



FileCloud Online Version 23.232

Third Party Integration Settings

Copyright Notice

©2024 CodeLathe Technologies, Inc. dba FileCloud

All rights reserved.

No reproduction without written permission.

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.

FileCloud

Phone: U.S: +1 (888) 571-6480

Fax: +1 (866) 824-9584

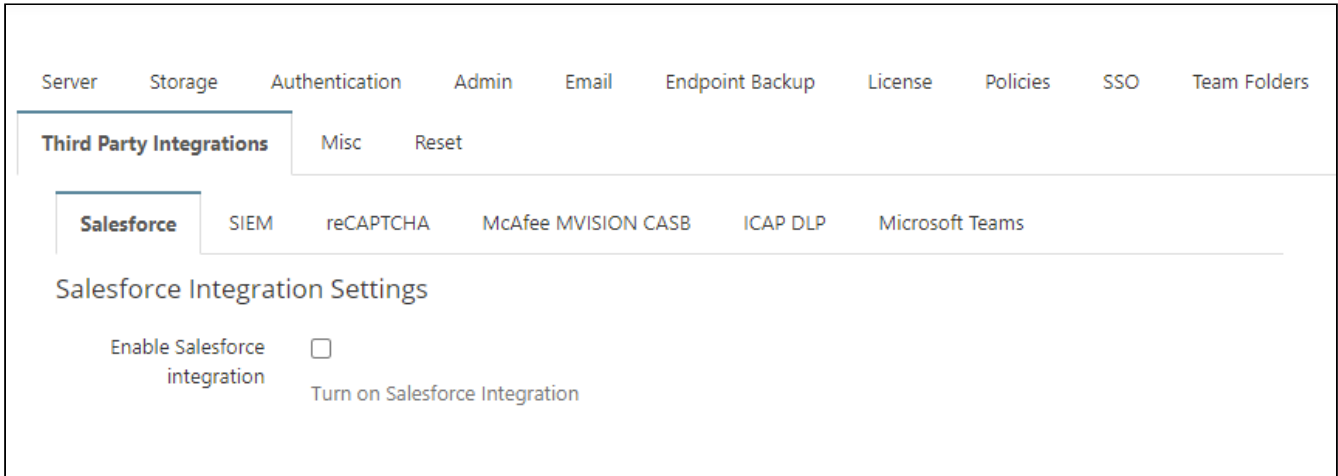
Email: support@filecloud.com

Table of Contents

Copyright Notice	2
Third Party Integrations.....	4
Integrating FileCloud with Salesforce.....	5
Adding FileCloud to Salesforce	6
Configuring FileCloud with Salesforce.....	17
SIEM Integration.....	21
FileCloud SIEM Configuration.....	22
Managing SIEM Mappings	24
SIEM Integration with Splunk Enterprise.....	40
reCaptcha Settings.....	47
To configure reCaptcha:	47
CASB integration	48
McAfee CASB integration	49
ICAP DLP	51
What is ICAP?	51
Integrating ICAP DLP with FileCloud	51
Microsoft Teams.....	54
For MS Teams Admins: Configuring FileCloud in Teams.....	54
For FileCloud Admins: Enabling Integration with MS Teams.....	69
Setting Up AutoCAD File Preview with Autodesk Viewer	71
Setting up integration of FileCloud and Autodesk Viewer	71
AI Integration.....	77

Third Party Integrations

The **Third Party Integrations** tab enables you to integrate external tools such as ClamAV, ICAP and reCaptcha with FileCloud. If you are using the Enterprise 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](#)
- [SIEM Integration](#)
- [reCaptcha Settings](#)
- [CASB integration](#)
- [ICAP DLP](#)
- [Microsoft Teams](#)
- [Setting Up AutoCAD File Preview with Autodesk Viewer](#)
- [AI Integration](#)

Integrating FileCloud with Salesforce

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.

FileCloud CCP Accounts Cases Contacts Leads Opportunities Chatter Configure FileCloud

Account
Specialty Coating Systems

Phone Billing Address Website Account Owner

Related Details **FileCloud**

Home > teamfold123 > Salesforce > Account > **Specialty Coating Systems-001DT000018Nul8YAC**

Specialty Coating Systems-001DT000018Nul8YAC

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

Upload Files Or drop files

Search File

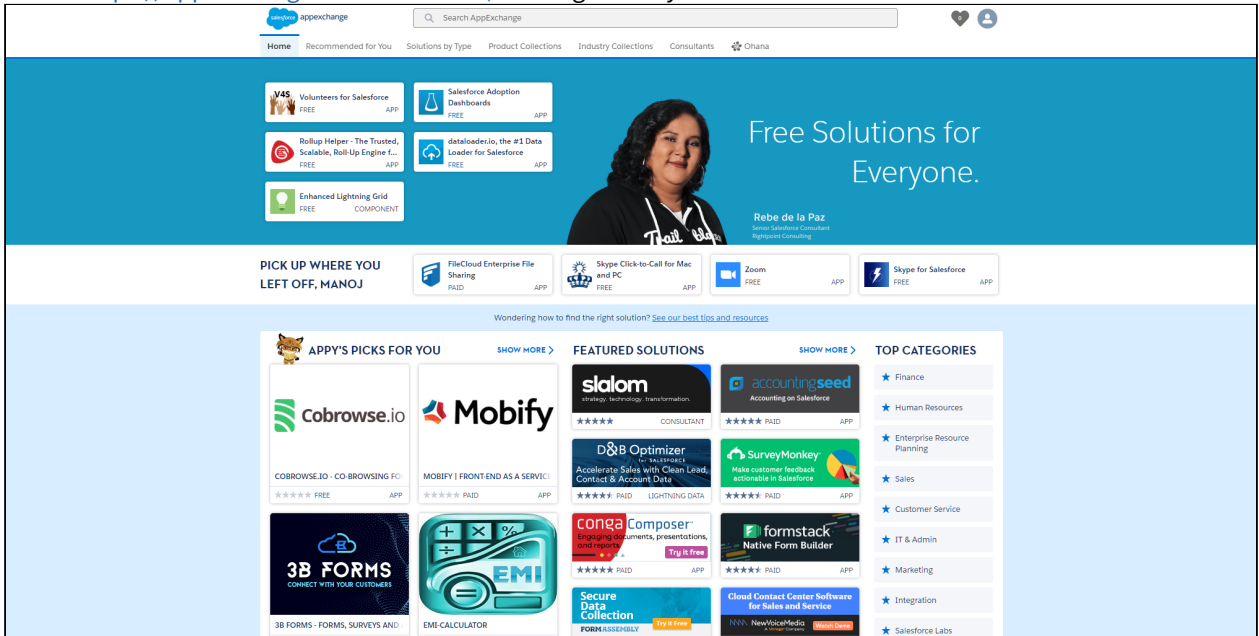
Name	Type	Size	Modify D...	Download
New Folder	Folder		Nov 29, 2...	
0bfile.txt	txt	1 B	Nov 29, 2...	

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.

