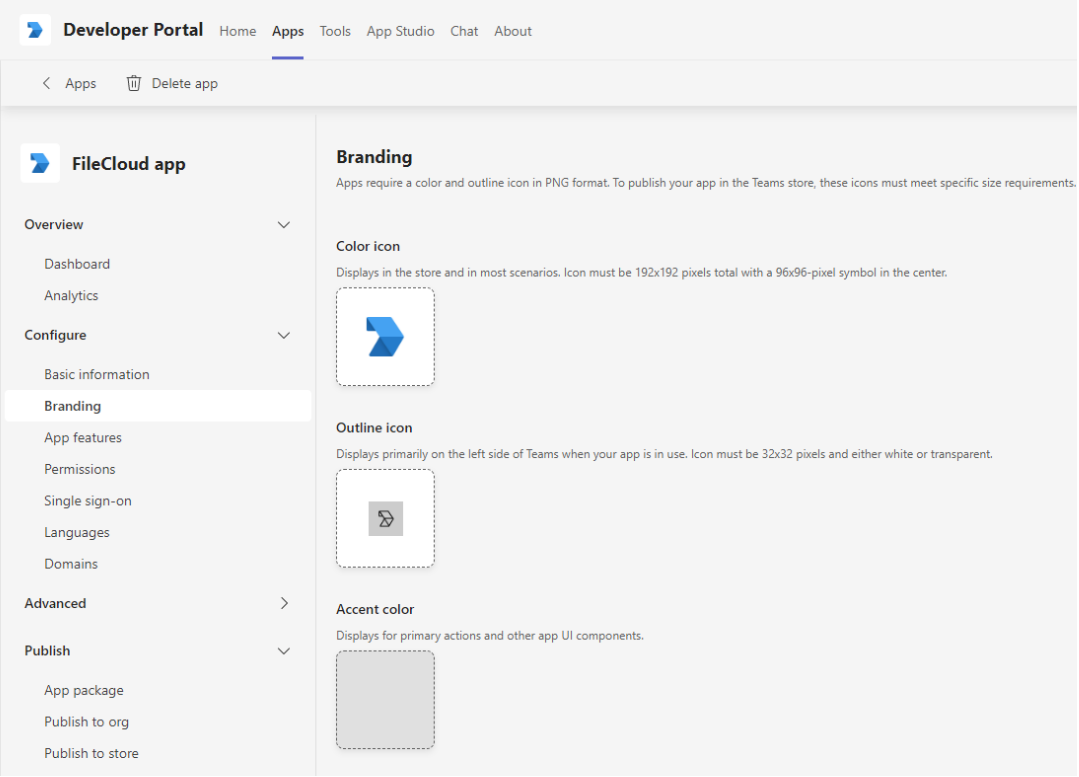
[redacted]

Descriptions

Short and long descriptions must be different. If you're publishing your app to the Teams store, the descriptions in your submission must match the ones here.

Short description - 80 characters or less*
FileCloud app for MS Teams

d. In the navigation pane, click **Branding**.
The **Branding** screen opens.



Branding

Apps require a color and outline icon in PNG format. To publish your app in the Teams store, these icons must meet specific size requirements.

Color icon

Displays in the store and in most scenarios. Icon must be 192x192 pixels total with a 96x96-pixel symbol in the center.

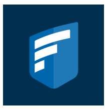
Outline icon

Displays primarily on the left side of Teams when your app is in use. Icon must be 32x32 pixels and either white or transparent.

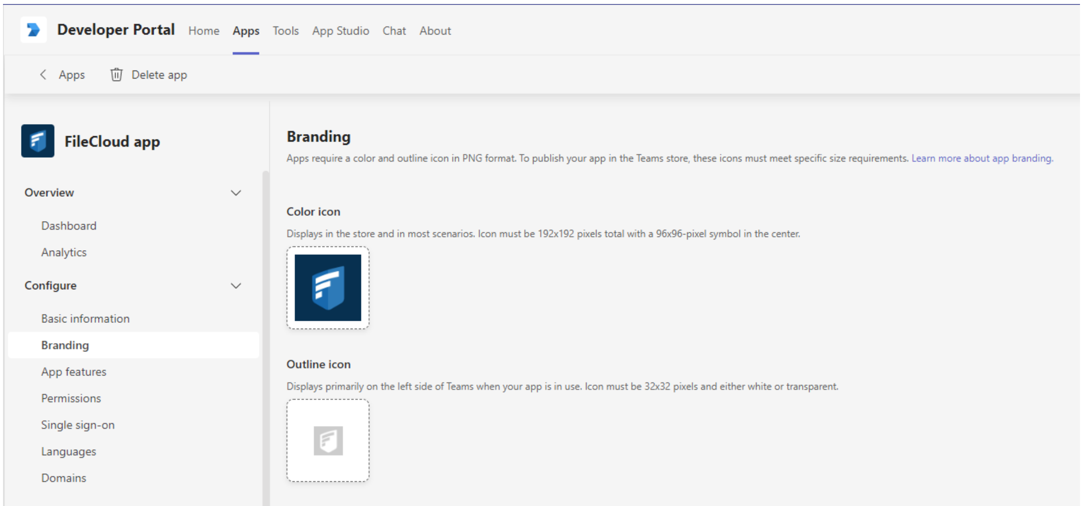
Accent color

Displays for primary actions and other app UI components.

e. Download the following two images (right-click and choose **Save image as**).



f. Upload the first image for **Color icon,** and the second image for **Outline icon**.
You may use custom images, but they must be 192px X 192px for the color image and 32px X 32px for the transparent outline.



Branding

Apps require a color and outline icon in PNG format. To publish your app in the Teams store, these icons must meet specific size requirements. Learn more about app branding.

Color icon

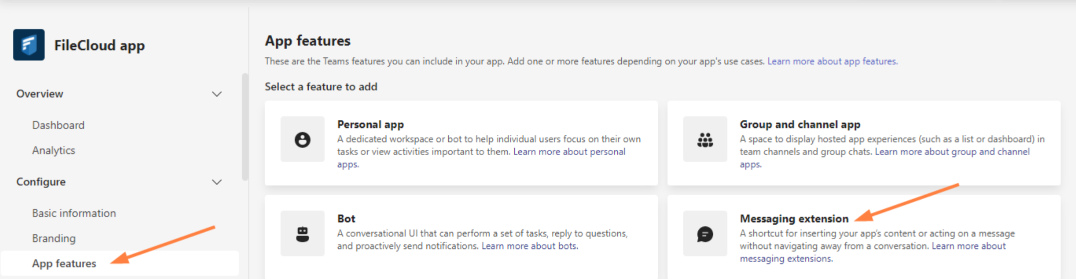
Displays in the store and in most scenarios. Icon must be 192x192 pixels total with a 96x96-pixel symbol in the center.

Outline icon

Displays primarily on the left side of Teams when your app is in use. Icon must be 32x32 pixels and either white or transparent.

4. Set up your MS Teams bot.

a. In the navigation pane, click **App Features**, and click **Messaging Extension**.



App features

These are the Teams features you can include in your app. Add one or more features depending on your app's use cases. Learn more about app features.

Select a feature to add

Personal app
A dedicated workspace or bot to help individual users focus on their own tasks or view activities important to them. Learn more about personal apps.

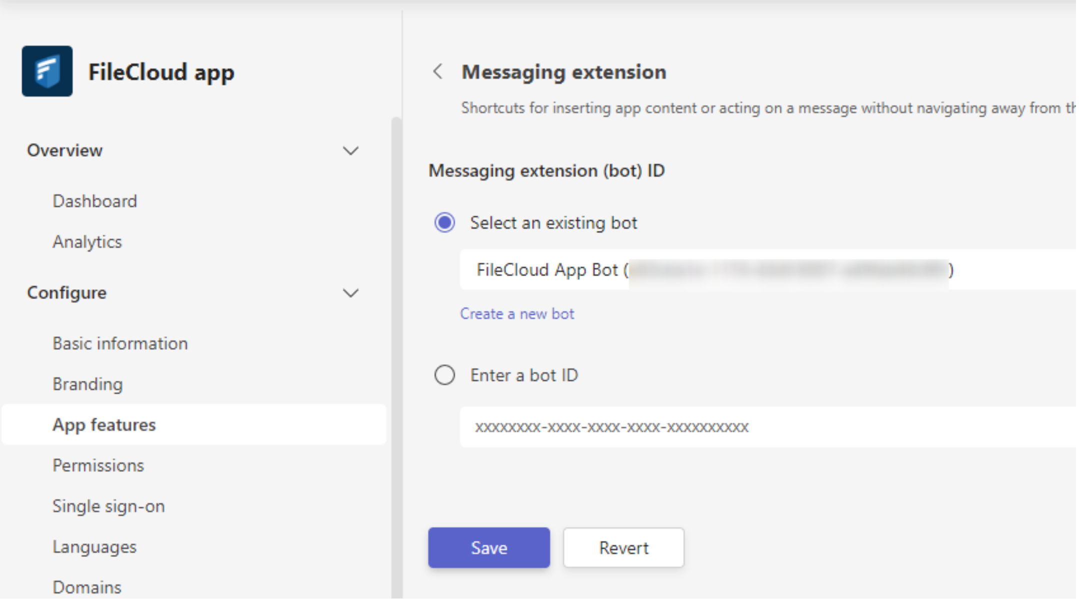
Group and channel app
A space to display hosted app experiences (such as a list or dashboard) in team channels and group chats. Learn more about group and channel apps.

Bot
A conversational UI that can perform a set of tasks, reply to questions, and proactively send notifications. Learn more about bots.

Messaging extension
A shortcut for inserting your app's content or acting on a message without navigating away from a conversation. Learn more about messaging extensions.

The **Messaging Extension** screen opens.

b. Choose **Select an existing bot**, and select the FileCloud bot that you just created, and click **Save**.



FileCloud app

Overview
- Dashboard
- Analytics

Configure
- Basic information
- Branding
- App features
- Permissions
- Single sign-on
- Languages
- Domains

Messaging extension

Shortcuts for inserting app content or acting on a message without navigating away from th

Messaging extension (bot) ID

● Select an existing bot

FileCloud App Bot ([redacted])

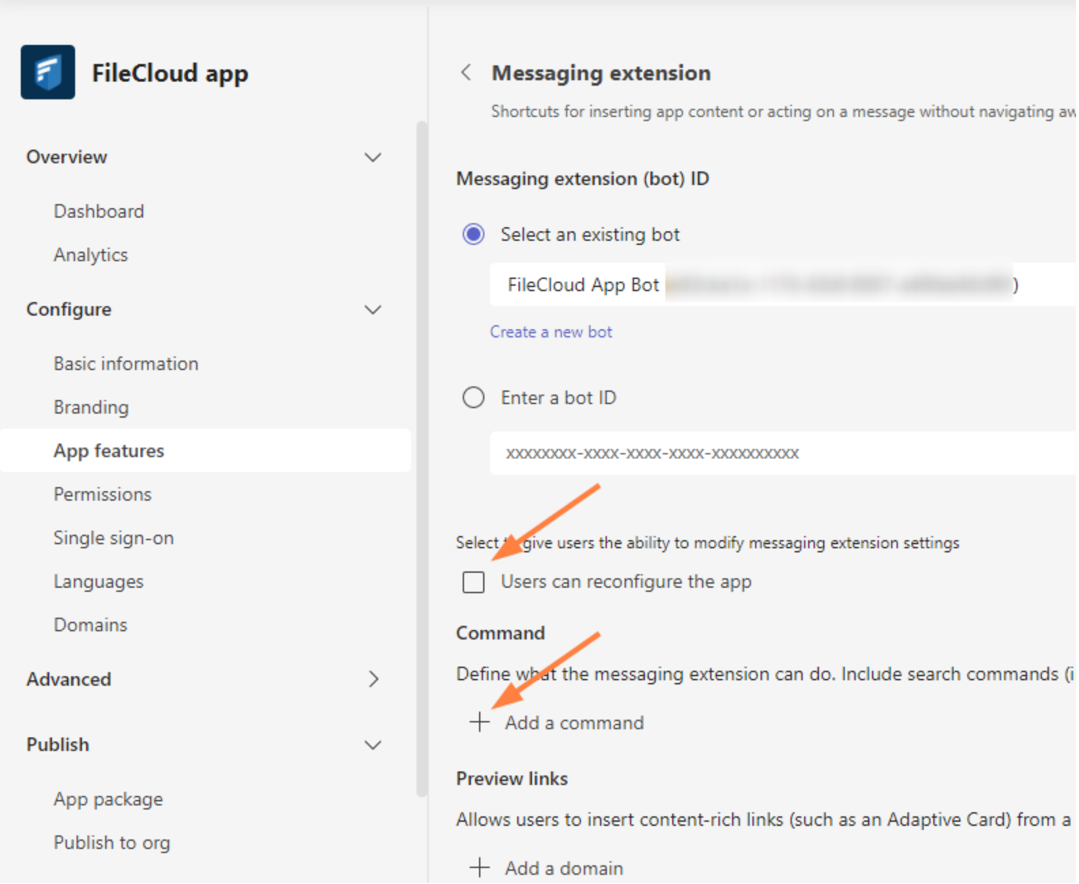
Create a new bot

○ Enter a bot ID

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Save | Revert

c. Uncheck **Users can reconfigure app**, and click **Add a command**.



FileCloud app

Overview
- Dashboard
- Analytics

Configure
- Basic information
- Branding
- App features
- Permissions
- Single sign-on
- Languages
- Domains

Advanced

Publish
- App package
- Publish to org

Messaging extension

Shortcuts for inserting app content or acting on a message without navigating aw

Messaging extension (bot) ID

● Select an existing bot

FileCloud App Bot [redacted])

Create a new bot

○ Enter a bot ID

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Select to give users the ability to modify messaging extension settings

□ Users can reconfigure the app

Command

Define what the messaging extension can do. Include search commands (i

+ Add a command

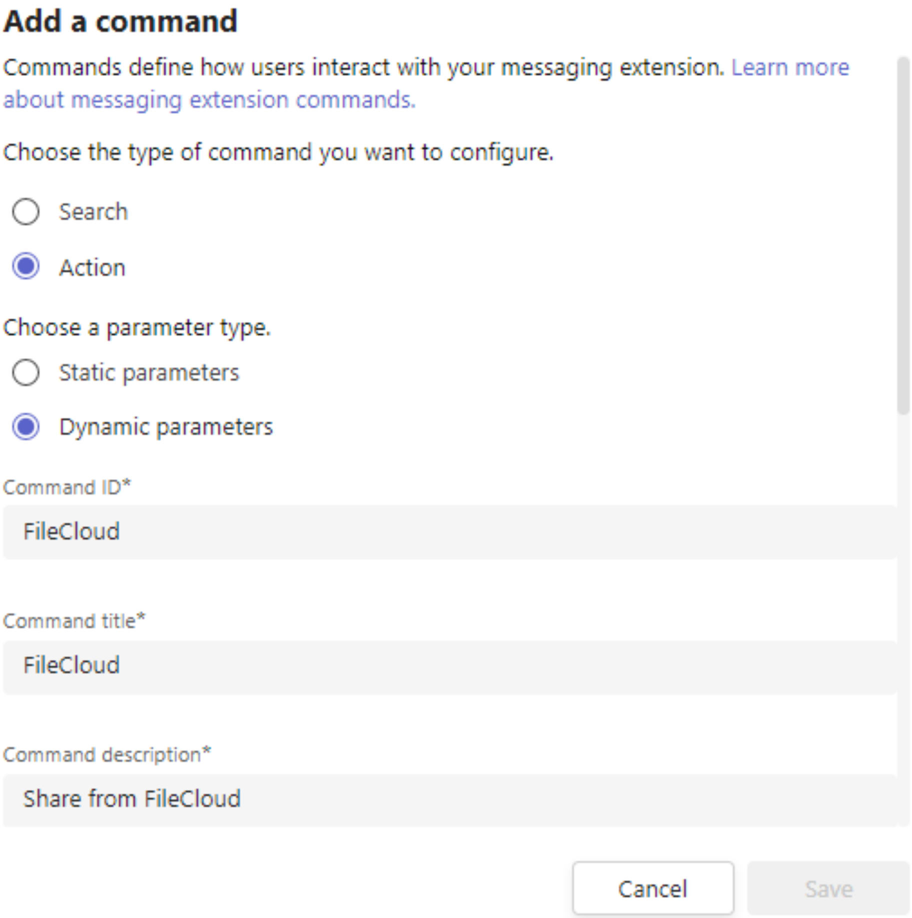
Preview links

Allows users to insert content-rich links (such as an Adaptive Card) from a

+ Add a domain

An **Add a command** dialog box opens.

d. Fill in the fields as shown in the following screenshots:



Add a command

Commands define how users interact with your messaging extension. Learn more about messaging extension commands.

Choose the type of command you want to configure.

○ Search

● Action

Choose a parameter type.

○ Static parameters

● Dynamic parameters

Command ID*

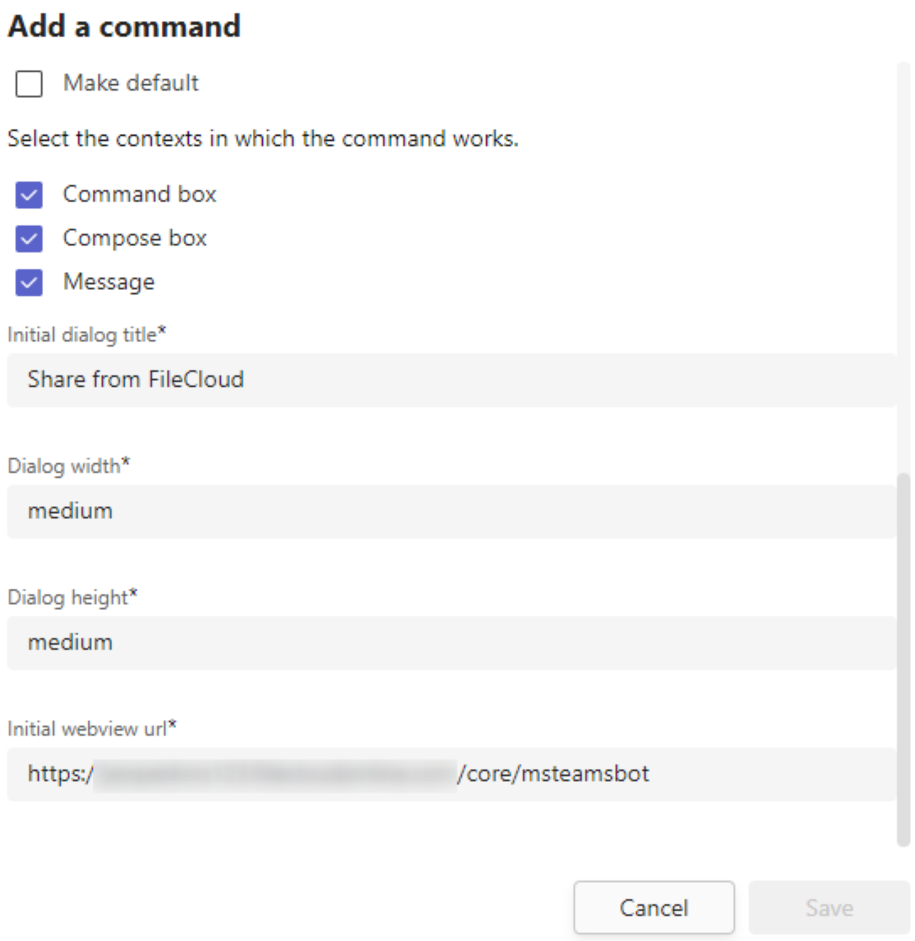
FileCloud

Command title*

FileCloud

Command description*

Share from FileCloud



Add a command

□ Make default

Select the contexts in which the command works.

☑ Command box

☑ Compose box

☑ Message

Initial dialog title*

Share from FileCloud

Dialog width*

medium

Dialog height*

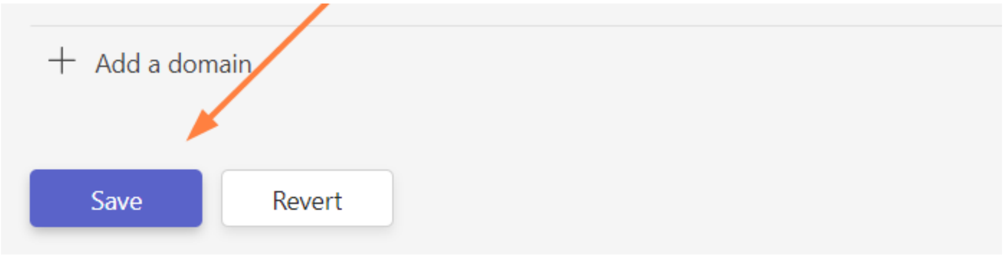
medium

Initial webview url*

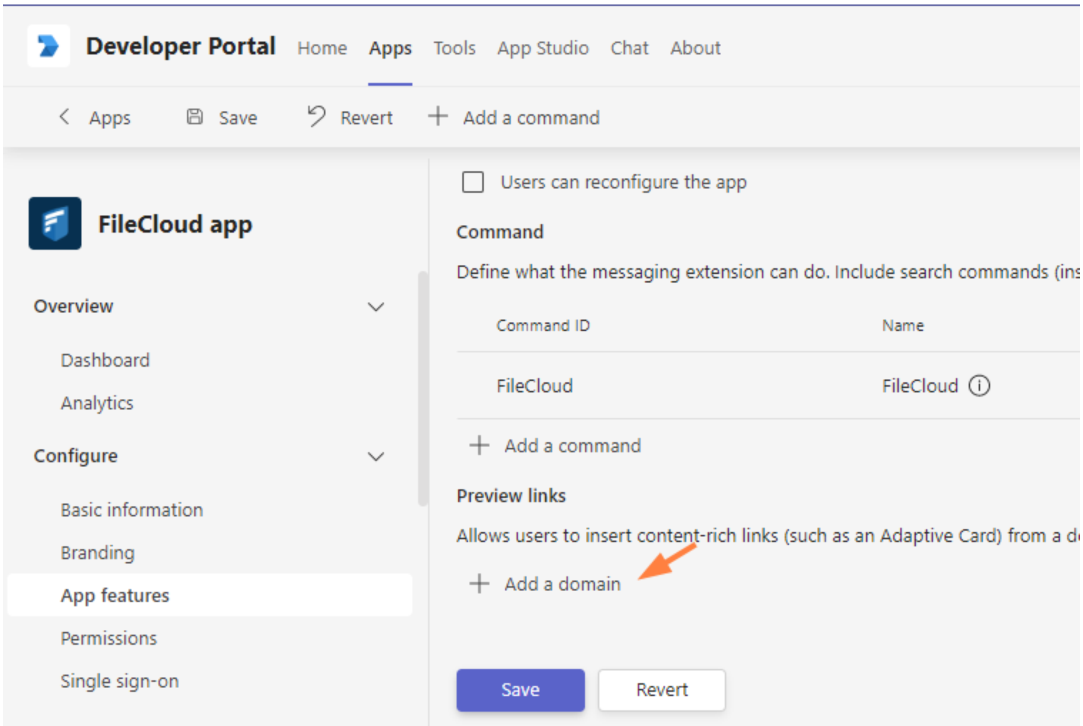
https:/[redacted]/core/msteamsbot

e. Click **Save**.
   You are returned to the **Messaging Extension** screen.

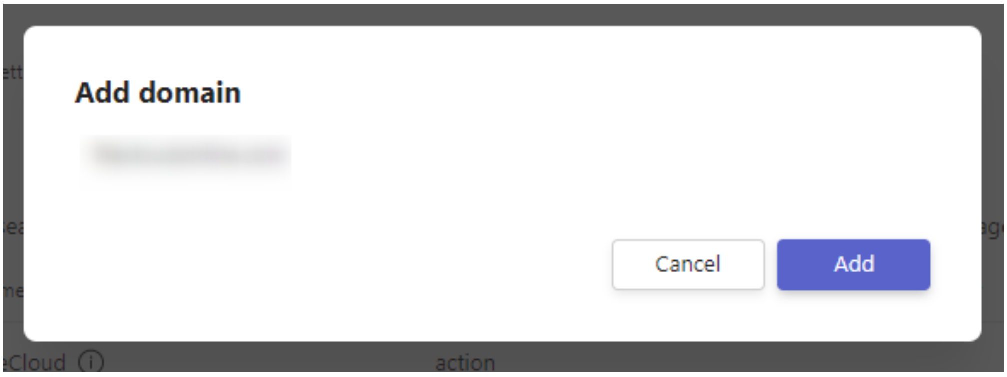
f. Click **Save** again, or the command will not be saved.



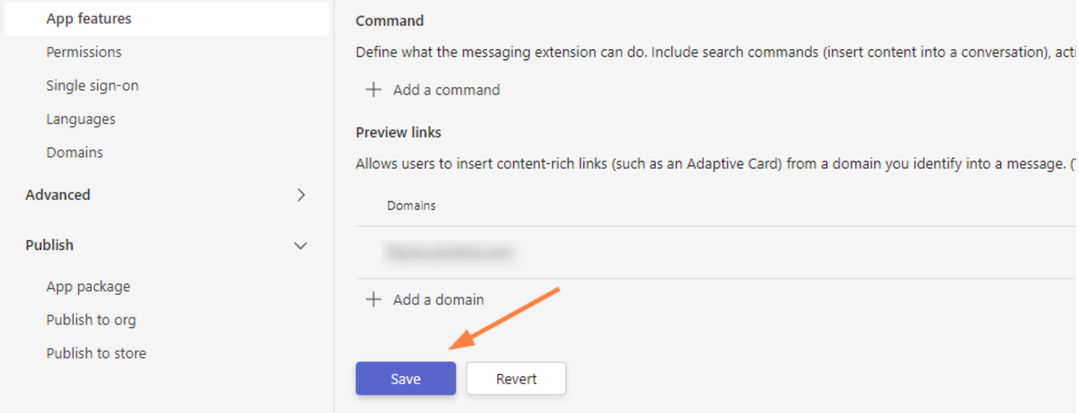
g. Now, in the **Messaging Extension** screen, click **Add a domain**.



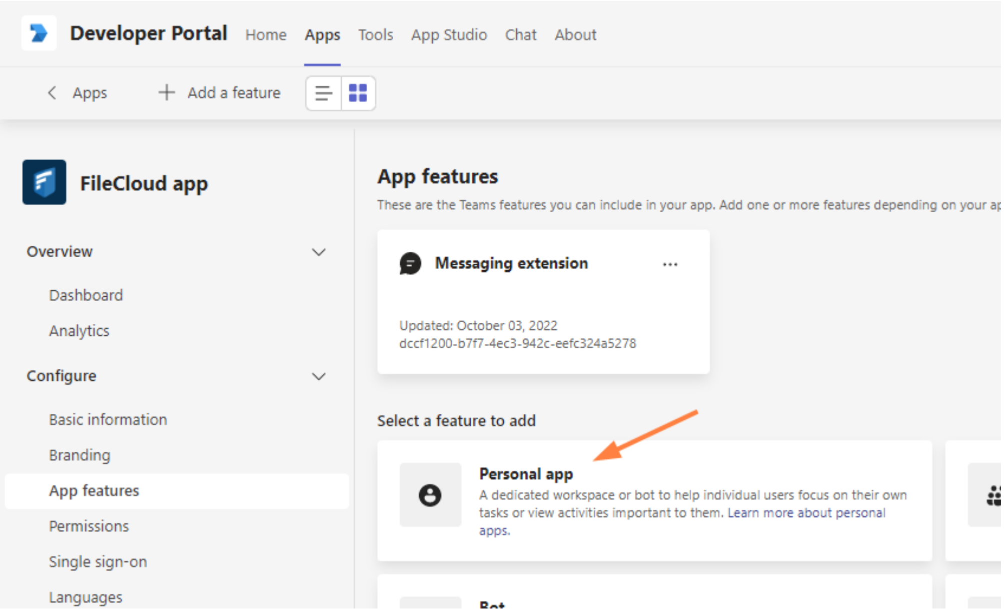
h. In the **Add Domain** dialog box, add your domain without the **https:// prefix**, and click **Add**.



i. In the **Messaging Extension** screen, click **Save**.


App features
Permissions
Single sign-on
Languages
Domains
Advanced
Publish
App package
Publish to org
Publish to store
Command
Define what the messaging extension can do. Include search commands (insert content into a conversation), acti
Add a command
Preview links
Allows users to insert content-rich links (such as an Adaptive Card) from a domain you identify into a message. (
Domains
Add a domain
Save
Revert

j. In the navigation pane, click **App Features** again, and click **Personal app**.

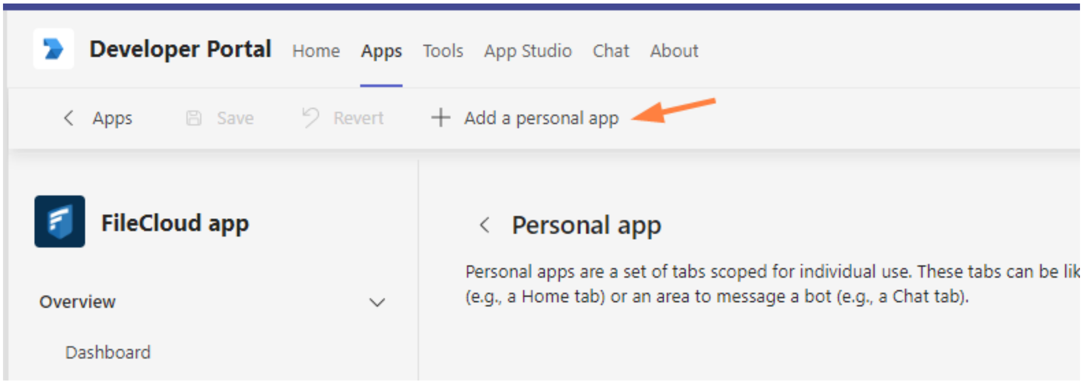


These are the Teams features you can include in your app. Add one or more features depending on your ap

Updated: October 03, 2022
dccf1200-b7f7-4ec3-942c-eefc324a5278

A dedicated workspace or bot to help individual users focus on their own tasks or view activities important to them. Learn more about personal apps.

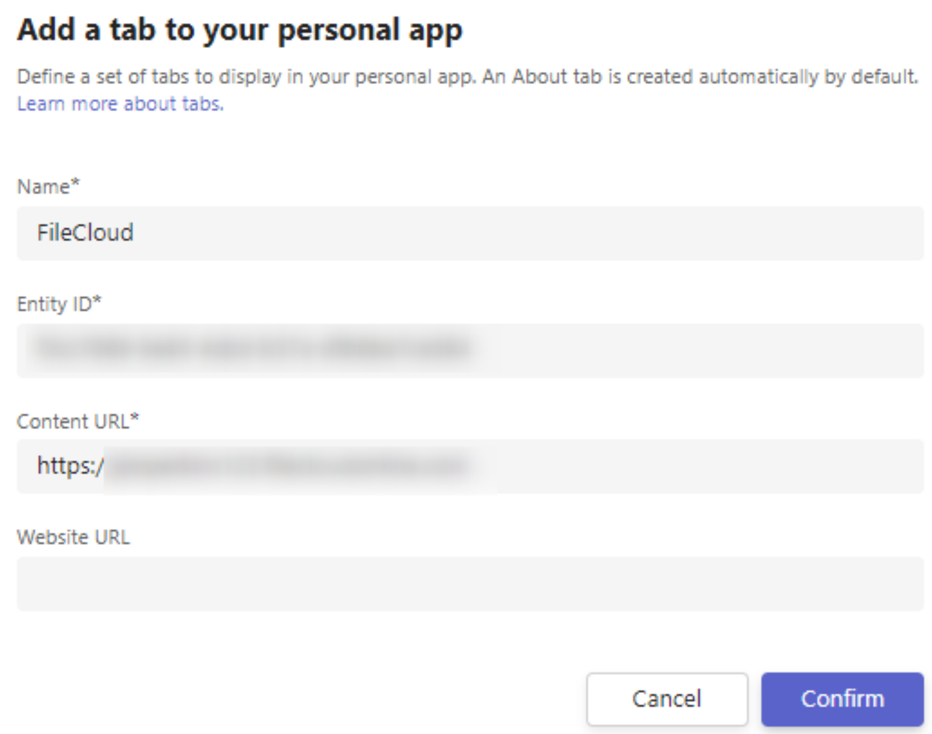
k. Click **Add a personal app**.



Personal apps are a set of tabs scoped for individual use. These tabs can be lik (e.g., a Home tab) or an area to message a bot (e.g., a Chat tab).

The **Add a tab to your personal app** dialog box opens.

l. Fill in the fields as follows. Your **Entity ID** will be entered for you.



Add a tab to your personal app

Define a set of tabs to display in your personal app. An About tab is created automatically by default. Learn more about tabs.

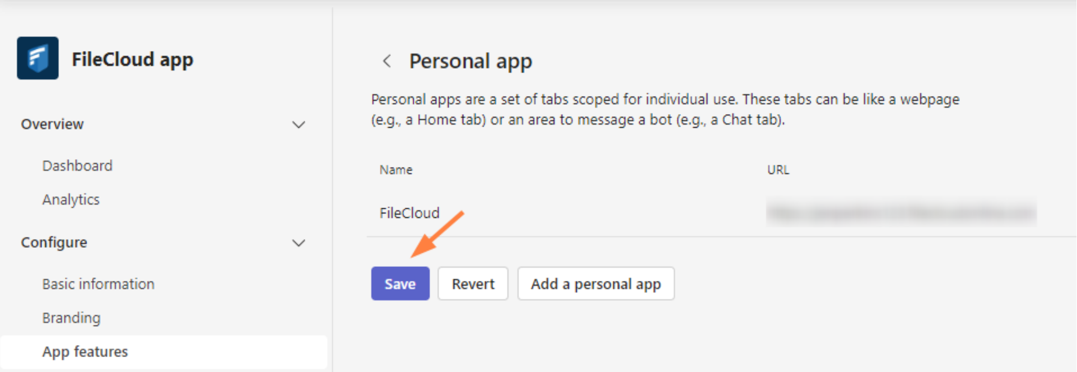
Name*
FileCloud

Entity ID*
[redacted]

Content URL*
https:/[redacted]

Website URL

m. Click **Confirm**.
In the **Personal app** screen, click **Save**.

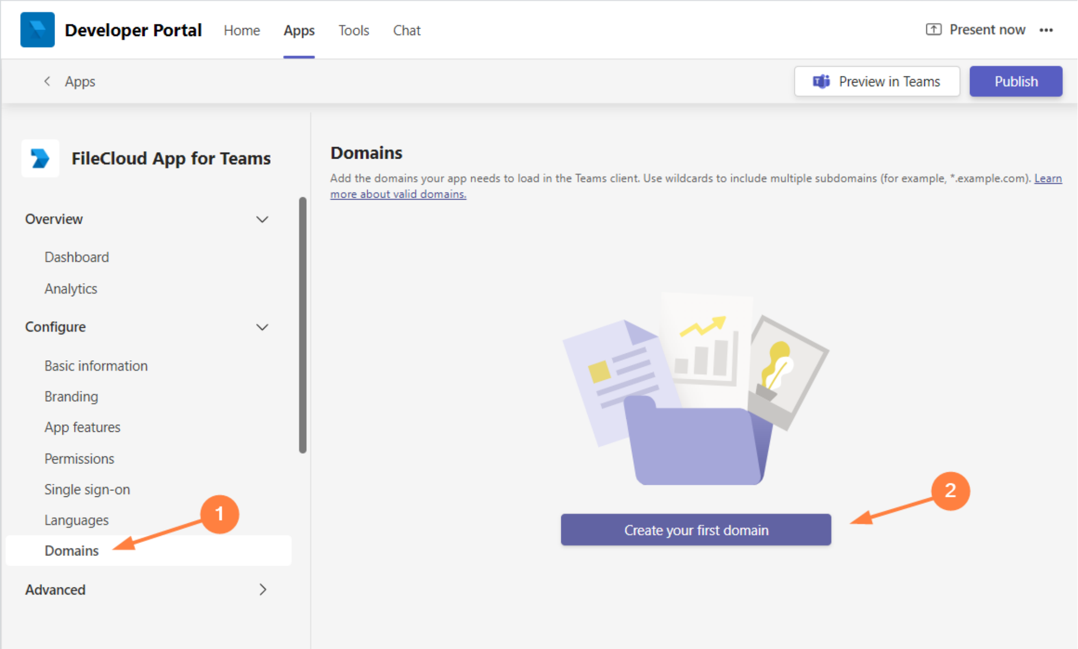


Personal app

Personal apps are a set of tabs scoped for individual use. These tabs can be like a webpage (e.g., a Home tab) or an area to message a bot (e.g., a Chat tab).

Name	URL
FileCloud	[redacted]

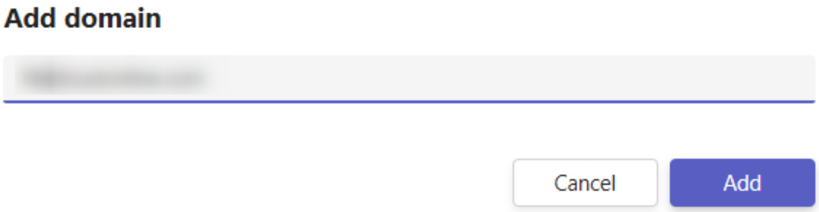
5. Add your domain to a global domains list.
   a. In the navigation pane, click **Domains**, and then click **Create your first domain**. (If you already have domains listed, click **Add a domain**.)



Domains

Add the domains your app needs to load in the Teams client. Use wildcards to include multiple subdomains (for example, *.example.com). Learn more about valid domains.