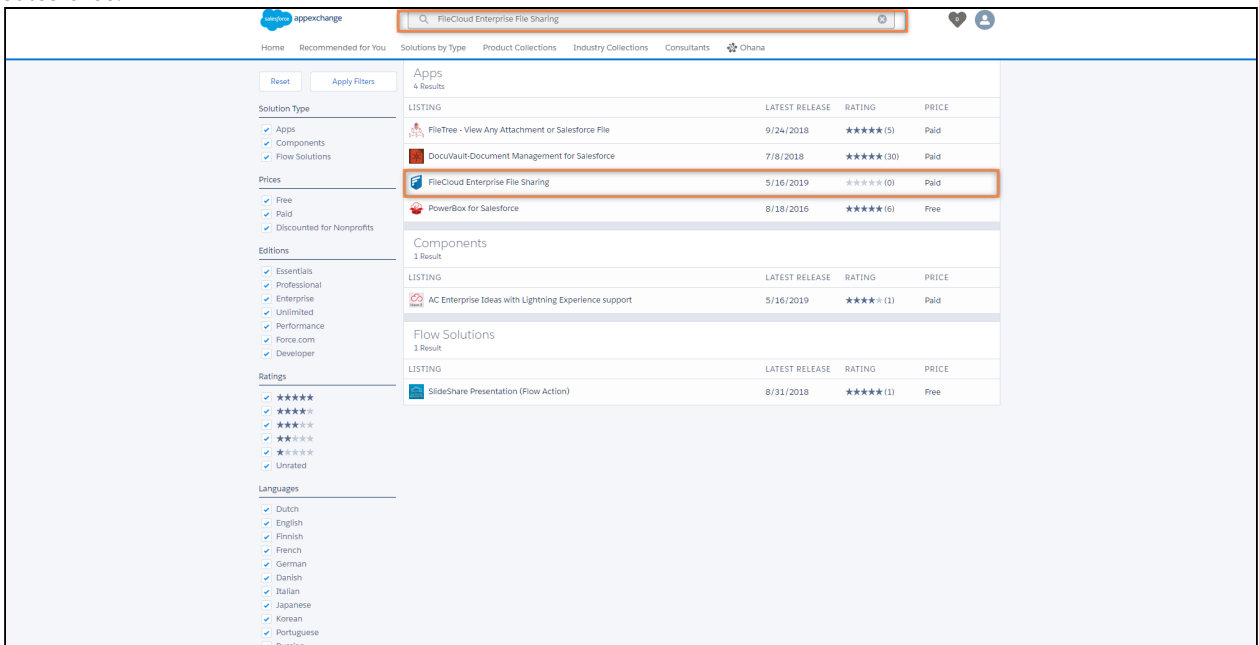
Adding FileCloud to Salesforce

To integrate FileCloud with Salesforce:

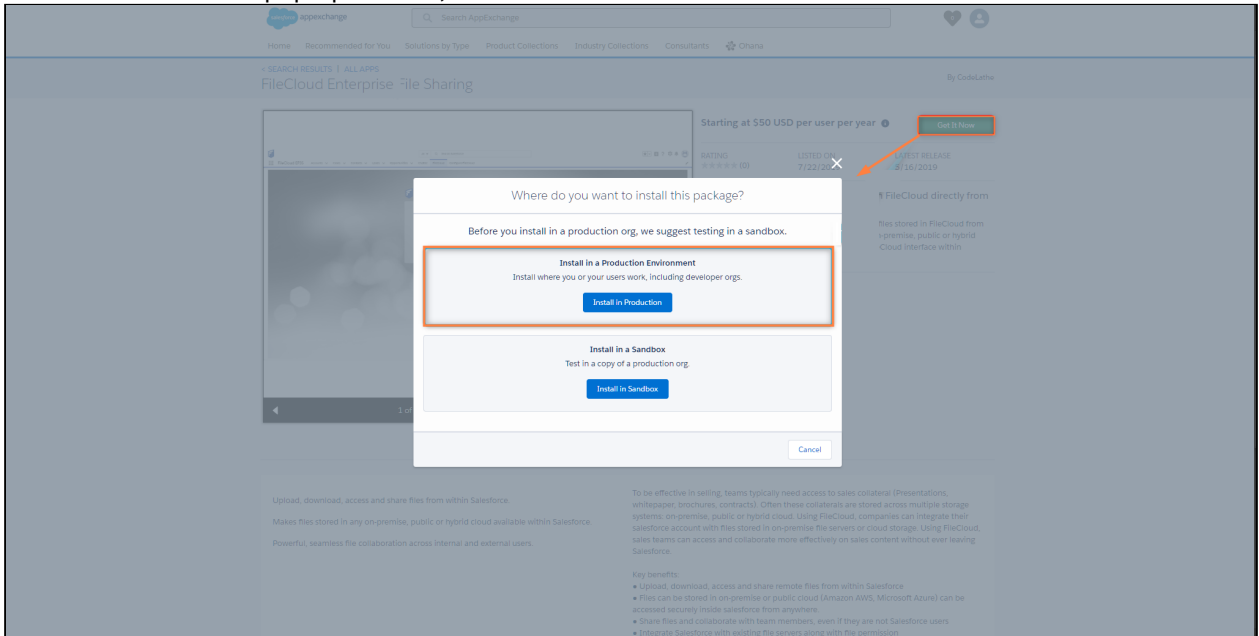
1. Access <https://appexchange.salesforce.com/> and login with your Salesforce credentials



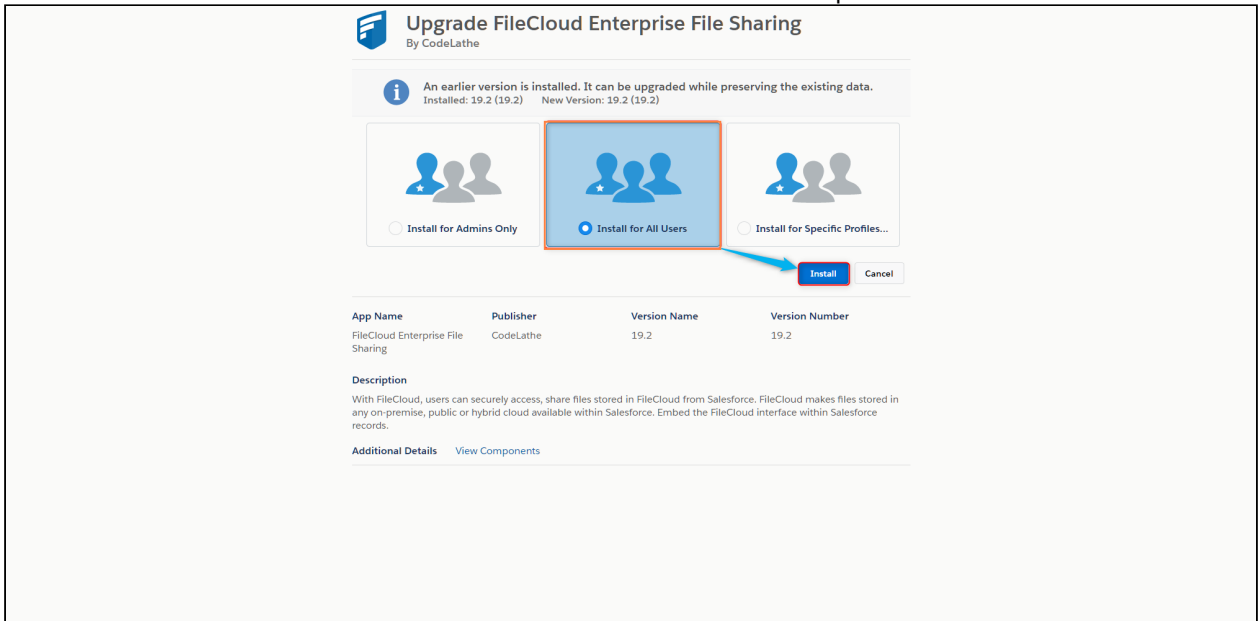
2. In the Search bar, enter **FileCloud Enterprise File Sharing**, and click the listing to enter our FileCloud App for Salesforce.