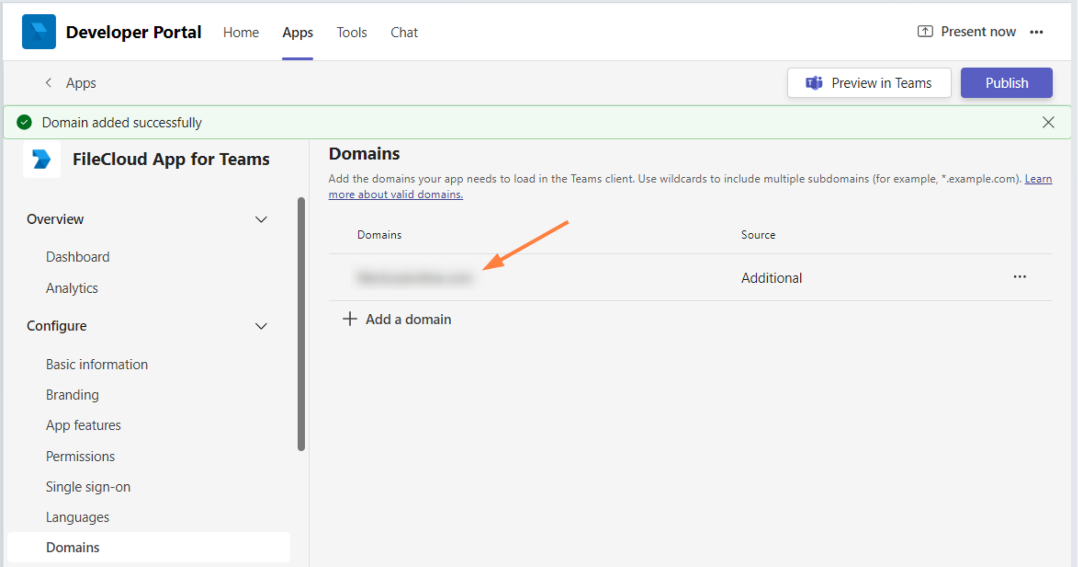
b. In the **Add domain** dialog box, enter your domain (the same one you entered above, in step 4h).



Add domain

[redacted]

c. Click **Add**.
The domain is added to the list:



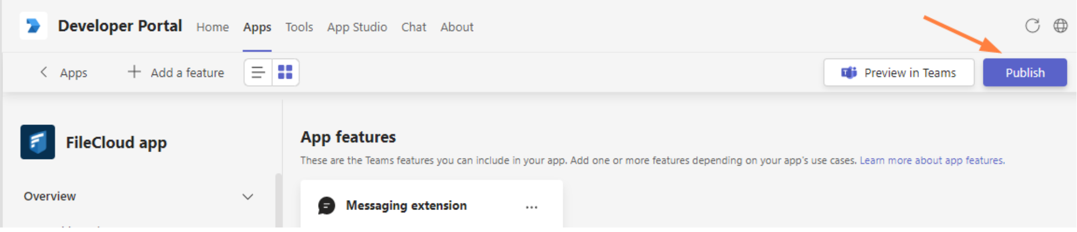
Domain added successfully

Domains

Add the domains your app needs to load in the Teams client. Use wildcards to include multiple subdomains (for example, *.example.com). Learn more about valid domains.

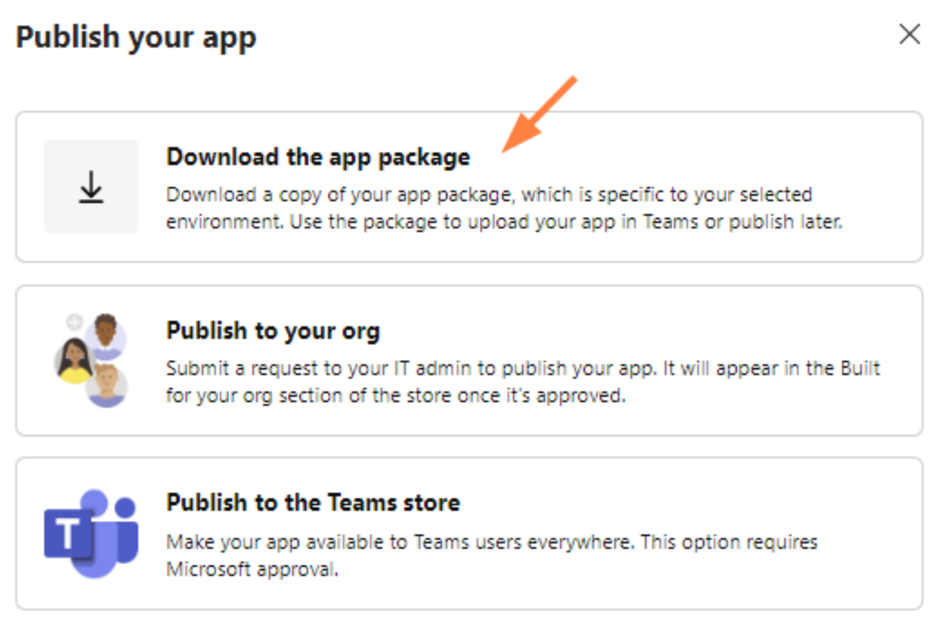
Domains	Source	
[redacted]	Additional	...

6. Export the application manifest zip file from Teams' **Developer Portal**.
   a. Click **Publish**.


Developer Portal
Home
Apps
Tools
App Studio
Chat
About
Apps
Add a feature
Preview in Teams
Publish
FileCloud app
Overview
App features
These are the Teams features you can include in your app. Add one or more features depending on your app's use cases. Learn more about app features.
Messaging extension

   The **Publish your app** dialog box opens.

   b. Click **Download the app package**.



Publish your app

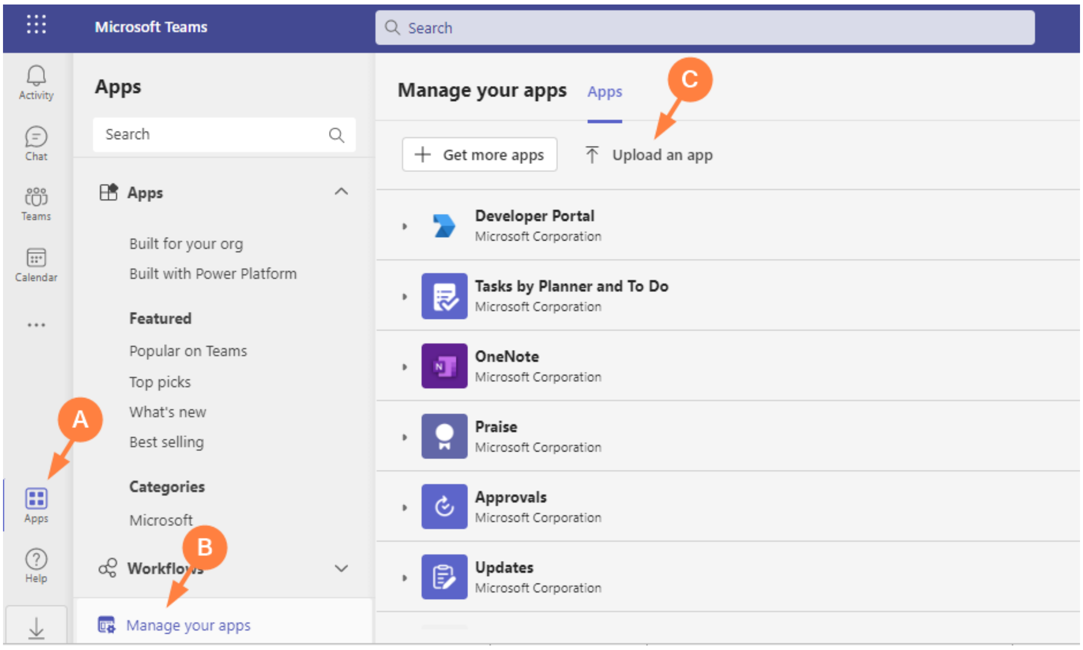
Download the app package
Download a copy of your app package, which is specific to your selected environment. Use the package to upload your app in Teams or publish later.

Publish to your org
Submit a request to your IT admin to publish your app. It will appear in the Built for your org section of the store once it's approved.

Publish to the Teams store
Make your app available to Teams users everywhere. This option requires Microsoft approval.

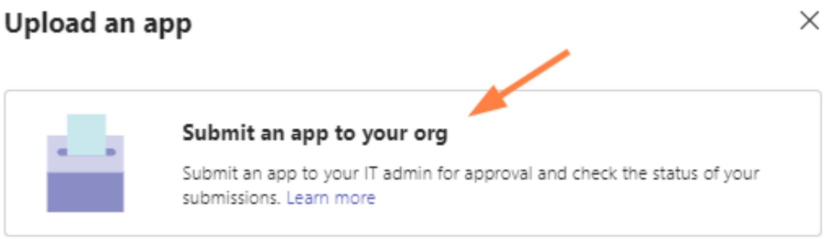
   c. Save the downloaded app package zip file.

7. Upload the application and submit it for approval in MS Teams.
   a. In the MS Teams navigation pane, click **Apps.**
   b. In the left panel click **Manage your apps**.
   c. In the **Manage your apps** screen, click **Upload an app**.



The **Upload an app** dialog box opens.

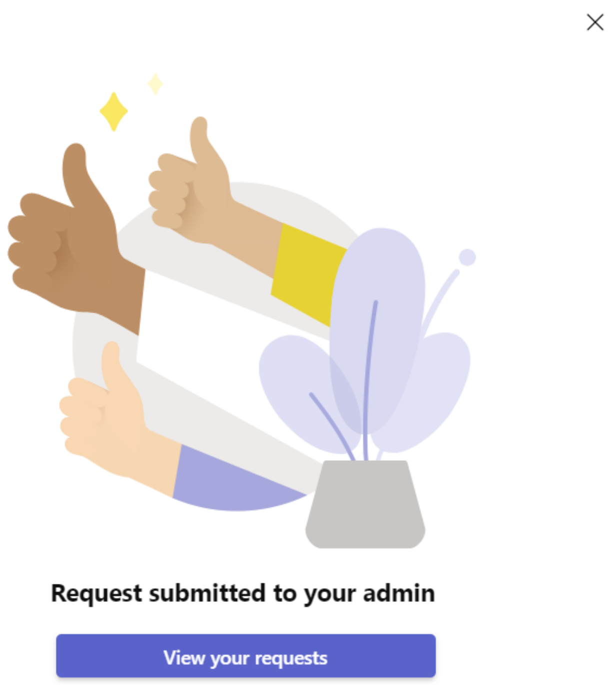
d. Click **Submit an app to your org.**



Submit an app to your IT admin for approval and check the status of your submissions. Learn more

Your file explorer opens.

e. Select your app package zip file.
You should now see:



Request submitted to your admin

f. As the Teams administrator, approve and publish the app.
   For more information, see https://docs.microsoft.com/en-us/MicrosoftTeams/manage-apps#approve-a-custom-app.
   The app's **Status** changes to **Approved**, and the app becomes available in your company's app store.

8. Next enable MS Teams integration in FileCloud (see page 113)

For FileCloud Admins: Enabling Integration with MS Teams

After FileCloud configuration in MS Teams (see page 97) has been completed by a Teams administrator, a FileCloud administrator must enable FileCloud/MS Teams integration in the FileCloud Admin portal.

> ℹ FileCloud Server must be able to communicate with Microsoft Servers in order for this integration to work. Internet connectivity, or access to the URL https://login.botframework.com/v1/.well-known/keys[8] is required, as well as 2-way communication with the domains teams.microsoft.com[9], *.teams.microsoft.com[10], and *.skype.com[11].

[8] https://login.botframework.com/v1/.well-known/keys%22
[9] http://teams.microsoft.com
[10] http://teams.microsoft.com

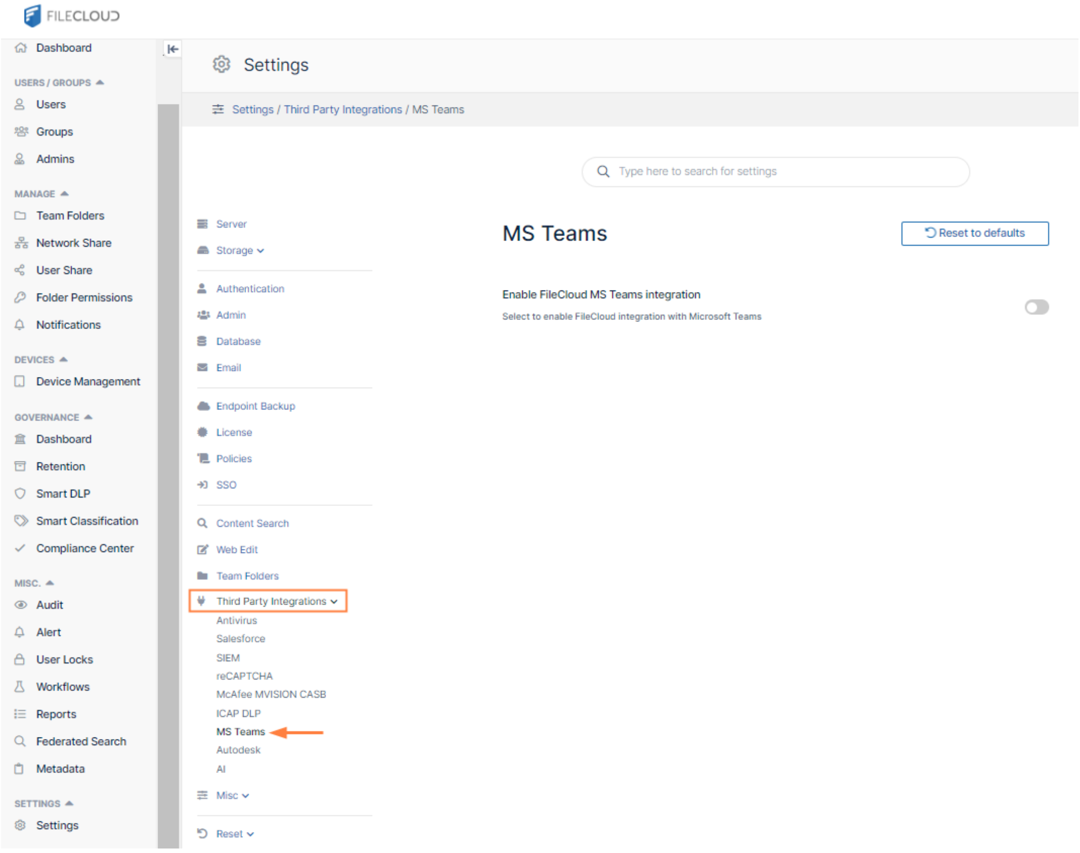
⚠ **Note regarding Chrome and Edge users**
Users who access MS Teams through Chrome or MS Edge will not be able to log in to FileCloud from MS Teams' FileCoud tab unless the cookie **SameSite** value is set to **None**.

Contact FileCloud Support to set your **SameSite** value to **None**,

To enable FileCloud integration with MS Teams:

1. Open the MS Teams settings page.
   To go to the MS Teams settings page

   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the Settings navigation page, click **Third Party Integrations**



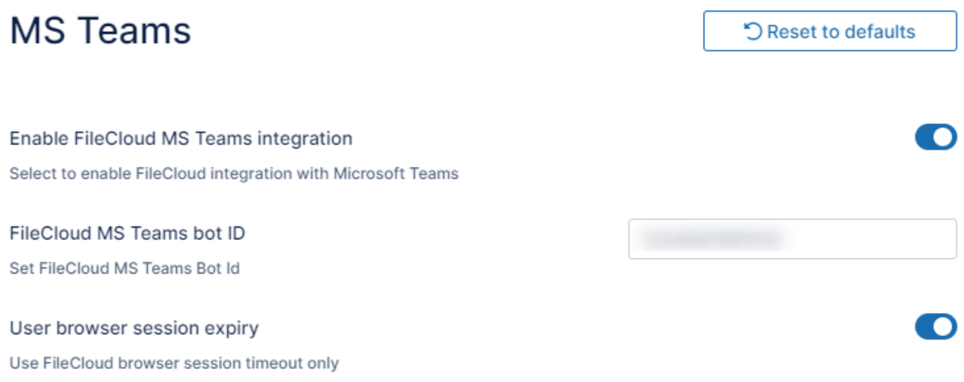
MS Teams

Enable FileCloud MS Teams integration
Select to enable FileCloud integration with Microsoft Teams

.

   b. In the inner navigation bar on the left of the Third Party Integrations page, expand the **Third Party Integrations** menu, and click **MS Teams**, as shown below.

[11] http://skype.com



MS Teams

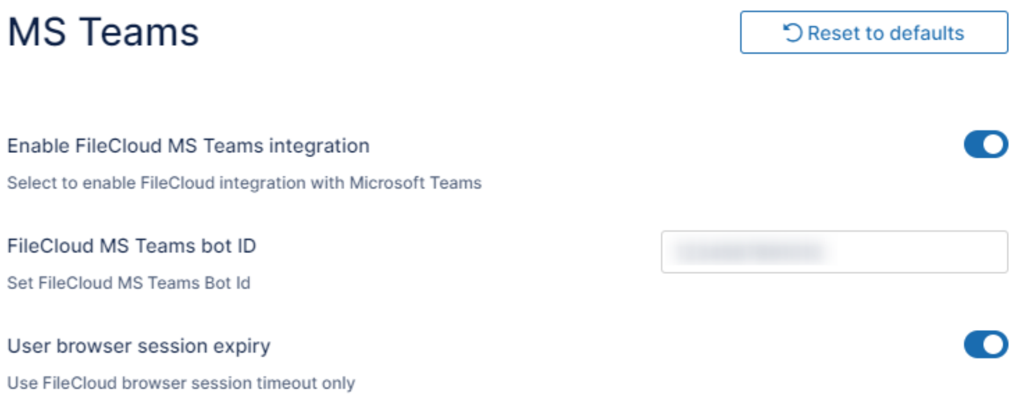
Enable FileCloud MS Teams integration
Select to enable FileCloud integration with Microsoft Teams

FileCloud MS Teams bot ID
Set FileCloud MS Teams Bot Id

User browser session expiry
Use FileCloud browser session timeout only

The **reCAPTCHA** settings page opens.
Open the **reCAPTCHA** settings page.

2. Enable the field **Enable FileCloud MS Teams integration**.
3. Enter the MS Teams Bot Id into **FileCloud MS Teams bot ID**.
   Get the MS Teams Bot Id from the Teams administrator or from Bot Management in MS Teams' App Studio app (see For MS Teams Admins: Configuring FileCloud in Teams (see page 97)).
4. Check **Use browser session expiry** to use the FileCloud session timeout setting (located in **Settings** on the **Server** tab).



MS Teams

Enable FileCloud MS Teams integration
Select to enable FileCloud integration with Microsoft Teams

FileCloud MS Teams bot ID
Set FileCloud MS Teams Bot Id

User browser session expiry
Use FileCloud browser session timeout only

5. Click **Save**.

Setting Up AutoCAD File Preview with Autodesk Viewer

⚠ Beginning with FileCloud 23.1, if a file has multiple 2D and 3D viewing options, the Autodesk viewer in FileCloud lets users display the different views.

ℹ Integration with Autodesk Viewer is available in FileCloud Version 22.1 and higher.
Each time an AutoCAD file is previewed, it is stored outside FileCloud on Autodesk's servers for 30 days.
The first time an AutoCAD file is previewed from your site, Autodesk charges you in flex tokens (cloud credits). Subsequent times the (unmodified) file is previewed, by any user on the site, you are not charged. You are charged again the initial time a file is previewed after being modified.
For information about purchasing flex tokens, see https://forge.autodesk.com/pricing

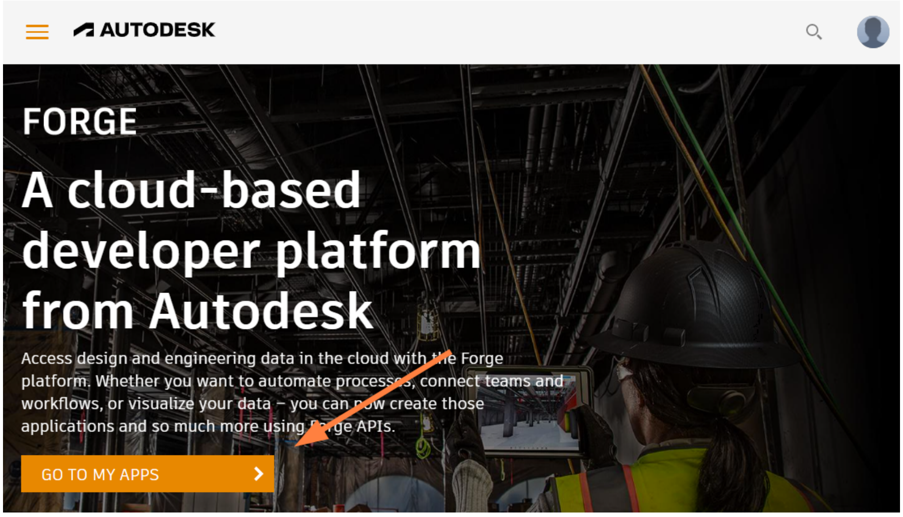
After you configure FileCloud integration with Autodesk Viewer, when users preview 3D and 2D model data file types, they are shown in Autodesk Viewer.

Setting up integration of FileCloud and Autodesk Viewer

Note: If your firewall blocks URLs that do not appear in an allowed list, make sure you add the Autodesk URL to the allowed list.

To integrate FileCloud with Autodesk Viewer:

1. Go to https://forge.autodesk.com/.
2. Sign in to your Autodesk account, or create a new one.
3. Click **GO TO MY APPS**.

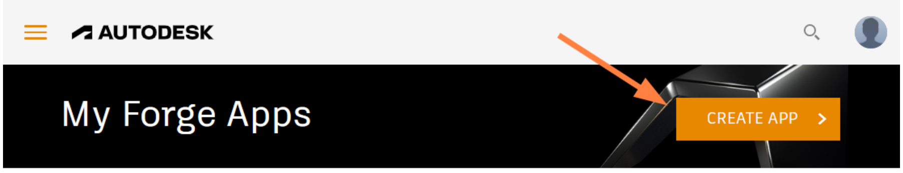


FORGE

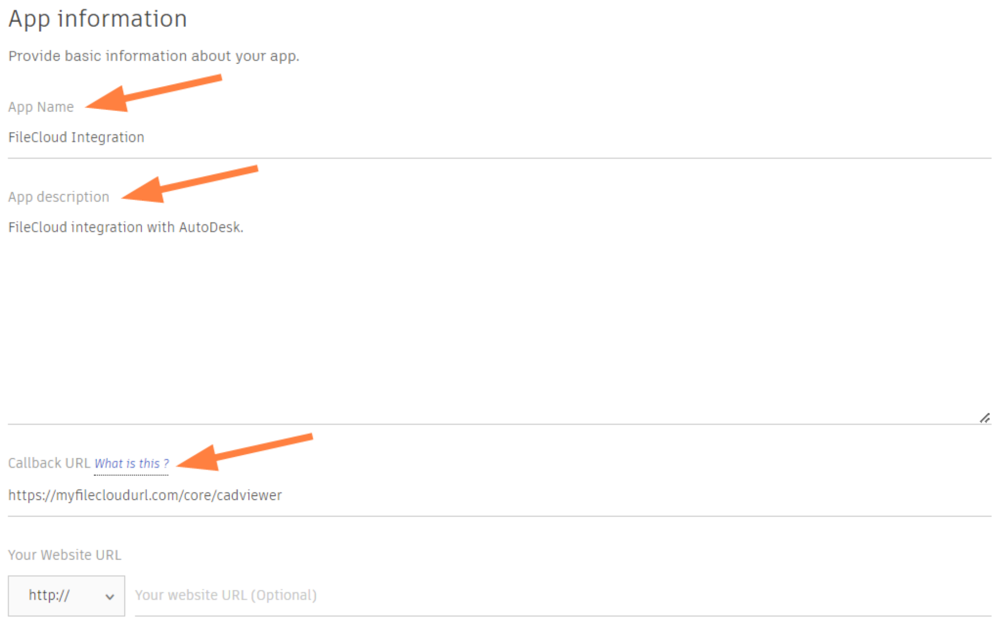
A cloud-based developer platform from Autodesk

Access design and engineering data in the cloud with the Forge platform. Whether you want to automate processes, connect teams and workflows, or visualize your data – you can now create those applications and so much more using Forge APIs.

4. Click **CREATE APP**.



5. Fill in the fields.
   - For Callback URL, enter your FileCloud url + **/core/cadviewer**, for example, https://myfilecloudurl.com/core/cadviewer.
   - You may leave **Site URL** blank, but must fill all other fields.



App information

Provide basic information about your app.

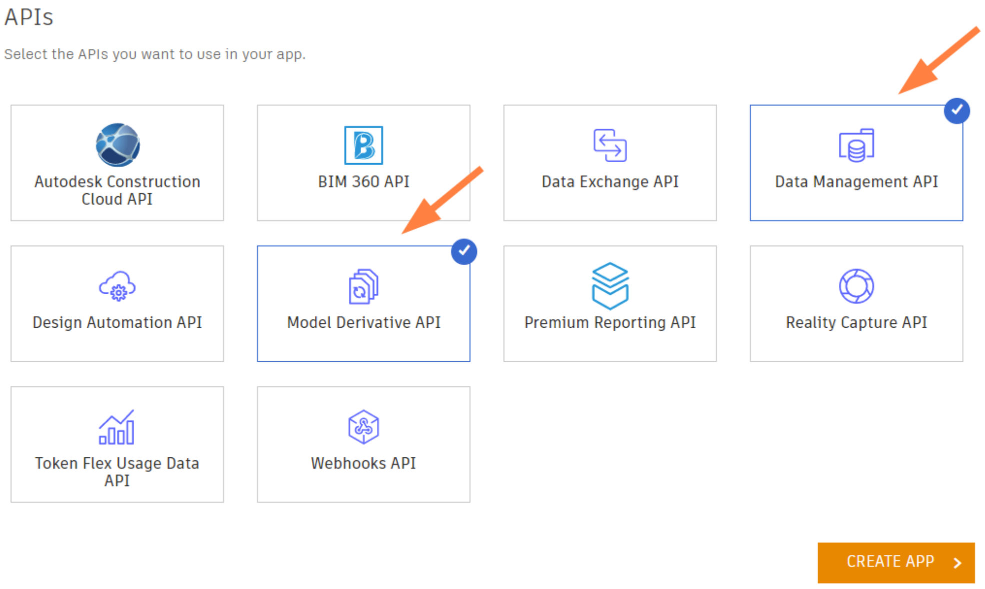
App Name: FileCloud Integration

App description: FileCloud integration with AutoDesk.

Callback URL *What is this ?*: https://myfilecloudurl.com/core/cadviewer

Your Website URL: http:// Your website URL (Optional)

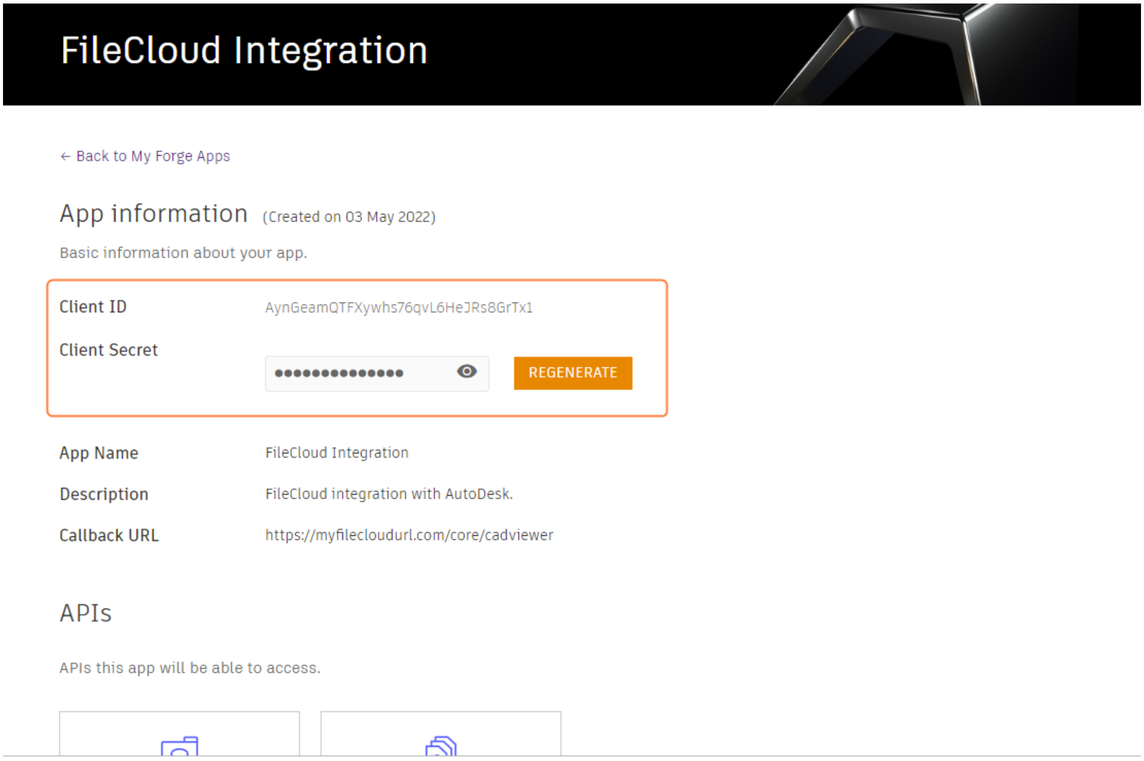
   - In the APIs section, select only **Data Management API** and **Model Derivative API**.



APIs

Select the APIs you want to use in your app.

6. Click **CREATE APP**.
   The screen lists your **Client ID** and **Client Secret**.



FileCloud Integration

← Back to My Forge Apps

App information (Created on 03 May 2022)

Basic information about your app.

Client ID AynGeamQTFXywhs76qvL6HeJRs8GrTx1

Client Secret ●●●●●●●●●●●●●●

App Name FileCloud Integration

Description FileCloud integration with AutoDesk.

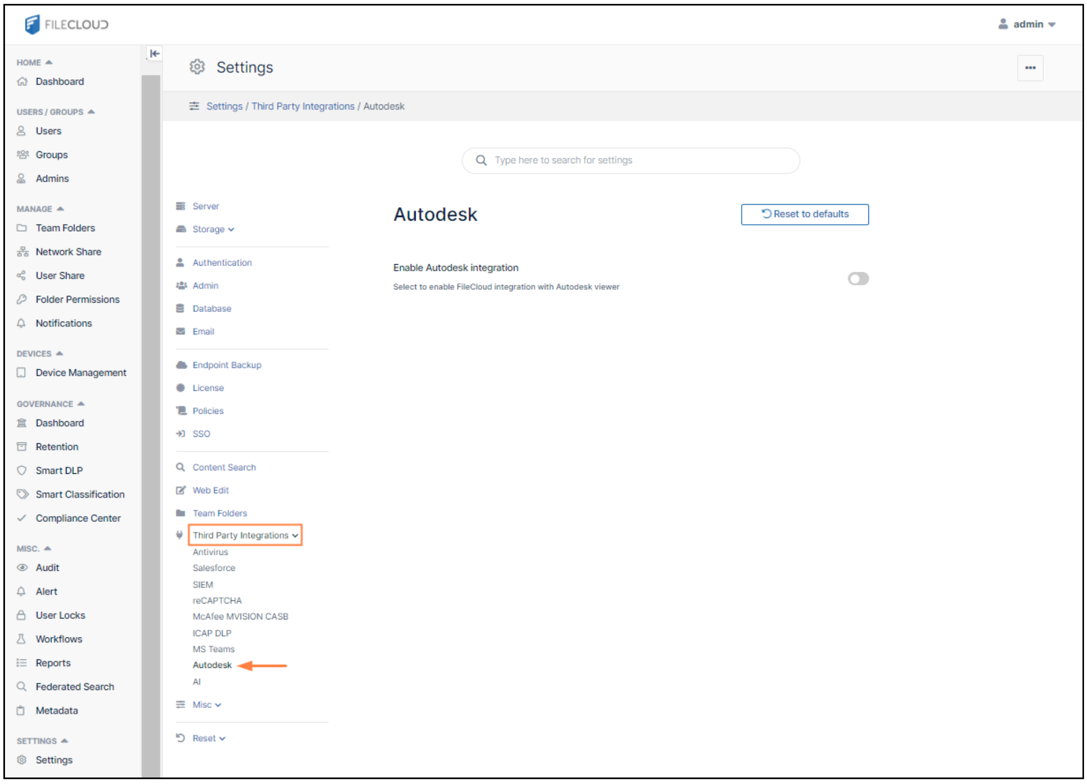
Callback URL https://myfilecloudurl.com/core/cadviewer

APIs

APIs this app will be able to access.

7. In the FileCloud admin portal, open the Autodesk settings page.
   To go to the Autodesk settings page

a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** .
b. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **Autodesk**, as shown below.



Settings / Third Party Integrations / Autodesk

Autodesk

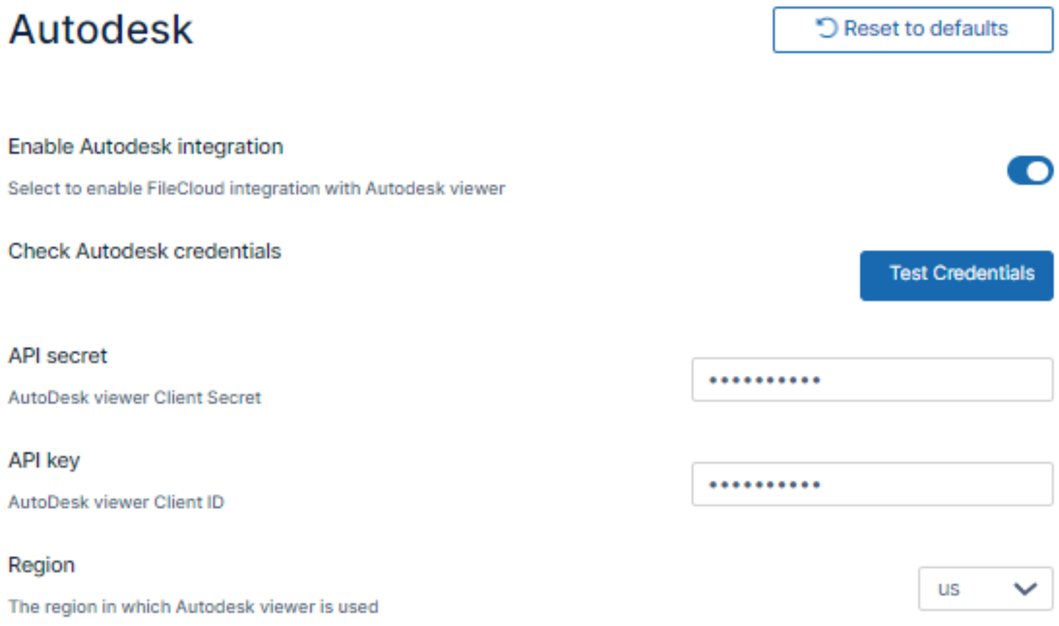
Enable Autodesk integration

Select to enable FileCloud integration with Autodesk viewer

The **Autodesk** settings page opens.

8. Enable the field **Enable Autodesk integration**.
   Additional fields appear.
9. In **API Secret,** enter your Autodesk Viewer **Client Secret**.
10. In **API key**, enter your Autodesk Viewer **Client ID**.