3. Click **Get it Now**. In the pop-up window, select **Install in Production**.



4. Select **Install for All Users** and click **Install**. Wait for the installation to complete.





Upgrade FileCloud Enterprise File Sharing

By CodeLathe

 **Installation Completed!**

App Name	Publisher	Version Name	Version Number
FileCloud Enterprise File Sharing	CodeLathe	19.2	19.2

Description

With FileCloud, users can securely access, share files stored in FileCloud from Salesforce. FileCloud makes files stored in any on-premise, public or hybrid cloud available within Salesforce. Embed the FileCloud interface within Salesforce records.

FileCloud EFSS appears under **Installed Packages**.

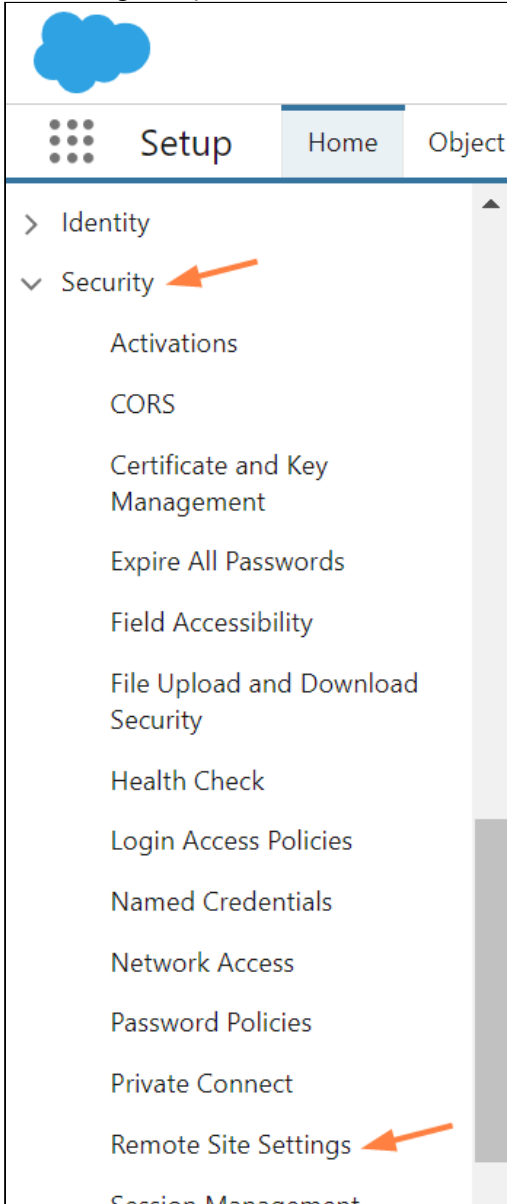
The screenshot shows the Salesforce Setup interface. The left sidebar contains navigation options like Setup Home, Lightning Experience Transition Assistant, and various administration and platform tools. The main content area is titled "Installed Packages" and includes a table of installed packages. The "FileCloud EFSS" package is highlighted with an orange border. Below the table, there is a section for "Uninstalled Packages" which is currently empty.

Action	Package Name	Publisher	Version Number	Namespace Prefix	Status	Allow
Uninstall	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]
Uninstall	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]
Uninstall	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]
Uninstall	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]
Uninstall	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]
Uninstall	FileCloud EFSS	CodeLathe	19.2	FileCloud	Free	N/A
Uninstall	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]	[Blurred]

5. In the upper-right of the screen, click the **Setup** icon, and choose **Setup**.

The screenshot shows the top right corner of the Salesforce interface. A gear icon (Setup) is highlighted with an orange arrow. A dropdown menu is open, showing options: Setup, Your Account, Developer Console, and Edit Page. The "Setup" option is also highlighted with an orange arrow.

6. In the navigation panel, scroll down to **Security** and expand it. Click **Remote Site Settings**.



The **Remote Site Settings** screen opens to the **All Remote Sites** view.

7. Click **New Remote Site**.

The screenshot shows the Salesforce Setup interface. At the top, it says 'Sandbox: newSandbox | Log out'. Below that is a search bar labeled 'Search Setup'. The navigation menu on the left includes 'Setup', 'Home', and 'Object Manager'. Under 'Setup', there are sections for 'Identity' and 'Security'. The 'Security' section is expanded, showing options like 'Activations', 'CORS', 'Certificate and Key Management', 'Expire All Passwords', 'Field Accessibility', 'File Upload and Download Security', 'Health Check', 'Login Access Policies', 'Named Credentials', 'Network Access', and 'Password Policies'. The main content area is titled 'Remote Site Settings' and 'All Remote Sites'. It includes a 'View: All Remote Sites' dropdown and a 'Create New View' link. Below that is a navigation bar with letters A through Z and 'Other' and 'All'. A red arrow points to a 'New Remote Site' button. Below the button is a table with columns: 'Action', 'Remote Site Name', 'Namespace Prefix', 'Remote Site URL', 'Active', 'Created By', and 'Created Date'. The table is currently empty. At the bottom of the page, there is a Windows taskbar with various application icons.

8. Add the FileCloud **Remote Site Name** and **Remote Site URL**, and click **Save**.

The screenshot displays the Salesforce Setup interface. At the top, it shows 'Sandbox: newSandbox | Log out' and a search bar labeled 'Search Setup'. The left sidebar contains a navigation menu with 'Setup' selected, and a sub-menu where 'Remote Site Settings' is highlighted. The main content area is titled 'Remote Site Settings' and 'Remote Site Edit'. It includes a 'Help for this Page' link and a warning: 'Enter the URL for the remote site. All s-controls, JavaScript OnClick commands in custom buttons, Apex, and AJAX proxy calls can access this Web address from salesforce.com.' The form fields are: 'Remote Site Name' (FileCloud), 'Remote Site URL' (https://my-filecloud-url.com), 'Disable Protocol Security' (unchecked), 'Description' (empty text area), and 'Active' (checked). At the bottom, there are 'Save', 'Save & New', and 'Cancel' buttons.

The remote FileCloud site is listed in the **All Remote Sites** view.