11. Change the **Region** if it is not accurate.



Autodesk

Reset to defaults

Enable Autodesk integration

Select to enable FileCloud integration with Autodesk viewer

Check Autodesk credentials

Test Credentials

API secret

AutoDesk viewer Client Secret

••••••••••

API key

AutoDesk viewer Client ID

••••••••••

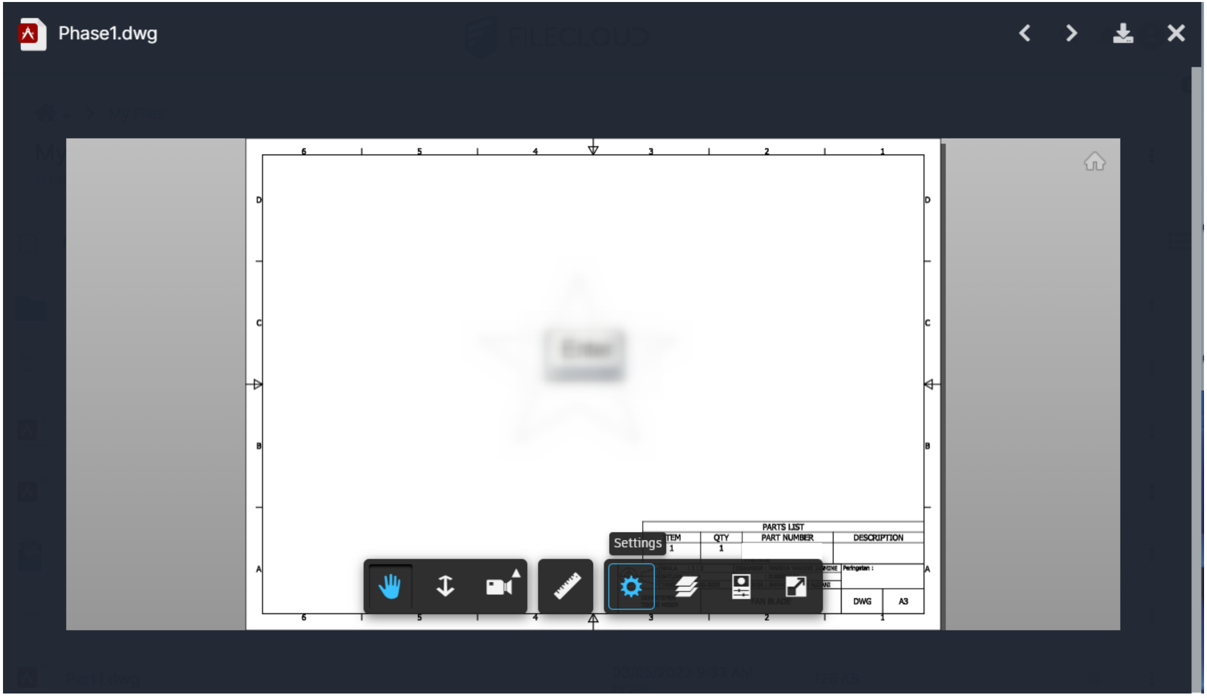
Region

The region in which Autodesk viewer is used

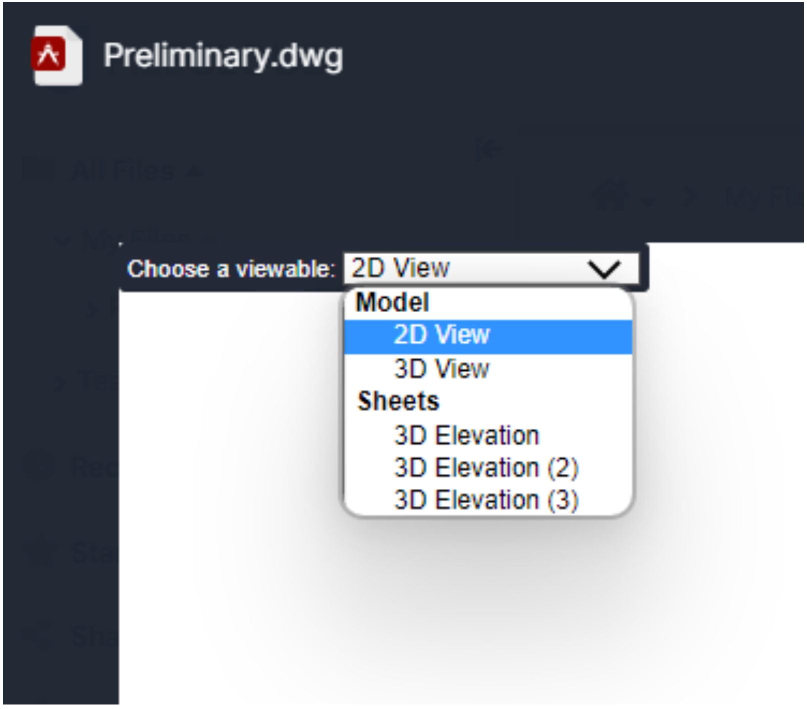
us

12. Click **Save**.
13. To complete integration of Autodesk Viewer and FileCloud, request that FileCloud Support add the **AllowEncodedSlashes** directive to the Apache SSL config file.

Your integration of Autodesk Viewer and FileCloud is now complete.
When users preview a model data file in FileCloud, they see the image in a screen similar to:



For files that have multiple views, the following drop-down list appears in the upper-left corner:



Note: The drop-down list with multiple options for viewing only appears for files that have multiple views available.

AI Integration

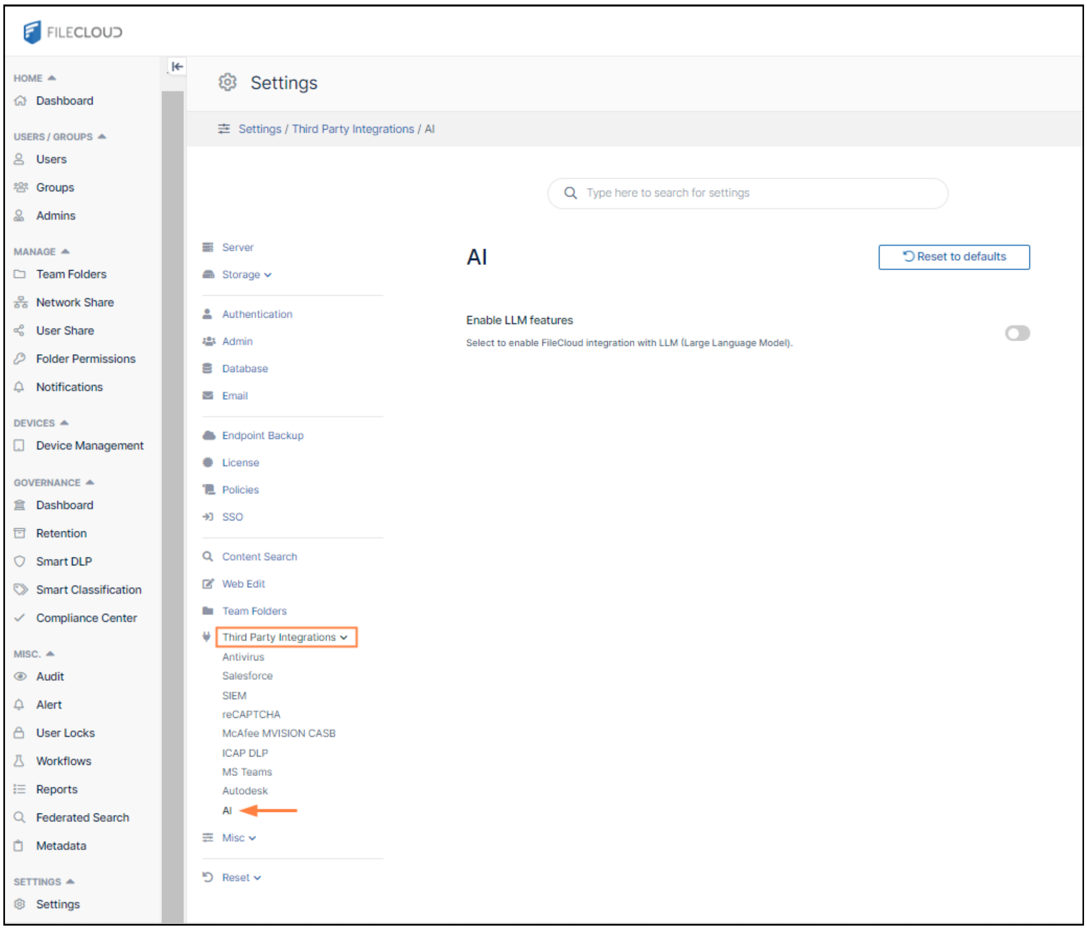
The ability to configure a Large Language Model for FileCloud Smart Classification is available in versions 23.232 and higher.

FileCloud's Smart Classification includes an AI classifier which requires integration with a Large Language Model (LLM) to function. A Large Language Model, which is trained on very large amounts of data, is a type of algorithm used in AI.

Currently, OpenAI is the only provider available for integrating FileCloud with a LLM.

To integrate FileCloud with OpenAI:

1. Open the AI settings page.
   To go to the AI settings page
    a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** 🧩.
    b. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **AI**, as shown below.

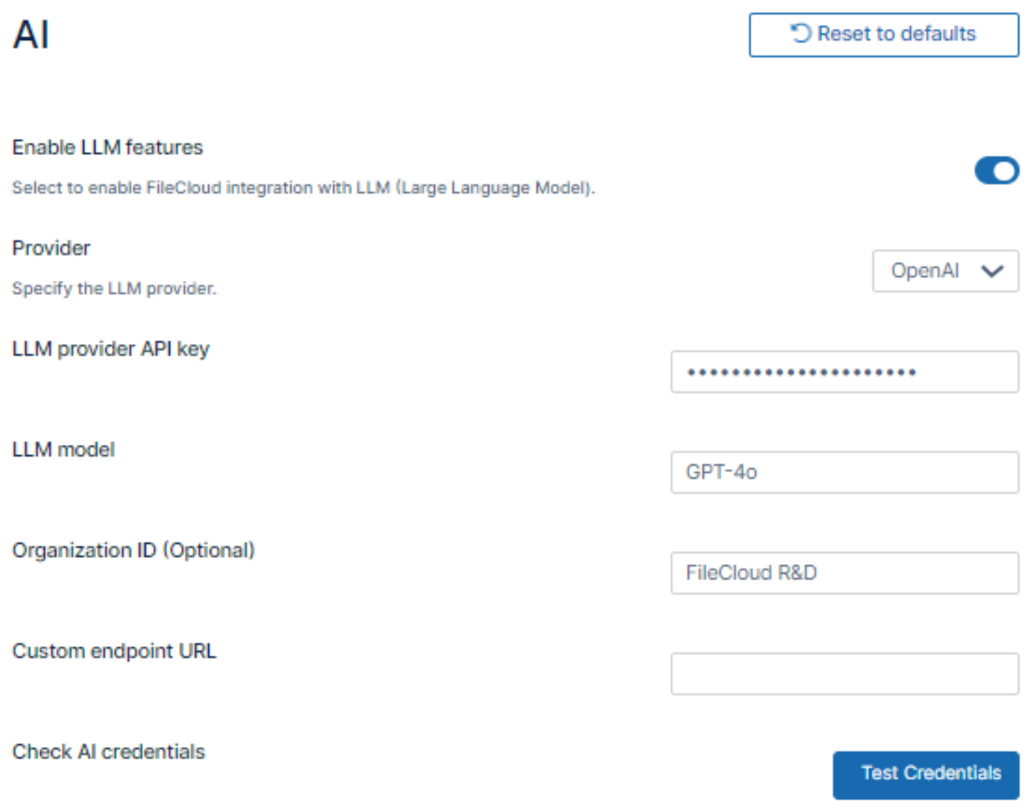


Enable LLM features

Select to enable FileCloud integration with LLM (Large Language Model).

The **AI** settings page opens.

2. Enable the setting **Enable LLM features**.
   The AI settings appear.



AI

Enable LLM features

Select to enable FileCloud integration with LLM (Large Language Model).

Provider

Specify the LLM provider.

OpenAI

LLM provider API key

••••••••••••••••••••

LLM model

GPT-4o

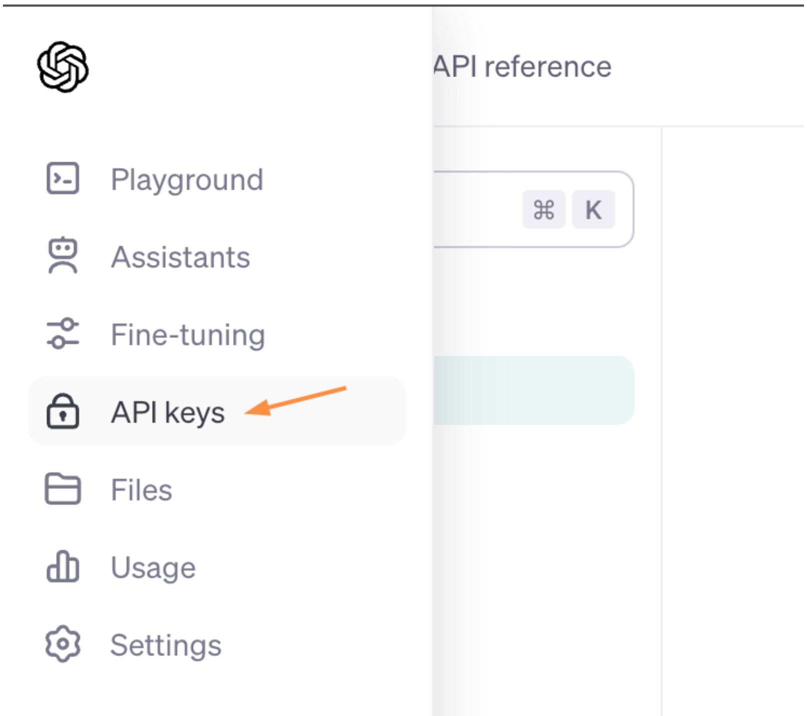
Organization ID (Optional)

FileCloud R&D

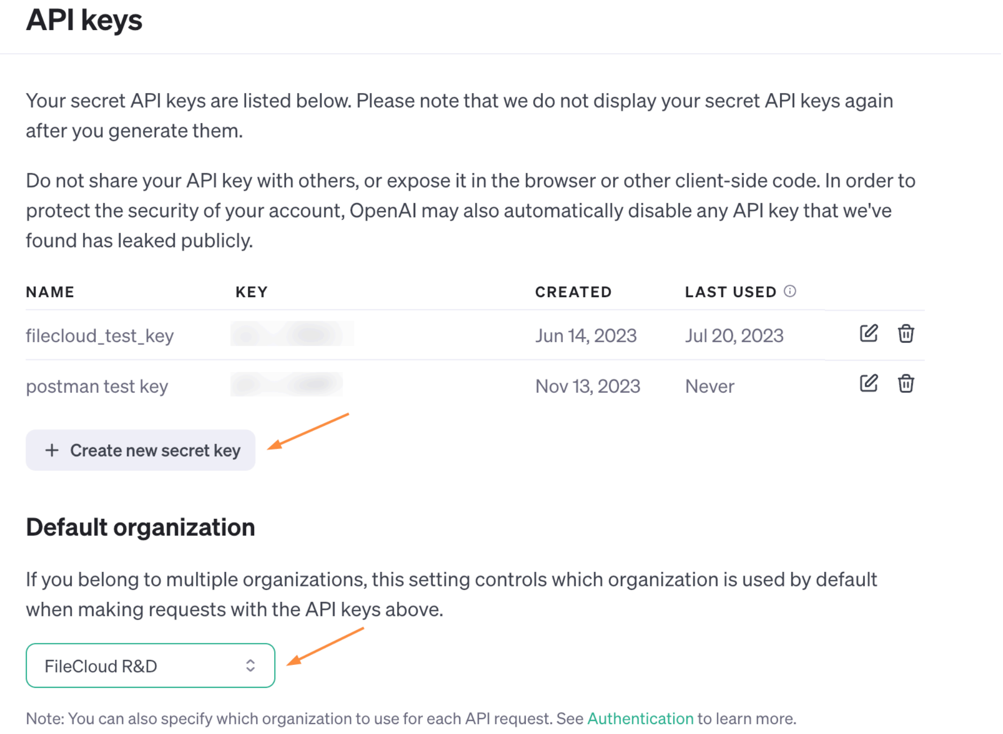
Custom endpoint URL

Check AI credentials

3. Check **Enable LLM Features**.
4. In **Provider**, choose **OpenAI**.
5. Enter the values for **LLM provider API Key** and **Organization ID**.
   To get these values, log in to the OpenAI platform at https://platform.openai.com/login (you must have a valid OpenAI subscription) and click **API keys** in the left navigation panel.



The **API keys** page opens:



API keys

Your secret API keys are listed below. Please note that we do not display your secret API keys again after you generate them.

Do not share your API key with others, or expose it in the browser or other client-side code. In order to protect the security of your account, OpenAI may also automatically disable any API key that we've found has leaked publicly.

NAME	KEY	CREATED	LAST USED ⓘ	
filecloud_test_key	[redacted]	Jun 14, 2023	Jul 20, 2023	
postman test key	[redacted]	Nov 13, 2023	Never	

Default organization

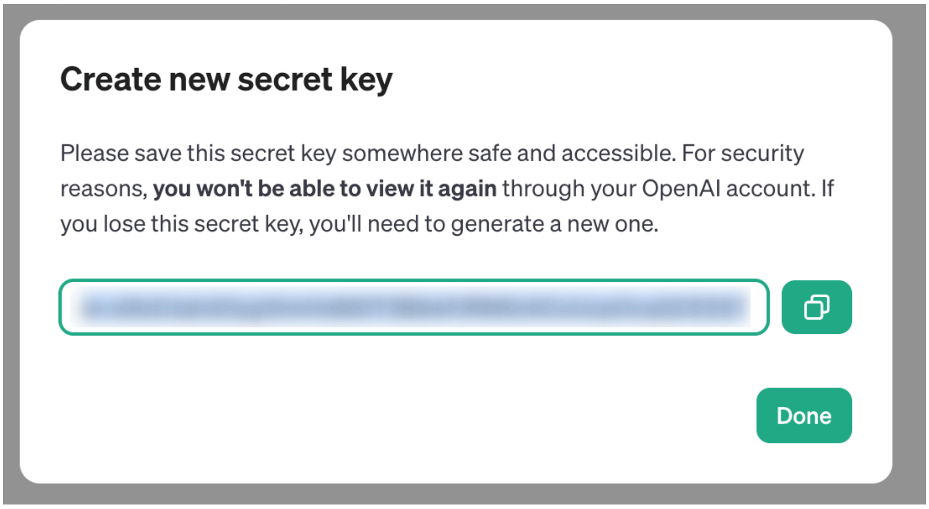
If you belong to multiple organizations, this setting controls which organization is used by default when making requests with the API keys above.

FileCloud R&D

Note: You can also specify which organization to use for each API request. See Authentication to learn more.

On the **API keys** page:

- Click **Create new secret key** and create a new key. Copy and save it (you cannot access it again through your AI account), and then enter it into **API key** on the FileCloud **AI Integration Settings** page.



Create new secret key

Please save this secret key somewhere safe and accessible. For security reasons, **you won't be able to view it again** through your OpenAI account. If you lose this secret key, you'll need to generate a new one.

- Under **Default organization**, view your organizations, and optionally, enter one into **Organization** on the FileCloud **AI Integration Settings** page to have it used with each API request.

6. In **Model**, enter the value for your model. For help determining your model, see https://platform.openai.com/docs/models.
7. In most cases you are not required to enter a **Custom URL**. It is only necessary if you use a custom OpenAI instance.
8. Click **Test Credentials** to confirm that **FileCloud** and **AI** are properly integrated.

To ensure optimal functionality and avoid disruptions, confirm that the LLM you select is currently supported by OpenAI. View the list of supported models and their deprecation timelines on OpenAI's model deprecation page[12].

[12] https://platform.openai.com/docs/deprecations

CDR Integration

> FileCloud integration with Forcepoint CDR is available in version 23.241.4 and higher.
> Forcepoint CDR is only available for customers with Advanced licenses; if you are upgrading FileCloud and intend to use Forcepoint CDR, please also upgrade your license.

When Forcepoint CDR (Content Disarm and Reconstruction) is integrated with FileCloud, each file (of a supported type) uploaded into FileCloud is put into a non-editable quarantine state and sent to Forcepoint CDR. Forcepoint CDR rebuilds the file, omitting any potentially malicious code, and returns the sanitized file to FileCloud.

Limitations:

- Forcepoint CDR does not send a notification to the user's FileCloud account if a threat is found; it simply returns the file to FileCloud with the threat removed.
- Only files in Network Folders that are changed within FileCloud are scanned and sanitized; files in Network Folders that are changed outside FileCloud are not.
- File changes made to a file in a WOPI Web edit co-editing session are not sent to Forcepoint for sanitization until all users in the session have closed the file for edit.
- While a file is in quarantine, FileCloud rejects new uploads of the file.

Integrating Forcepoint CDR with FileCloud

Required settings:

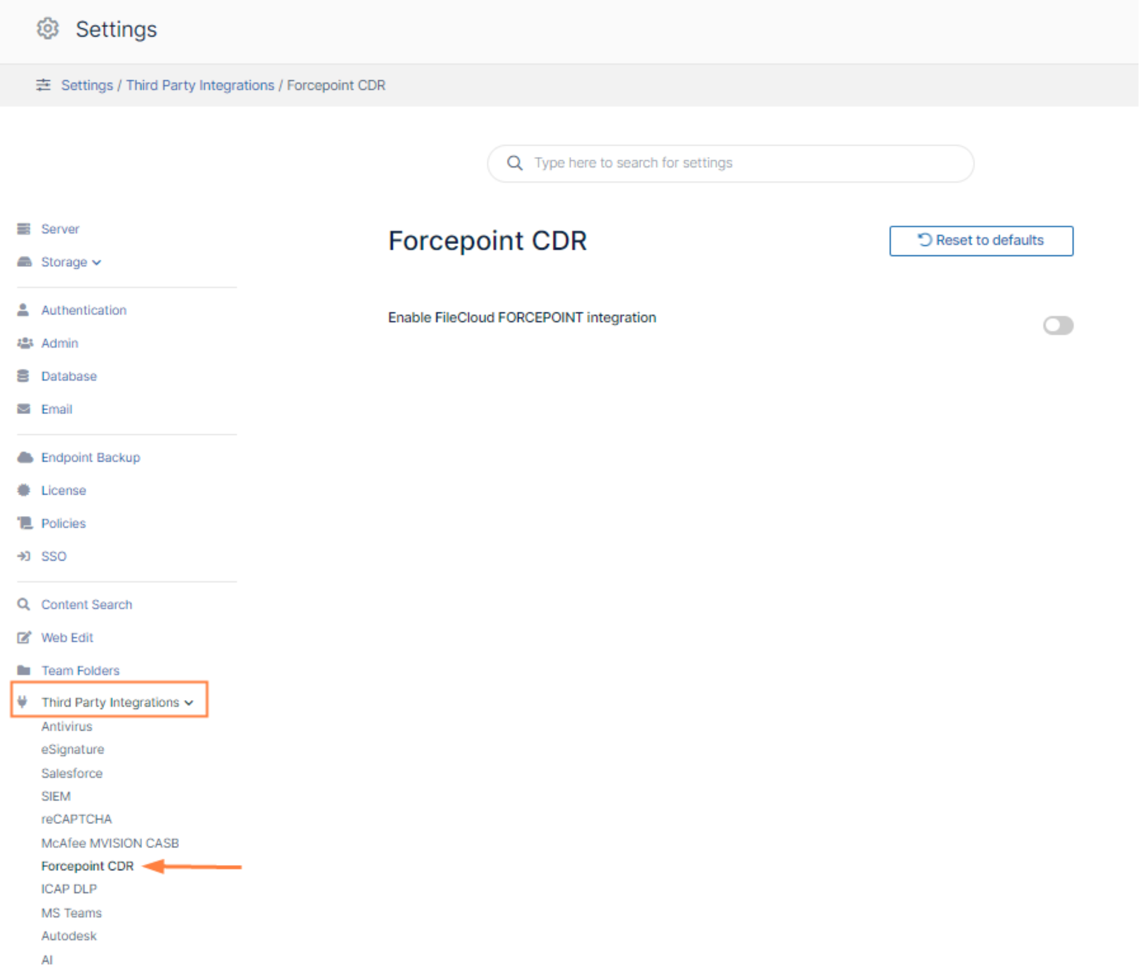
- Forcepoint CDR integration works only if locking is enabled (the default setting). For help enabling locking, see Misc Settings.
- We recommend setting **Number of old versions to keep for each file** to **1** or higher (default is **3**) before using Forcepoint CDR integration to avoid losing data. Without this setting, loss of original versions of files will occur if Forcepoint CDR returns an unsupported file and **Delete extensions that Forcepoint CDR does not support** is enabled. For help setting this value, see Setting up Managed Storage.

To set up integration Forcepoint CDR with FileCloud:

1. Open the **Forcepoint CDR** page.

To go to the Forcepoint CDR page

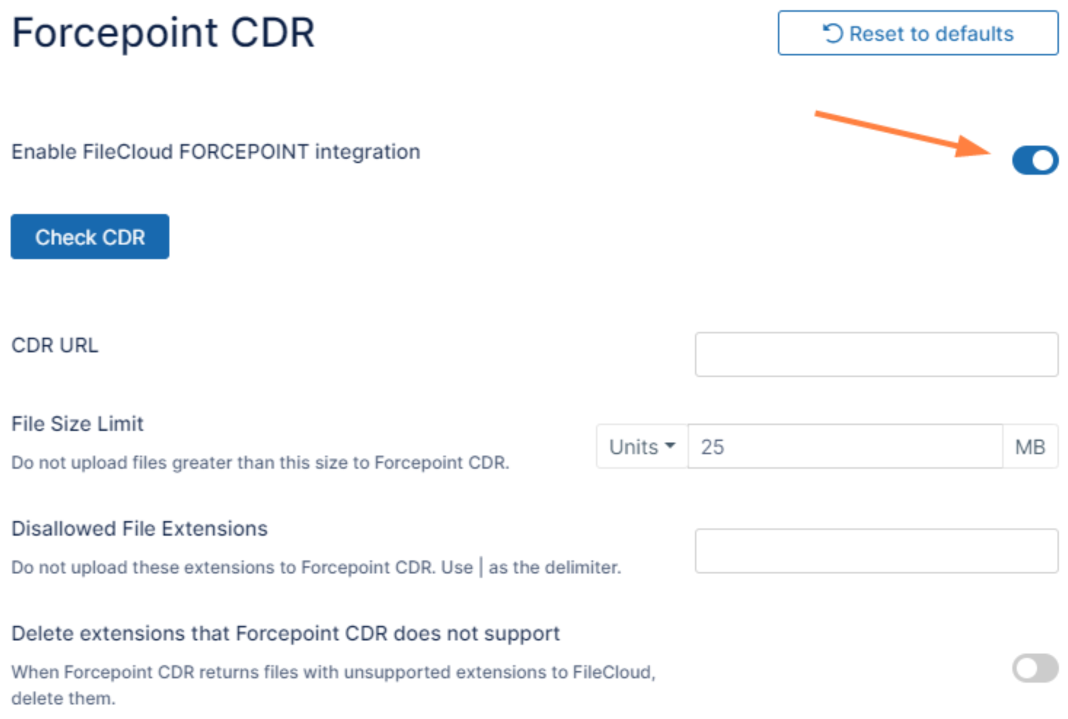
1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** 🧩 .
2. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **Forcepoint CDR**, as shown below.



Enable FileCloud FORCEPOINT integration

The Forcepoint CDR settings page opens.

2. Toggle on **Enable FileCloud FORCEPOINT integration** to view the Forcepoint fields.



Forcepoint CDR

Enable FileCloud FORCEPOINT integration

CDR URL

File Size Limit

Do not upload files greater than this size to Forcepoint CDR.

Units 25 MB

Disallowed File Extensions

Do not upload these extensions to Forcepoint CDR. Use | as the delimiter.

Delete extensions that Forcepoint CDR does not support

When Forcepoint CDR returns files with unsupported extensions to FileCloud, delete them.

3. Fill in the fields as indicated in the following table.

Field	Description	Default value	Notes
Enable FileCloud FORCEPOINT Integration	Turn integration with Forcepoint CDR on and off.	disabled	
Check CDR	Click to confirm that your **CDR URL** is valid.	N/A	
CDR URL	The URL of your company's Forcepoint CDR server	blank	

Field	Description	Default value	Notes
File Size Limit	The largest size of a file that FileCloud can send to Forcepoint CDR.	25	The maximum size we have tested that was processed successfully in Forcepoint was 100 MB. However, the maximum size any Forcepoint server can process depends on the hardware configuration of the Forcepoint server.
Disallowed File Extensions	File extensions that you want to prevent from being uploaded to Forcepoint CDR. These files remain in FileCloud but are not sanitized. (There are also file types that Forcepoint CDR cannot process. These files are treated differently; they are uploaded to Forcepoint and returned as unsupported).	blank	
Delete extensions that Forcepoint CDR does not support	Deletes files that are returned because they have extensions that Forcepoint CDR does not support. File types that are not supported for sanitization include file types that Forcepoint does not support in general, such as PSD and MP4, and file types blocked by your Forcepoint CDR configuration. For more information see Forcepoint's online CDR help[13].	disabled	

4. To ensure that integration with Forcepoint CDR runs efficiently, add the following configuration in the message queue config file:
   a. Open the message queue config file:
      Windows location: **C:/xampp/htdocs/src/Scripts/config/default.json**
      Linux location: **/var/www/html/src/Scripts/config/default.json**

[13] https://help.forcepoint.com/frbi/en-us/onlinehelp/guid-203e1b9b-4770-413b-9a2e-0d8e1dd41af8.html

b. Set the field **parallel_high_priority_workers_count** to a value of **1** or higher.
We recommend initially setting the value to around 20% of the value in **parallel_workers_count**, and modifying it as necessary for your environment.

If Forcepoint CDR cannot sanitize a file due to an error a notification is sent to the user and both a notification and an email are sent to the admin.

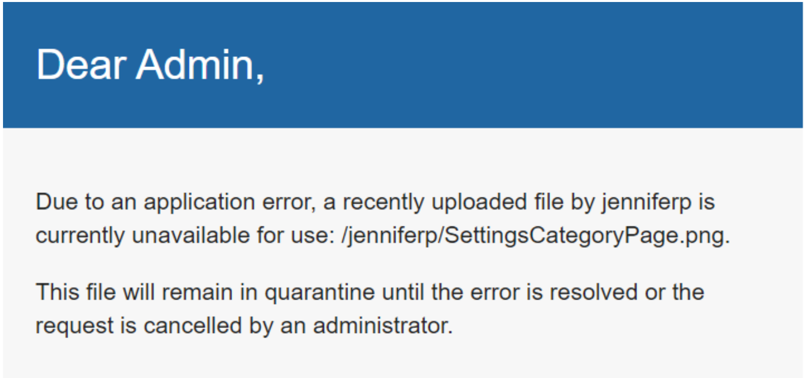
- Files that cannot be sanitized due to an error are repeatedly resent for sanitization until it is successful or the admin goes to the **Quarantined Files** page and either deletes the non-sanitized file version or removes it from quarantine.
- If **Delete extensions that Forcepoint CDR does not support** is enabled, files with extensions that are not supported by Forcepoint CDR are deleted from FileCloud. If there is a prior version of the file in FileCloud (if it was an update to a file) the original version is not deleted.
- To customize the email sent to the user, go to Customization > Email Templates and edit the template **Errors During Sanitization On Forcepoint CDR Email Template**.

While a file is being sanitized, the file and its parent folders are locked for editing and other changes. The screen does not reflect that the file has been returned from Forcepoint CDR and is now unlocked until the user refreshes the screen, as in the following video.

Notice that the size of the file in the video is reduced after processing. This may happen when the file is recreated in Forcepoint CDR, making it slightly smaller or larger. If it takes longer than a minute to process the uploaded/modified file in Forcepoint CDR, the file's modified date will reflect the time change.

Deleting file versions in quarantine

If a file cannot be sanitized due to an error, it is repeatedly resent for sanitization until it is successful or an admin either deletes the non-sanitized file version or removes it from quarantine. Each time it is sent for sanitization and fails FileCloud sends you a notification:



Dear Admin,

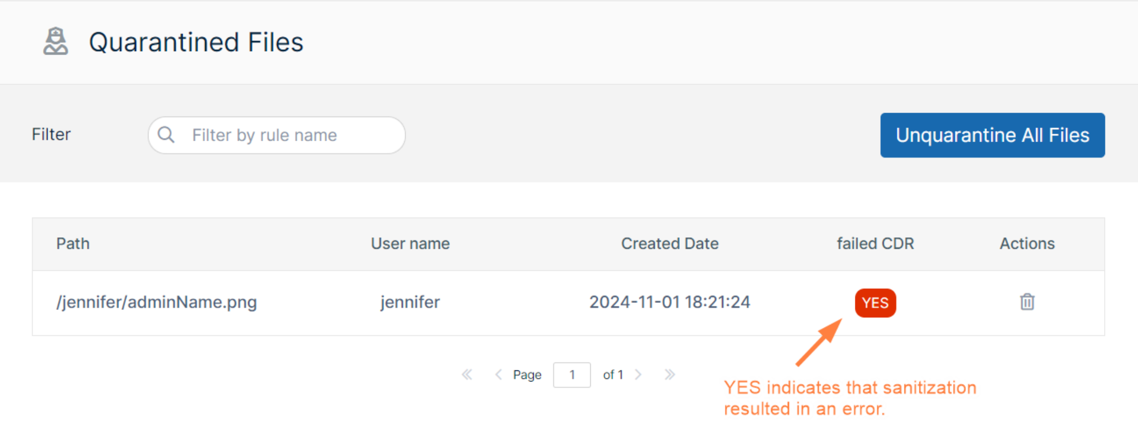
Due to an application error, a recently uploaded file by jenniferp is currently unavailable for use: /jenniferp/SettingsCategoryPage.png.

This file will remain in quarantine until the error is resolved or the request is cancelled by an administrator.

The file listed in the **Quarantined Files** screen is the version of the file that has been quarantined and sent for sanitization, which is the latest version of the file. Earlier versions of the file may exist in FileCloud and will remain in FileCloud even if you delete the versions in quarantine.

To delete a file that is repeatedly being sent for sanitization:

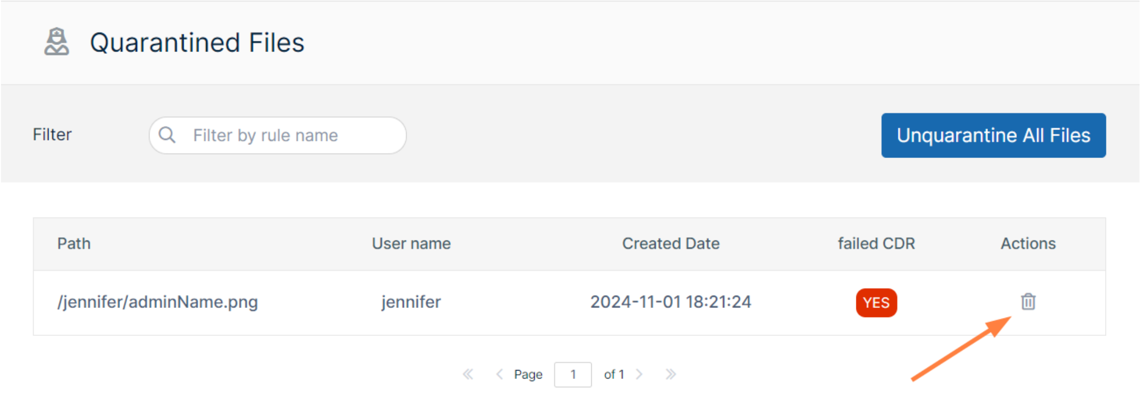
1. In the admin portal navigation panel, click **Quarantined Files**.
   All quarantined files are listed, including those that haven't finished the initial sanitization process as well as those that are being repeatedly sent for sanitization due to an error.
   Files listed because they have not finished the initial sanitization process do not have the **Delete** option.
   If files are listed because of an error, the failed CDR column displays **YES**.



Path	User name	Created Date	failed CDR	Actions
/jennifer/adminName.png	jennifer	2024-11-01 18:21:24	YES	🗑

YES indicates that sanitization resulted in an error.

2. To delete a file version (a sanitization request) stuck in quarantine, in the **Actions** column, click the Delete icon.



Path	User name	Created Date	failed CDR	Actions
/jennifer/adminName.png	jennifer	2024-11-01 18:21:24	YES	

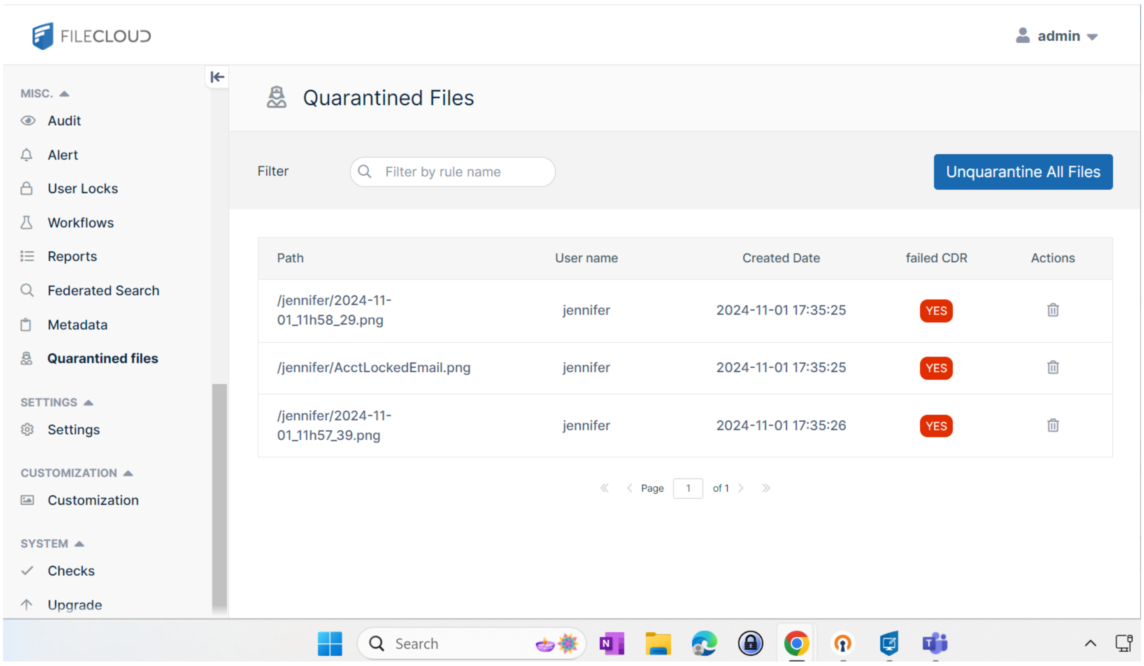
The file no longer appears in the **Quarantined Files** page.
The deleted version of the file is removed from FileCloud, and is no longer sent for sanitization.
Note: If this is the only version of the file in FileCloud, the file is deleted permanently from FileCloud and is not sent to the recycle bin.

Removing all files from quarantine

The **Quarantined Files** page includes a button for removing all files from quarantine. If you click this button, all file versions in quarantine, including those that have not yet completed the sanitization process and those that are stuck in the sanitization process due to an error, are removed from quarantine but not deleted from FileCloud. All of these versions of files become available for use in FileCloud in their non-sanitized state.