Remote Site Settings

All Remote Sites

Below is the list of Web addresses that your organization can invoke from salesforce.com. To add another Web a

View: [Create New View](#)

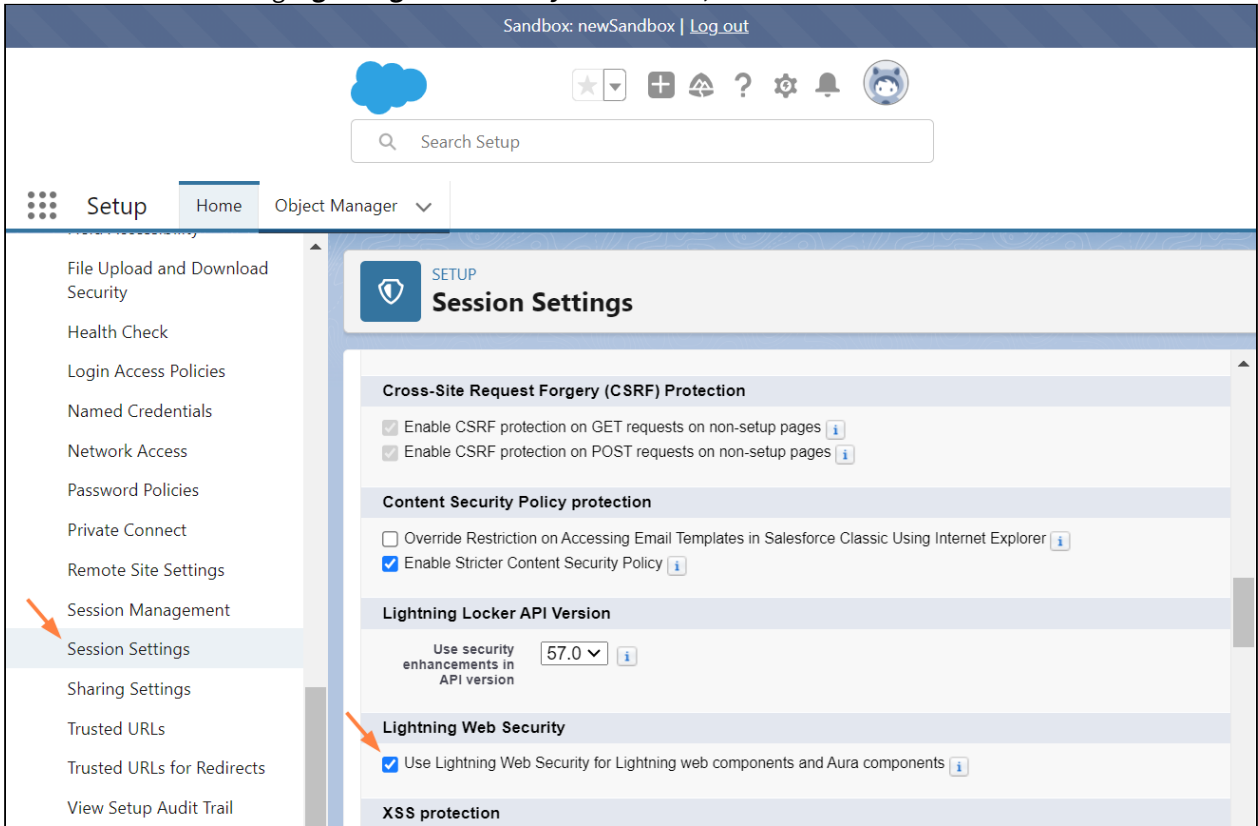
A | B | C |

Action	Remote Site Name ↑	Namespace Prefix	Remote Site URL
Edit Del	[Redacted]	[Redacted]	[Redacted]
Edit Del	FileCloud	-	https://my-filecloud-url.com
Edit Del	[Redacted]	[Redacted]	[Redacted]

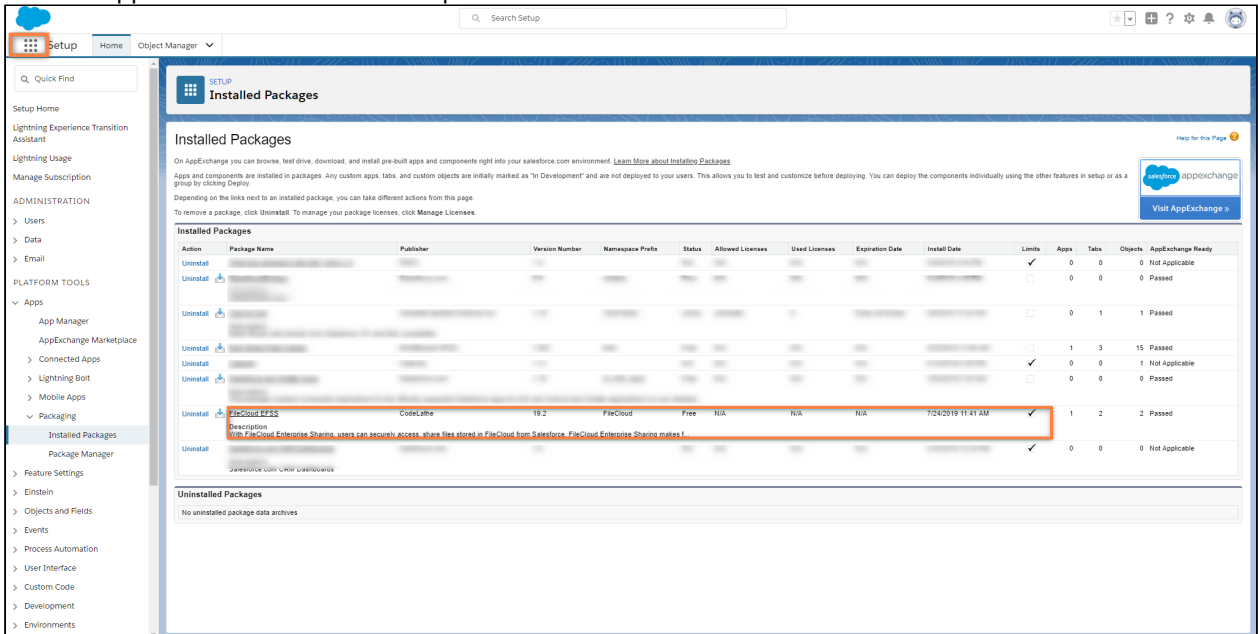
[New Remote Site](#)

- In the navigation panel, go to **Security > Session Settings**.

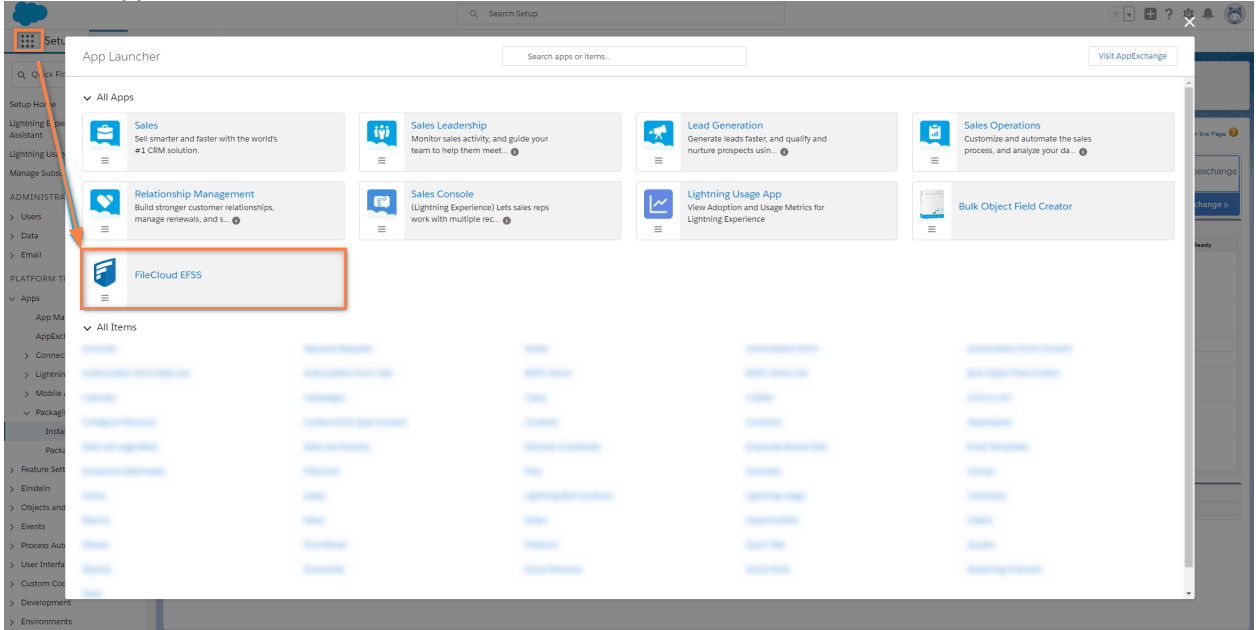
10. Scroll down to the setting **Lightning Web Security** and check it, and click **Save** at the bottom of the screen.



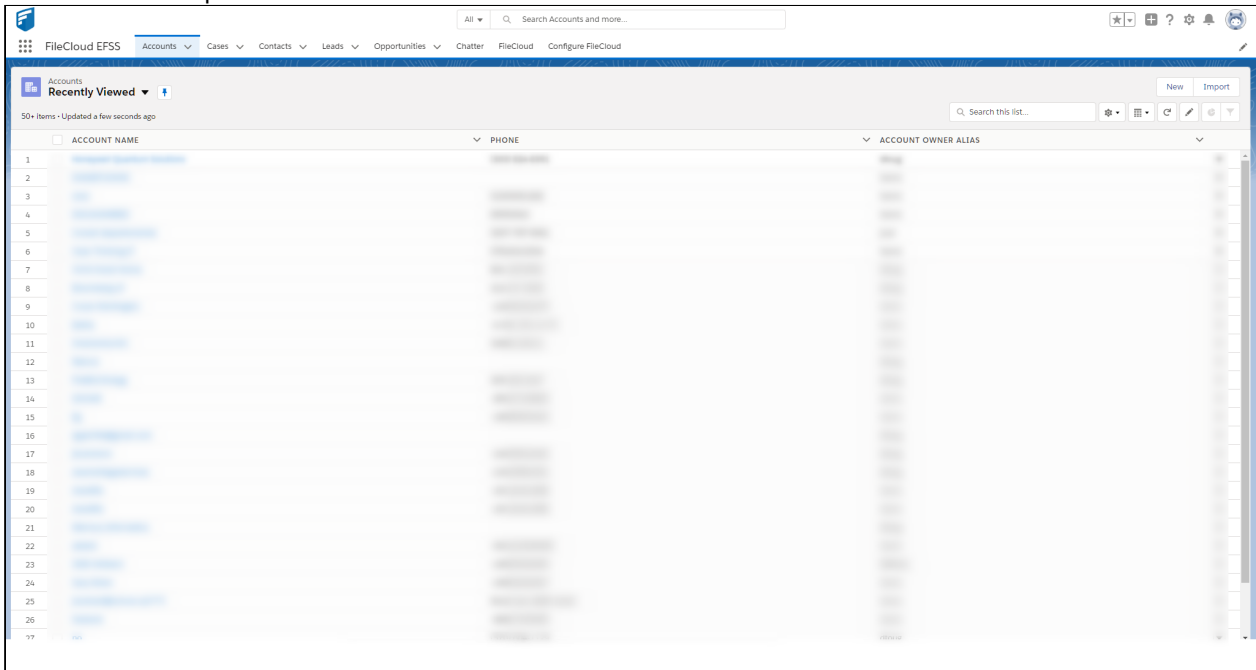
11. Click the App Launcher located in the top-left corner of the screen.



12. From the App Launcher, click FileCloud EFSS.



Installation is complete.



Configuring FileCloud with Salesforce

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

1. First [Contact FileCloud Support](#) to enable integration with Salesforce in your FileCloud configuration.
2. Configure Salesforce in FileCloud.
 - a. In FileCloud's Admin portal, go to **Settings > Third Party Integrations > Salesforce**.
 - b. Check **Enable Salesforce Integration**.
 - c. Click **Generate Secret**, then copy the key and click **Save**.
 - d. In FileCloud Team Folders, create a Team Folder named **Salesforce**. Sub-folders for your Salesforce objects will automatically be created in this Team Folder. (You may give the folder another name, but make sure you change the folder name entered in **Salesforce Team Folder Name** to match it.)

The screenshot shows the FileCloud interface for configuring Salesforce integration. The navigation menu includes Server, Storage, Authentication, Admin, Email, Endpoint Backup, License, and Third Party Integrations. Under Third Party Integrations, the Salesforce section is active, with sub-options for SIEM, reCAPTCHA, McAfee MVISION CASB, ICAP DLP, and Microsoft Telemetry. The Salesforce Team Folder Name is set to 'Salesforce'.

Salesforce Integration Settings

Enable Salesforce integration

Turn on Salesforce Integration

Client Secret

.....

Salesforce Client Secret, which has to be provided in the Salesforce client app to allow authentication

Generate Secret

Supported Salesforce object types

account,lead,contact,opportunity,case

Specifies which Salesforce Object types will be automatically handled in FileCloud [Comma separated list of object types]

Salesforce Team Folder Name

Salesforce

Name of the main directory under which all files/folders related to Salesforce objects will be stored

3. 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 **Admin approved users are pre-authorized**

Enable Single Logout

Session Policies

Timeout Value --None--

Custom Connected App Handler

Apex Plugin Class

Run As

User Provisioning Settings

Enable User Provisioning

Save Cancel

- d. Click **Save**.