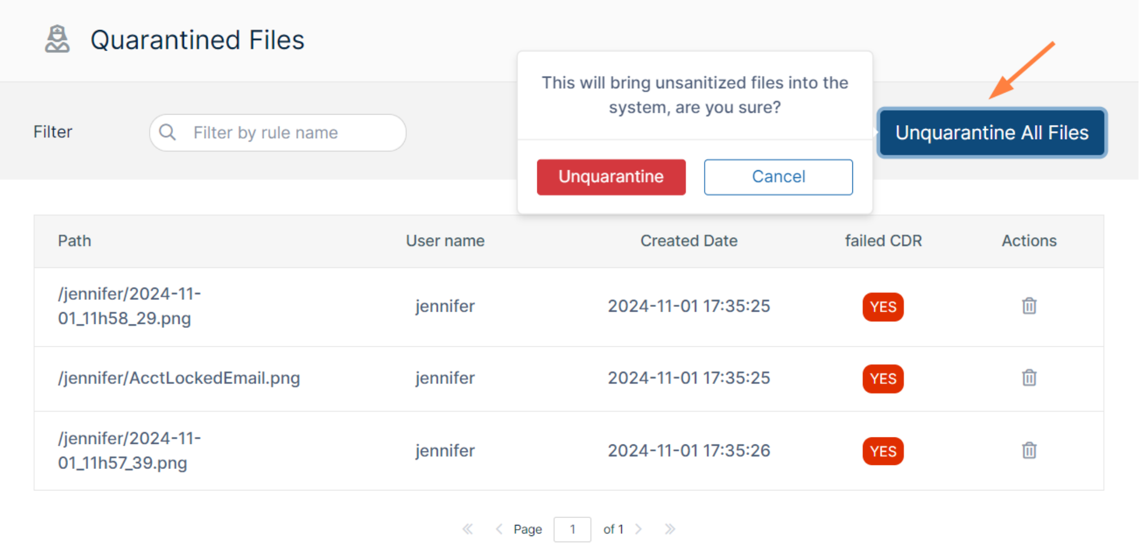
To remove all files from quarantine:

1. In the admin portal navigation panel, click **Quarantined files**.
   All quarantined files are listed.



Path	User name	Created Date	failed CDR	Actions
/jennifer/2024-11-01_11h58_29.png	jennifer	2024-11-01 17:35:25	YES	🗑
/jennifer/AcctLockedEmail.png	jennifer	2024-11-01 17:35:25	YES	🗑
/jennifer/2024-11-01_11h57_39.png	jennifer	2024-11-01 17:35:26	YES	🗑

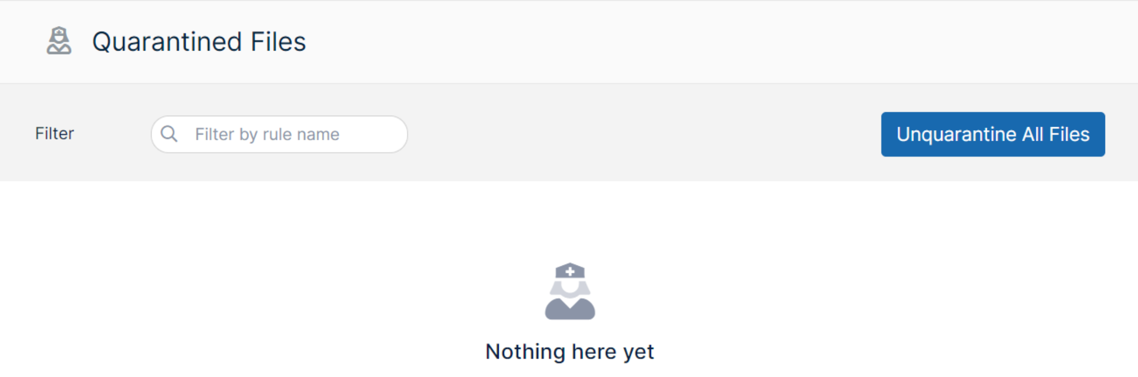
2. To remove all files from quarantine, click the **Unquarantine All Files** button.
   A confirmation box that warns you that unsanitized files will be brought into the system pops up.
3. If it is okay for the files to remain unsanitized, click **Unquarantine** in the confirmation box.



This will bring unsanitized files into the system, are you sure?

Path	User name	Created Date	failed CDR	Actions
/jennifer/2024-11-01_11h58_29.png	jennifer	2024-11-01 17:35:25	YES	🗑
/jennifer/AcctLockedEmail.png	jennifer	2024-11-01 17:35:25	YES	🗑
/jennifer/2024-11-01_11h57_39.png	jennifer	2024-11-01 17:35:26	YES	🗑

All of the files are removed from the **Quarantined files** screen:



Quarantined Files

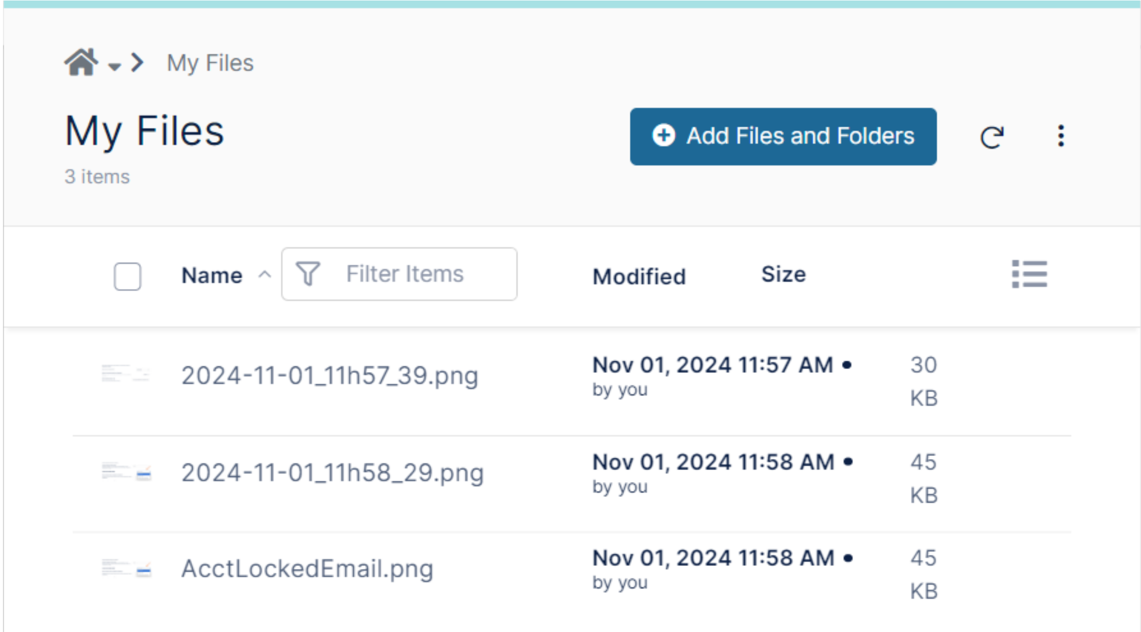
Filter

Filter by rule name

Unquarantine All Files

Nothing here yet

The files remain available to the user who created or uploaded them:



My Files

3 items

Name	Modified	Size
2024-11-01_11h57_39.png	Nov 01, 2024 11:57 AM • by you	30 KB
2024-11-01_11h58_29.png	Nov 01, 2024 11:58 AM • by you	45 KB
AcctLockedEmail.png	Nov 01, 2024 11:58 AM • by you	45 KB

eSignature Integration

ⓘ Integration of FileCloud with Signority's eSignature platform is available in FileCloud versions 23.241.4 and higher.
Some user's plans may not include the digital signature option discussed here.

☒ To ensure that your connection to Signority works properly, if you are using a firewall or blocking public connections, please allow requests from 52.60.130.76, Signority's IP address.

FileCloud can be configured to integrate with Signority's eSignature platform to enable your users to submit files for eSignatures.

How the eSignature process works

In FileCloud, the user selects one or more files to be signed. FileCloud creates a new PDF containing the file or files and prompts the user to specify a name for the PDF, a location for the signed document in FileCloud, and recipients who will be sent the document for signing. (The original files remain as they are, and can be used to create other signature documents.)

After the eSignature document is created, the user sends it from FileCloud to Signority and is prompted to add signature fields to the document for each recipient. The user then directs Signority to send signing requests to each recipient.
Users have the option of sending a document for eSignature or digital signature. To understand the difference between eSignatures and digital signatures, see signority-esignature-vs-digital-signature-infographic.pdf[14]

The user can now follow the signature document's status in FileCloud when the recipients sign it, and it moves from **In Progress** to **Completed**. The user also receives emails when each recipient finishes signing the document and when all recipients have finished signing.

[14] https://www.signority.com/wp-content/uploads/2020/03/signority-esignature-vs-digital-signature-infographic.pdf

Now, the user can access the signed PDF in the FileCloud location specified for storing the signed document.

eSignature documents for signing requests that are in draft or in progress are stored in Signority as well as FileCloud. When a signing request is completed, deleted, or expired, the eSignature document is removed from Signority.

The signer's experience

Reviewing and signing the document

The signer receives an email alerting them that a document is waiting for them to sign it. The signer clicks a link in the email to access the document in Signority. Once the user has reviewed the document in Signority they can sign it, and their task is complete. Signority automatically sends the signed document back to FileCloud.

Prerequisites for FileCloud/Signority integration

- You must have a trial or paid Signority account, obtained either prior to setting up integration or obtained through FileCloud's admin portal **eSignature** screen.
- eSignature must be enabled in a user's policy for the user to be able to use the eSignature feature. By default, the feature is enabled in all policies.
- Document Converter must be installed and running in FileCloud.

File types supported for eSignature

The file types currently supported in FileCloud for eSignature are:

- PDF
- DOCX
- PPTX
- PNG
- JPG/JPEG

File types that are not supported for eSignature do not show the **eSignature** option in the More [...] drop-down list.

Limitations

- The combined size of all files in a single signing request may not exceed 50 MB.

- Translations of the user interface are available in Arabic, French, Portuguese, and Spanish. However:
  - Messages from the server, which appear when users view a request in the eSignature screen, are not translated.
  - The admin portal does not support these translations.
- Audit details are omitted by default, but can be returned combined with an eSignature document or as a separate file. See To return audit details, below, for information on returning audit details.
- DLP rules that block files from being shared do not block them from being sent for eSignatures.

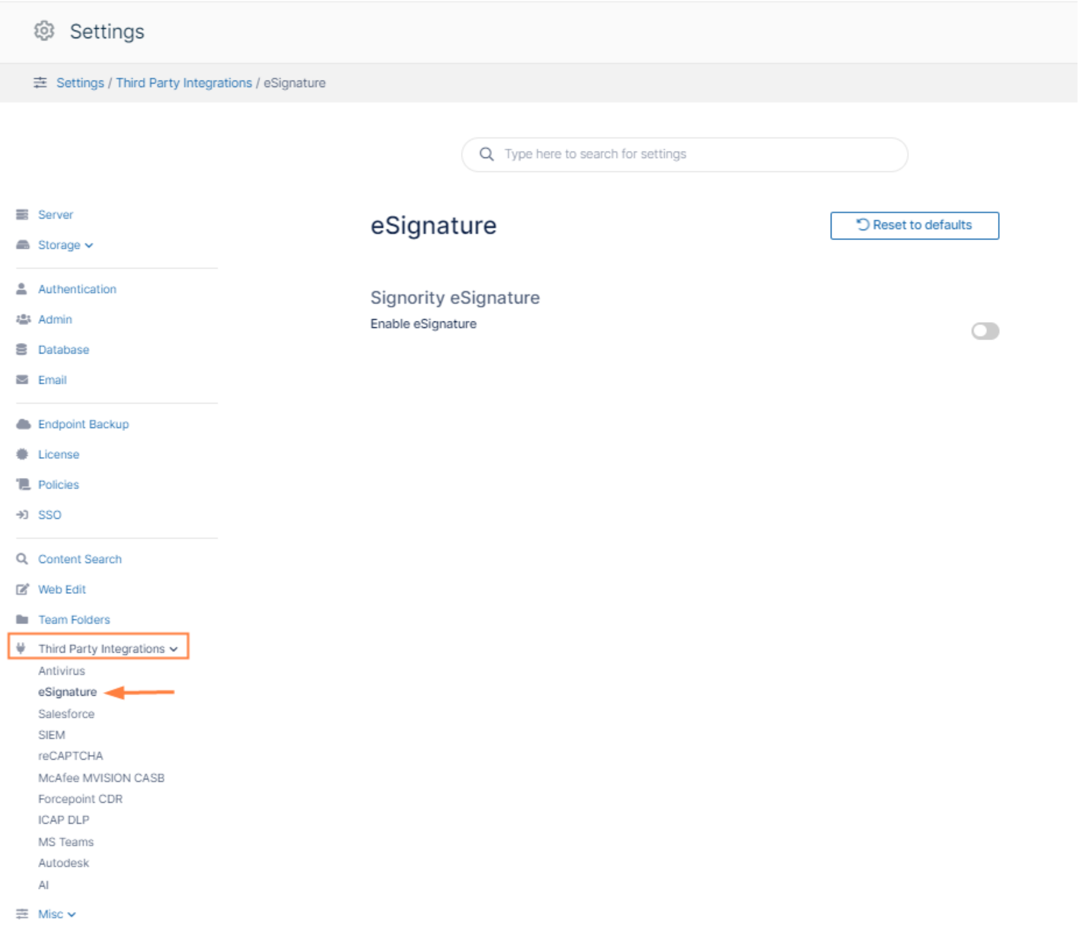
Integrate FileCloud with Signority

The first time you access the eSignature screen you are required to either obtain a trial Signority account through FileCloud or enter the credentials for your existing Signority account

To enable eSignature:

1. Install and run FileCloud Document Converter if it is not running already. For help, see FileCloud Document Converter[15].
2. Go to the **eSignature** page.
   To go to the eSignature page
   a. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings.** Then, on the **Settings** navigation page, click **Third Party Integrations** .
   b. In the inner navigation bar on the left of the **Third Party Integrations** page, expand the **Third Party Integrations** menu, and click **eSignature**, as shown below.

[15] https://www.filecloud.com/supportdocs/fcdoc/latest/server/filecloud-administrator-guide/filecloud-site-setup/document-settings/setting-up-document-preview/filecloud-document-converter



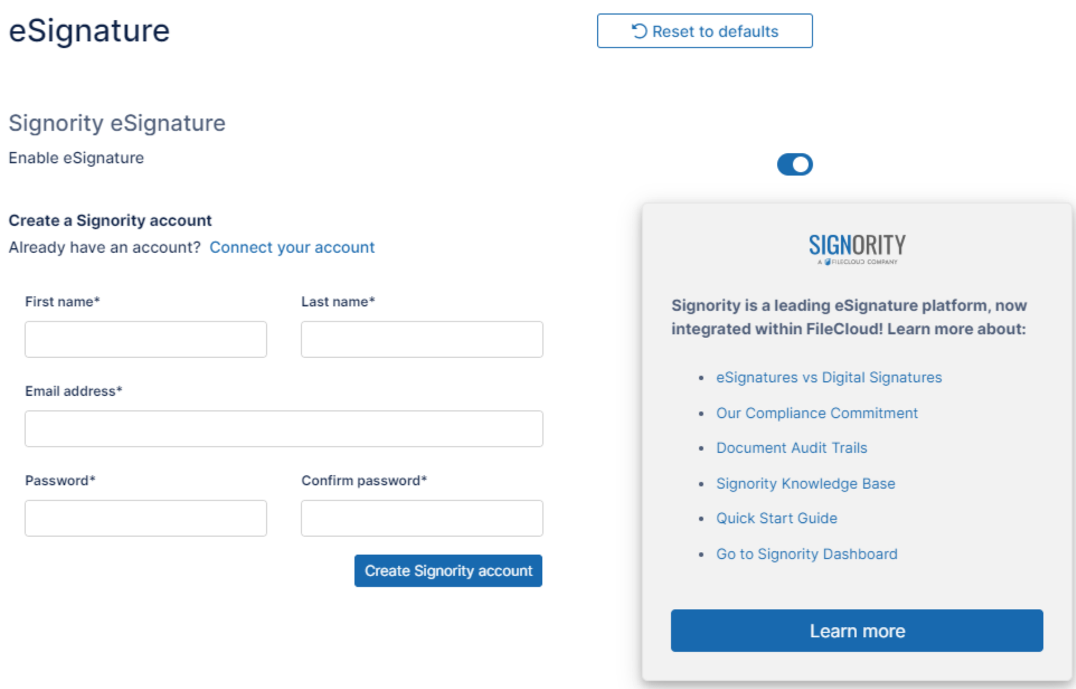
eSignature

Signority eSignature

Enable eSignature

The eSignature settings page opens.

3. Enable the **Enable eSignature** setting.
   Fields for creating a trial Signority Account appear along with the link **Connect your account** for users who already have accounts.



eSignature

Reset to defaults

Signority eSignature

Enable eSignature

Create a Signority account

Already have an account? Connect your account

First name*

Last name*

Email address*

Password*

Confirm password*

Create Signority account

SIGNORITY

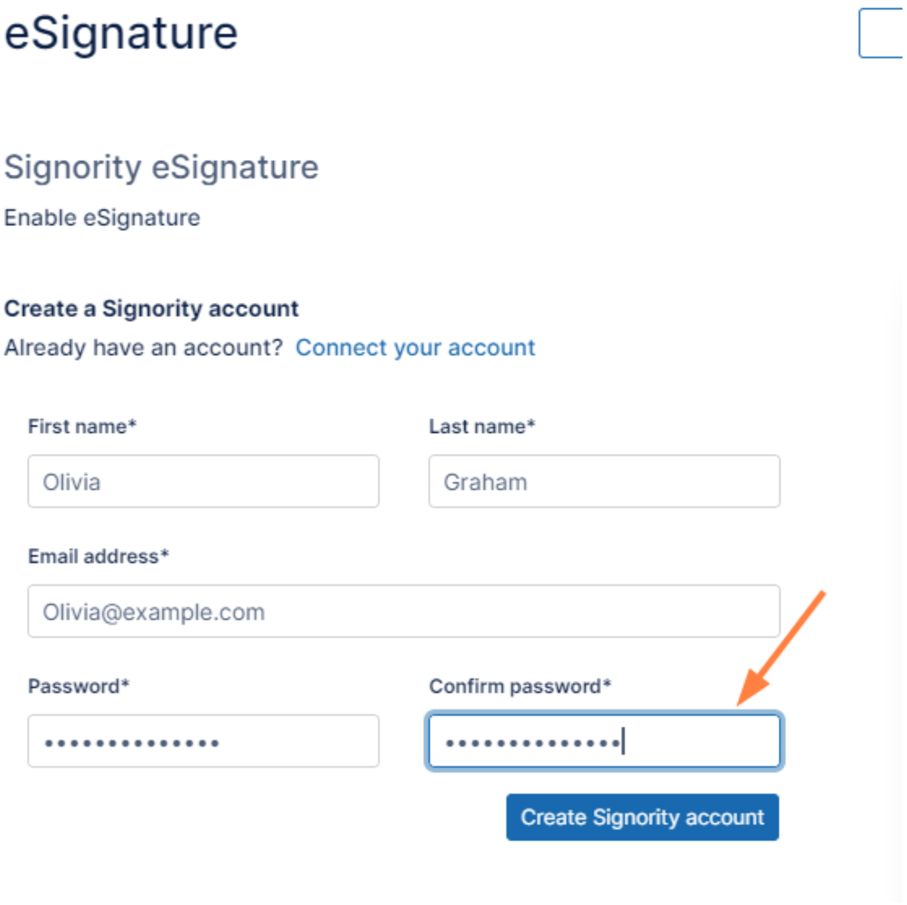
Signority is a leading eSignature platform, now integrated within FileCloud! Learn more about:

- eSignatures vs Digital Signatures
- Our Compliance Commitment
- Document Audit Trails
- Signority Knowledge Base
- Quick Start Guide
- Go to Signority Dashboard

Learn more

To create a trial Signority account:

1. Enter the information requested, and click **Create Signority Account**.



eSignature

Signority eSignature

Enable eSignature

Create a Signority account

Already have an account? Connect your account

First name*: Olivia

Last name*: Graham

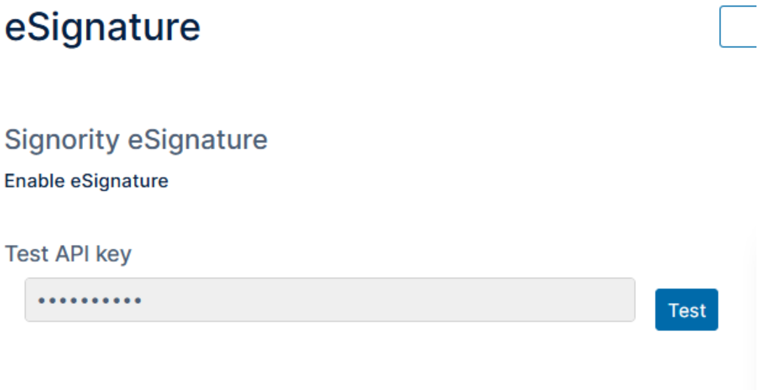
Email address*: Olivia@example.com

Password*: ••••••••••••••

Confirm password*: ••••••••••••••

Your Signority account is created. The screen now appears as follows, with **Enable eSignature** checked and your **API Key** automatically filled in.