4. 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 EFSS Accounts Cases Contacts Leads Opportunities Chatter FileCloud **Configure FileCloud**

FileCloud Settings

Edit FileCloud Settings Save Cancel

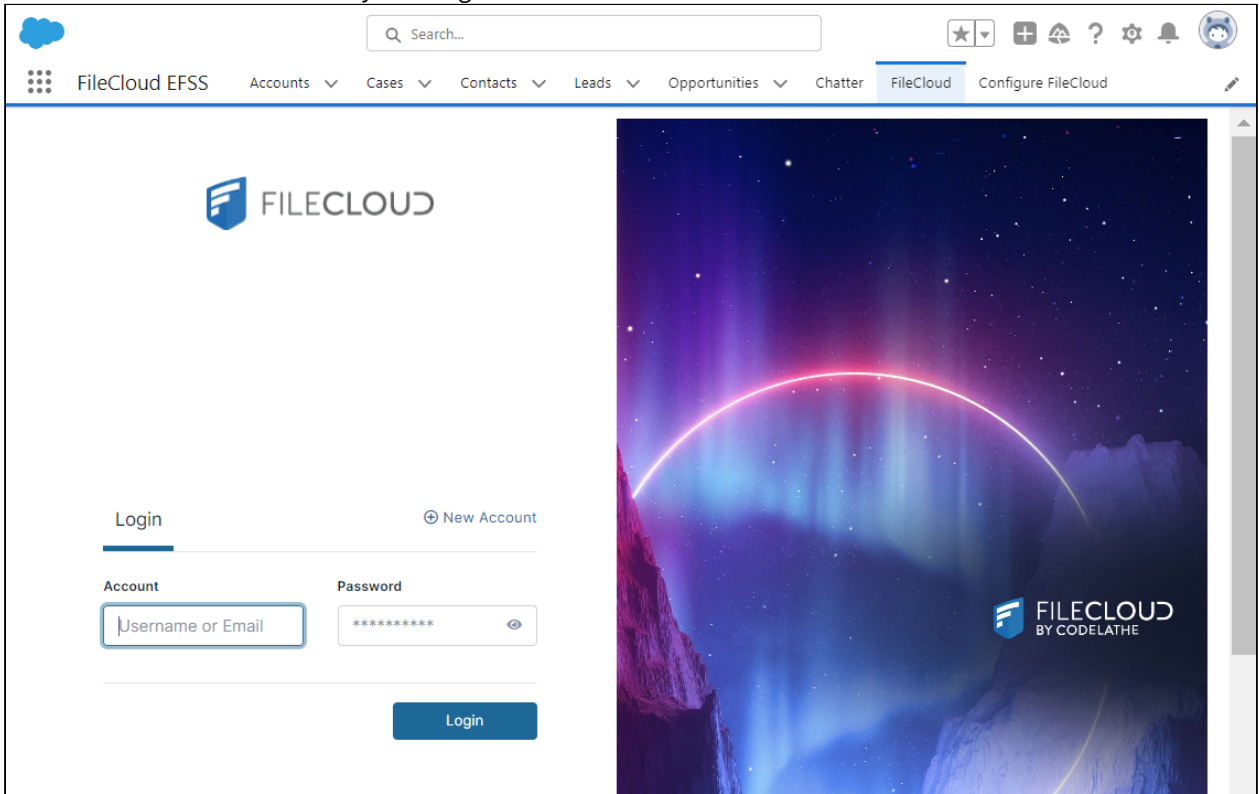
Connection Settings

Domain

Client Secret

Save Cancel

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



SIEM Integration

SIEM Integration

SIEM Integration is available from FileCloud 19.2

In the field of computer security, security information and event management (**SIEM**), software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Since version 19.2, FileCloud has allowed system administrators to integrate FileCloud's system alerts and auditing with external SIEM systems, enabling them to monitor all alerts and potential security issues in one place.

FileCloud SIEM Configuration

SIEM Integration Settings

Enable SIEM integration Turn on SIEM Integration

SIEM Integration Method: Select SIEM Integration Method

SIEM Server Host: Specify the SIEM Server Host

SIEM Server Port: SIEM Server Port

SIEM Message Format: Select Message Format

Enable Audit Trail Enable Audit Trail - if turned off Audit entries will be completely ignored

Enable System Alert Trail Enable System Alert Trail - if turned off System Alerts will be completely ignored

To configure SIEM Integration Settings

1. Open a browser and log into *Admin Portal*.
2. In the left navigation panel, under *SETTINGS*, select *Settings*.
3. On the *Manage Settings* screen, select the *Third Party Integrations* tab.
4. Select the *SIEM* tab.
5. Modify settings as needed.
6. Click *Save*.

If you select **LEEF** in the drop-down list for **SIEM Message Format**, the fields **LEEF Version** and **LEEF Message Delimiter** also appear:

SIEM Message Format: Select Message Format

LEEF Version: Select LEEF format version

LEEF Message Delimiter: Select LEEF message delimiter

The following options are available:

Option	Description
Enable SIEM Integration	Turns SIEM integration ON or OFF

Option	Description
SIEM Integration method	<p>Specifies the SIEM Integration method. Following options are available:</p> <ul style="list-style-type: none"> ▪ 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 <p>Note: SIEM software providers should specify supported integration methods in the SIEM documentation.</p>
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	<p>Specifies the SIEM Message format. The following formats are available:</p> <ul style="list-style-type: none"> ▪ CEF - Common Event Format ▪ LEEF - Log Event Extended Format <p>NOTE: SIEM software provider should specify supported formats in the SIEM documentation.</p>
LEEF Version (LEEF Format only)	<p>Specifies the version of the LEEF format message. Available versions:</p> <ul style="list-style-type: none"> ▪ 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)	<p>Tests connection to the server specified by the Host and Port.</p> <p>NOTE: All settings have to be saved first. Connection tests are based on the currently saved settings.</p>

Option	Description
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.

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 (later than Ubuntu 14.04)	Linux (earlier than Ubuntu 14.04)
c:\xampp\htdocs	/var/www/html	/var/www

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

Property	Description	Values
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	<p>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.</p> <p>The request can be mapped as a full object, and its info will be sent to the SIEM server as a string. For example: <code>`request' => '\$request'`</code>, will be sent as <code>`{"op":"logginguest","userid":"john.doe","password":"xxx"}`</code></p> <p>Each field can also be sent individually if provided in the mapping: <code>`loggedUser' => '\$request.userid'`</code>, where <code>`userid'`</code> is one of the parameters of the request.</p>
response	Response payload	<p>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.</p> <p>Each operation has a different response, so it is better to use this for dedicated rules.</p> <p>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),</p> <p>This is not recommended for production as it may affect performance and usually is not needed for auditing.</p>
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.