2. Click **Test** to make sure integration with Signority works correctly.



eSignature

Signority eSignature

Enable eSignature

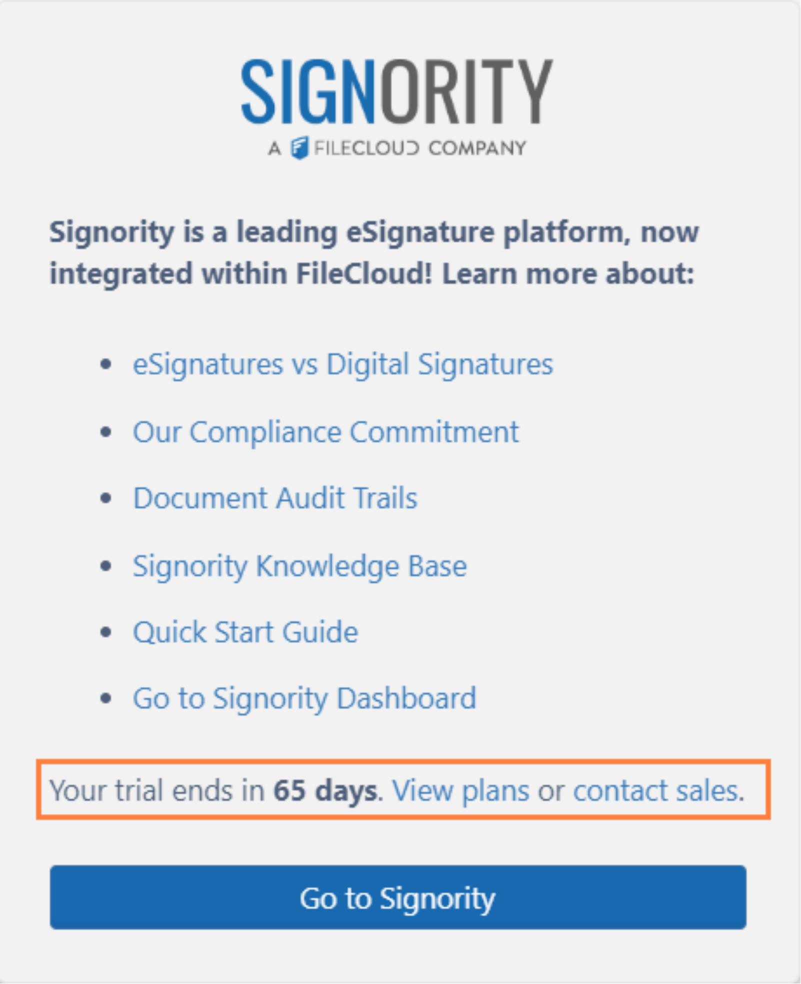
Test API key: ••••••••••

If the test returns a success message, FileCloud integration with Signority is complete, and your users are now able to obtain eSignatures on files.

The trial account lasts for 90 days. You are sent notifications prior to expiration reminding you that before the trial expires, you must purchase a paid account to maintain eSignature capability. If you haven't purchased a paid account by the time your trial account expires, any documents already sent for eSignature can still be signed and processed; however, no new documents can be sent for eSignatures.

To convert a Signority account from trial to paid

The eSignature screen includes Signority box that keeps count of the days remaining in your trial account and gives you links for viewing Signority account plans or contacting Signority sales:



Signority is a leading eSignature platform, now integrated within FileCloud! Learn more about:

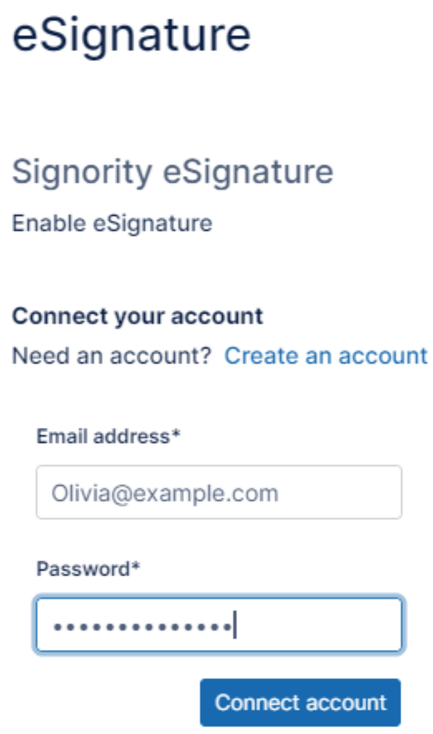
- eSignatures vs Digital Signatures
- Our Compliance Commitment
- Document Audit Trails
- Signority Knowledge Base
- Quick Start Guide
- Go to Signority Dashboard

Your trial ends in **65 days**. View plans or contact sales.

Click **contact sales** to proceed with your Signority license purchase.

If you already have a Signority account:

1. Click **Connect your account**.
2. Enter your email address and password into the corresponding fields, and click **Connect Account**.



eSignature

Signority eSignature

Enable eSignature

Connect your account

Need an account? Create an account

Email address*

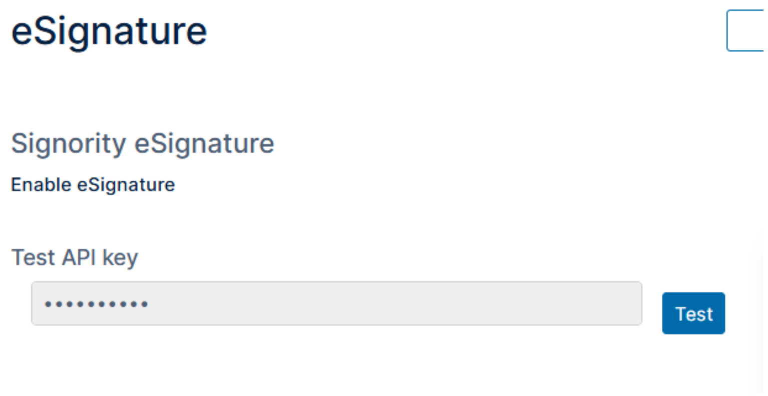
Olivia@example.com

Password*

••••••••••••••

The screen now appears as follows, with **Enable eSignature** checked and your **API Key** automatically filled in.

3. Click **Test** to make sure integration with Signority works correctly.



eSignature

Signority eSignature

Enable eSignature

Test API key

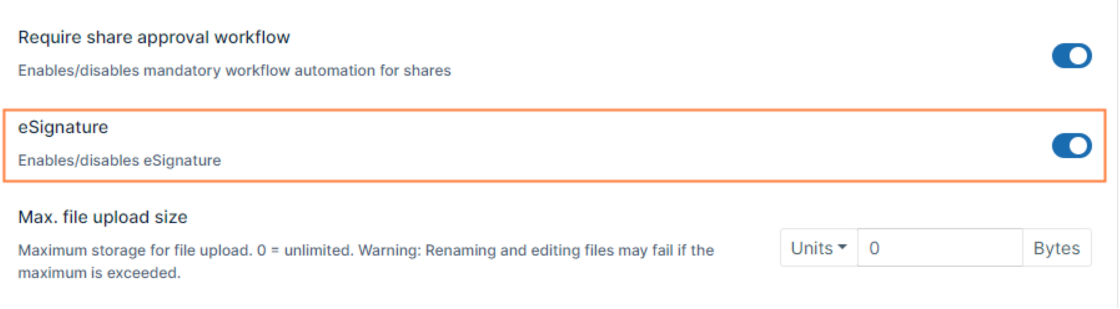
••••••••••

If the test returns a success message, FileCloud integration with Signority is complete, and your users are now able to obtain eSignatures on files.

To enable/disable eSignatures for certain users:

By default, the eSignature feature is enabled in users' policies.

1. In the FileCloud admin portal's left navigation bar, scroll down and click **Settings**. Then, on the **Settings** navigation page, click **Policies** .
   The **Policies** page opens.
2. Edit the users' policy.
3. Click the **User Policy** tab.
   Scroll down until you see the **eSignature** field.
4. Enable or disable **eSignature**.



Require share approval workflow
Enables/disables mandatory workflow automation for shares

eSignature
Enables/disables eSignature

Max. file upload size
Maximum storage for file upload. 0 = unlimited. Warning: Renaming and editing files may fail if the maximum is exceeded.

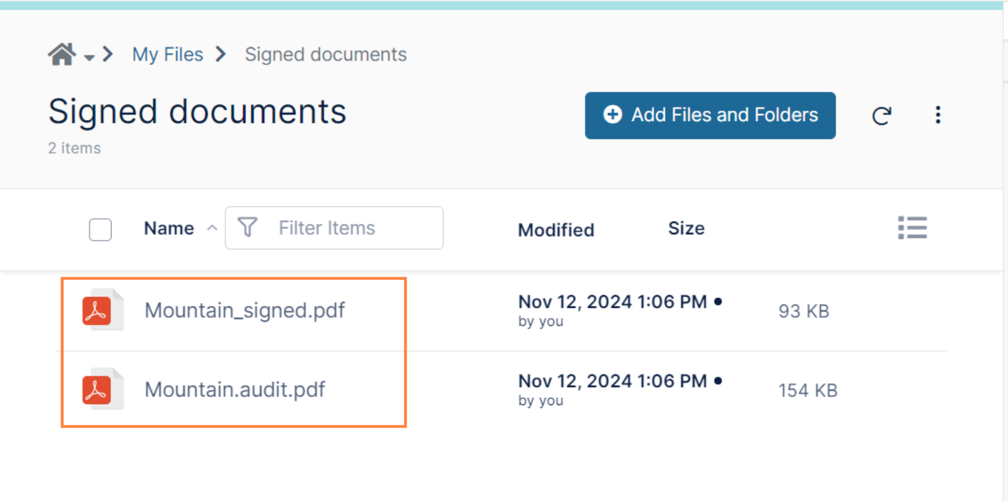
For information about the eSignature process for users, see eSignature Requests.

To return audit details

When the files are accessed in FileCloud:

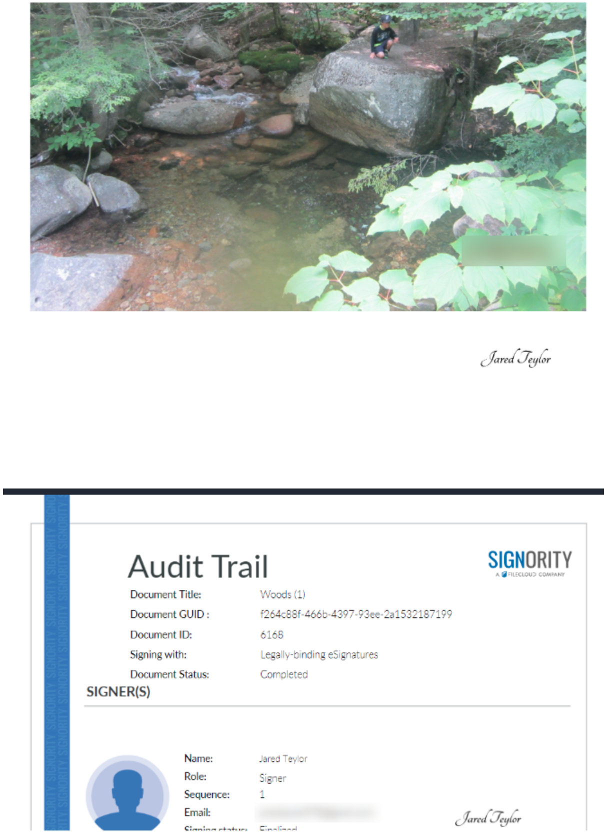
By default, when the eSignature document is returned to the destination path specified by the user or the Completed panel in the eSignature page in FileCloud, the document is returned without audit details. However, you may configure the process to either return a separate audit file or audit details attached to the eSignature document in the destination folder,

When separate signed and audit files are configured, they appear in the destination folder as:



Name	Modified	Size
Mountain_signed.pdf	Nov 12, 2024 1:06 PM • by you	93 KB
Mountain.audit.pdf	Nov 12, 2024 1:06 PM • by you	154 KB

When audit details are attached to the eSignature document, the audit information follows the signature file in the eSignature pdf:



Jared Teylor

Audit Trail

Document Title:	Woods (1)
Document GUID :	f264c88f-466b-4397-93ee-2a1532187199
Document ID:	6168
Signing with:	Legally-binding eSignatures
Document Status:	Completed

SIGNER(S)

Name:	Jared Teylor
Role:	Signer
Sequence:	1
Email:	[redacted]
Signing status:	Finalized

Jared Teylor

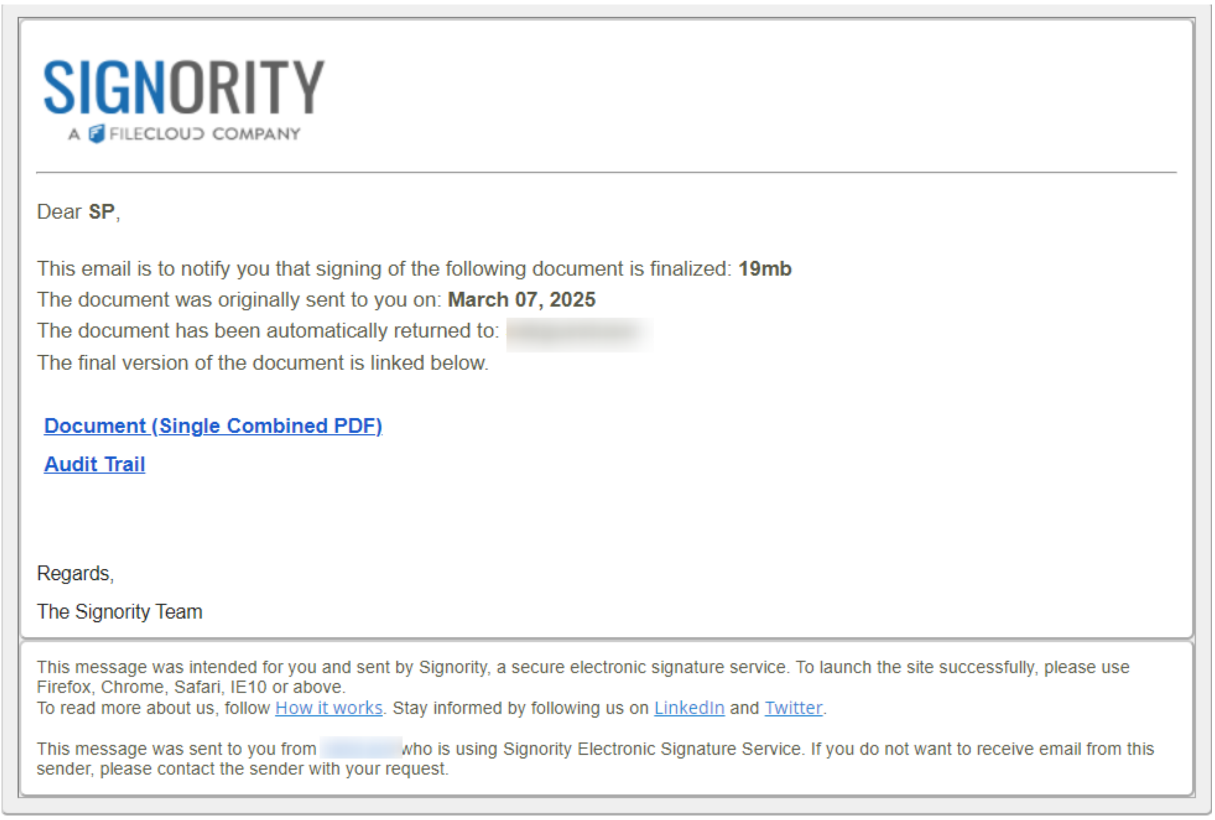
The options for receiving audit details are the following:

- No audit details (default)
- A separate audit file is sent to the destination with the eSignature document.
- Audit details are attached to the eSignature document.

To receive audit details either as a separate file or attached to the eSignature document, please Contact FileCloud Support.

When the files are accessed from the Email notifying the requestor that the file has been signed:

By default, in the email notifying a signature requestor that an eSignature document has been signed, a link to the signed document is included. By default it includes separate links to the signed file and the audit details file.



SIGNORITY
A FILECLOUD COMPANY

Dear **SP**,

This email is to notify you that signing of the following document is finalized: **19mb**
The document was originally sent to you on: **March 07, 2025**
The document has been automatically returned to: [redacted]
The final version of the document is linked below.

Document (Single Combined PDF)
Audit Trail

Regards,
The Signority Team

This message was intended for you and sent by Signority, a secure electronic signature service. To launch the site successfully, please use Firefox, Chrome, Safari, IE10 or above.
To read more about us, follow How it works. Stay informed by following us on LinkedIn and Twitter.

This message was sent to you from [redacted] who is using Signority Electronic Signature Service. If you do not want to receive email from this sender, please contact the sender with your request.

However, since this email is sent from Signority, you can log in to Signority to configure whether or not the audit trail is sent as well as whether multiple signed documents are combined into a single PDF.

To specify what is included in the email notifying the requestor that the document has been signed:

1. Log in to Signority.
2. In the Signority navigation panel, click **Admin**, and then click **Settings > Global Settings**.
3. In **Global Settings**, locate **Notifications** settings and configure options for the requestor notification email.