Property	Description	Values
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)
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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> upload (file upload operation) downloadfile

Property	Description	Values	Supported operations
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
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: <ul style="list-style-type: none"> ▪ 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' => [
      'user' => '$userName',
      'host' => '$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' => [
            'user' => '$userName',
            'host' => '$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
$mappings[] = [
    'id' => 'loginquest',
    'prefilter' => [
        //List of conditions that audit entry has to met in order to be processed (or
        //filtered out if excluded option is there)
        'resultCode' => '0', //incidents only
        'exclude' => false // optional 'include' is used by default
    ],
    'map' => [
        'eventClass' => 'login',
        'eventName' => 'Invalid login attempt',
        'severity' => 2,
        'extension' => [
            'user' => '$userName',
            'ip' => '$ip',
            'host' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
        ]
    ]
];

```

```

    ]
];

//Failed SSO login attempt
$mappings[] = [
    'id' => 'samlss0',
    'prefilter' => [
        //List of conditions that audit entry has to met in order to be processed (or
        filtered out if excluded option is there)
        'resultCode' => '0', //incidents only
        'exclude' => false // optional 'include' is used by default
    ],
    'map' => [
        'eventClass' => 'login',
        'eventName' => 'Invalid SSO login attempt',
        'severity' => 2,
        'extension' => [
            'user' => '$userName',
            'ip' => '$ip',
            'shost' => '$hostname', // name of the host
            'recordId' => '$recordId', // Audit record id
        ]
    ]
];

//Successful SSO login attempt
$mappings[] = [
    'id' => 'samlss0',
    'prefilter' => [
        //List of conditions that audit entry has to met in order to be processed (or
        filtered out if excluded option is there)
        'resultCode' => '1',
        'exclude' => false // optional 'include' is used by default
    ],
    'map' => [
        'eventClass' => 'login',
        'eventName' => 'Successfull SSO login attempt',
        'severity' => 2,
        'extension' => [
            'user' => '$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

Property	Description	Values
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_ERROR 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	
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.

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 Domain 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.

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](#)

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](#)

Source Type

Source Type Category

Source Type Description

App Context

Method ?

Select New

FileCloud

Custom ▾

FileCloud Audit Logs

Apps Browser (appsbrowser) ▾

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. Log in to the FileCloud admin portal, and go to **Settings > Third Party Integrations > SIEM**.
2. Check **Enable SIEM integration**, and in **SIEM Integration Method**, choose **TCP Receiver**.
3. 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](#).

SIEM Integration Settings

Enable SIEM integration Turn on SIEM Integration

SIEM Integration Method Select SIEM Integration Method

SIEM Server Host Specify the SIEM Server Host

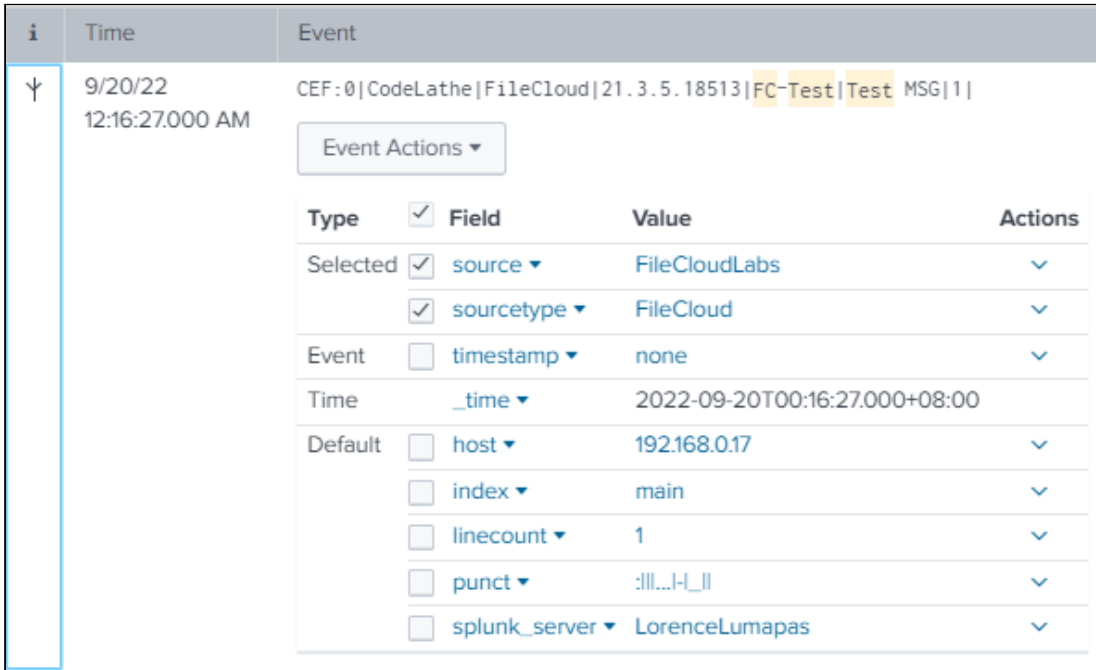
SIEM Server Port SIEM Server Port

SIEM Message Format Select Message Format

Enable Audit Trail Enable Audit Trail - if turned off Audit entries will be completely ignored

Enable System Alert Trail Enable System Alert Trail - if turned off System Alerts will be completely ignored

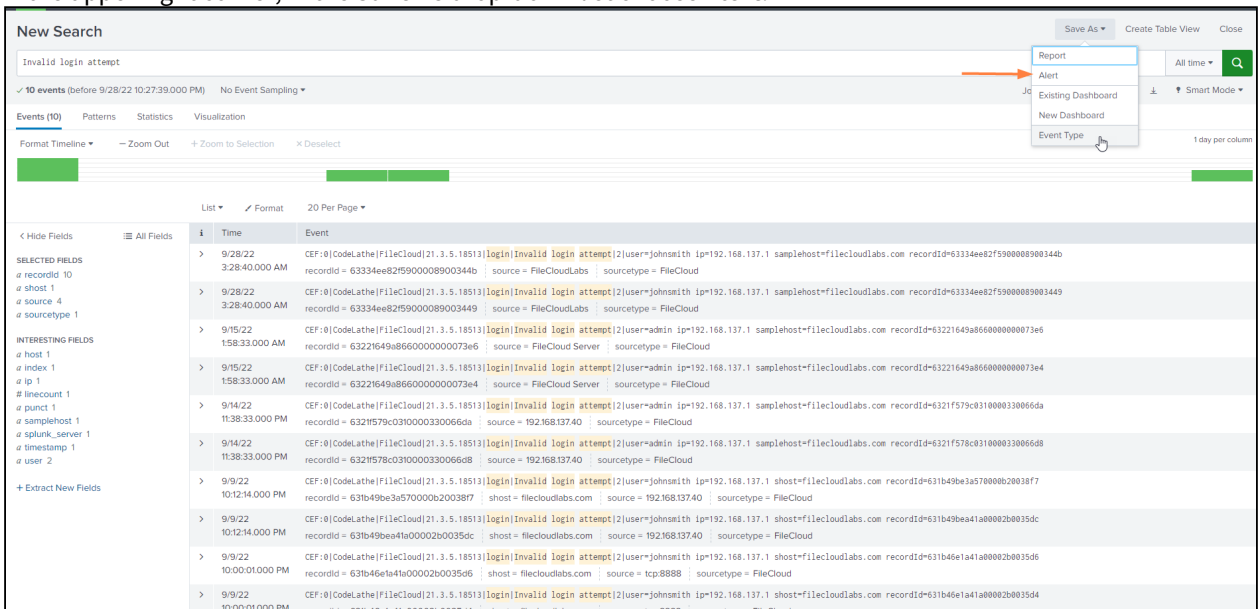
4. Validate your configuration by clicking the **Test Connection**, **Send Test Message**, and **Validate Mappings** buttons. The **Send Test Message** button should send a test connection to the Splunk server, for example:



NOTE: Additional fields can be added by modifying the mappings from the **auditmap.php** and **systemalertsmap.php** files in FileCloud. See [Managing SIEM Mappings](#) 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**:



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

Description

Permissions Private Shared in App

Alert type Scheduled Real-time

Run every hour ▼

At minutes past the hour

Expires day(s) ▼

Trigger Conditions

Trigger alert when

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

Subject

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

Message

Include Link to Alert Link to Results
 Search String Inline

Trigger Condition Attach CSV

Trigger Time Attach PDF

Allow Empty Attachment

Type

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.



reCaptcha Settings

Starting with Version 19.3, 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. In the FileCloud admin portal, go to **Settings > Third Party Integrations > reCAPTCHA**.

The screenshot shows the FileCloud admin portal interface. On the left is a navigation sidebar with categories like GOVERNANCE, MISC., and SETTINGS. The main content area is titled 'reCAPTCHA Integration Settings' and contains the following elements:

- Navigation tabs: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup.
- Sub-sections: Third Party Integrations, Misc, Reset.
- Integration options: Salesforce, Anti-Virus, SIEM, **reCAPTCHA**, McAfee MVISION CASB, ICAP DLP.
- Section title: reCAPTCHA Integration Settings.
- Enable reCAPTCHA integration: Select to enable Captcha.
- reCAPTCHA Host Name: . Below it, a note states: "If planning to use a non-default reCAPTCHA site, enter the site hostname in the format <www.hostname.com>."
- reCAPTCHA Site Key: with an eye icon to toggle visibility. Below it, the text "Enter reCAPTCHA Site Key" is displayed.
- reCAPTCHA Secret: with an eye icon to toggle visibility. Below it, the text "Enter reCAPTCHA Secret" is displayed.

3. Check **Enable reCAPTCHA integration**.
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**.
6. Click **Save**.

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 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. In the Admin portal navigation pane, click **Settings**, and then select **Third Party Integrations > McAfee MVISION CASB**.
2. Check **Enable FileCloud CASB** Integration.
The field **FileCloud CASB API Key** appears.

The screenshot shows the FileCloud Admin portal navigation pane with the following tabs: Server, Storage, Authentication, Admin, Database, Email, Endpoint Backup, License. Under the 'Third Party Integrations' tab, there are sub-tabs: ServerLink, Misc, Reset, Salesforce, SIEM, reCAPTCHA, **McAfee MVISION CASB**, and ICAP DLP. The 'McAfee MVISION CASB' sub-tab is active, displaying the 'McAfee MVISION CASB Integration Settings' page. The page contains the following settings:

- Enable FileCloud CASB integration:** Select to enable McAfee MVISION CASB
- FileCloud CASB API Key:** Set 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](#) for instructions.

[McAfee CASB integration](#)

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 content classification engine \(CCE\)](#), 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 a browser and log in to the Admin Portal.
2. On the left navigation panel, click **Settings**.
3. Select the **Third Party Integrations** tab.
4. Select the **ICAP DLP** tab.
5. Fill in the fields according to the table below.
6. Click **Save**.

Server Storage Authentication Admin Email Endpoint Backup License Policies

Third Party Integrations Misc Reset

Salesforce SIEM reCAPTCHA McAfee MVISION CASB **ICAP DLP** Microsoft Teams

AutoCAD Viewer

Server Local IP

Specify this server's local IP (must not be 127.0.0.1)

ICAP Remote Hostname

Specify the ICAP server remote hostname

ICAP Port

Specify the ICAP server port.
Typically 1344 for regular ICAP or 11344 for secure ICAP server

Secure ICAP

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

File Size Limit

Units ▾ 25 MB

Files larger than this size will not be scanned

ICAP Service name

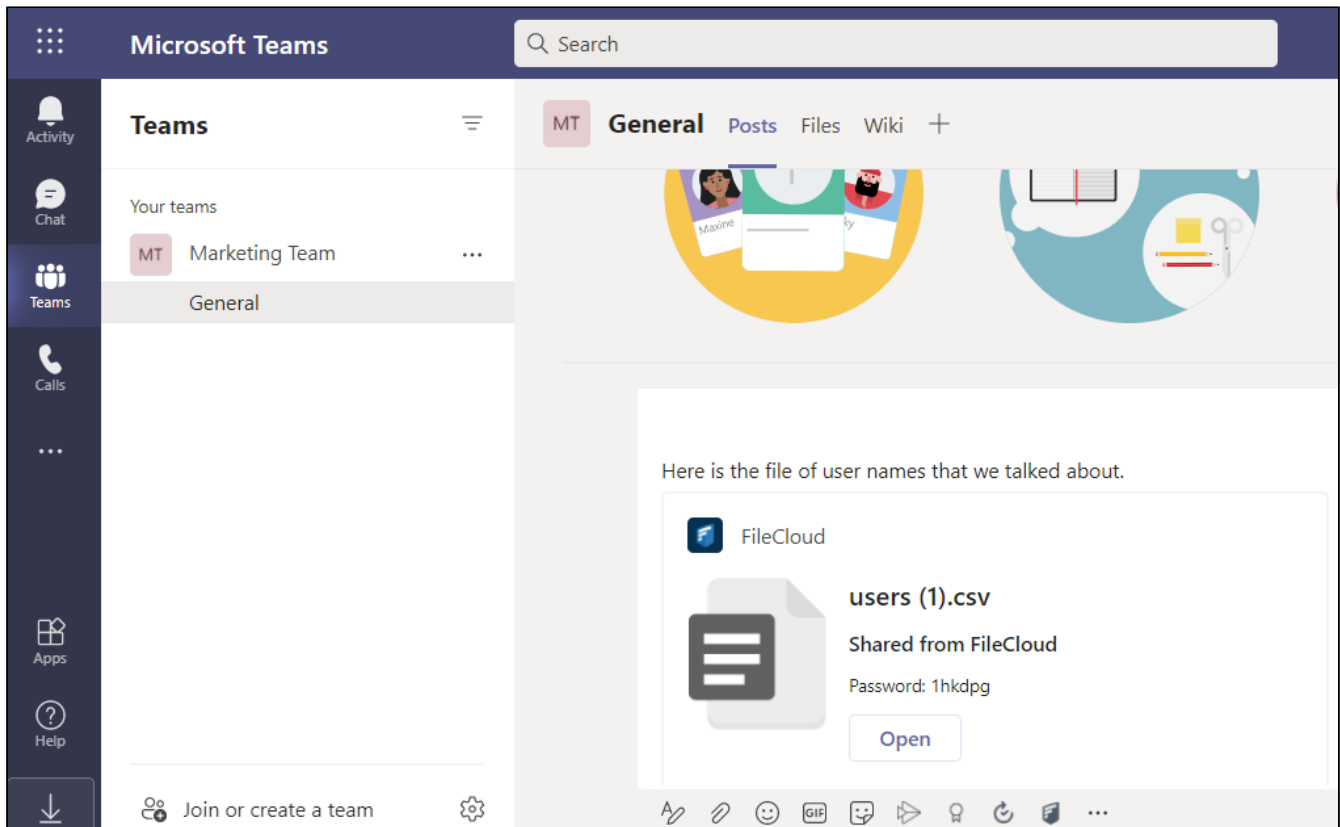
Enter the name of this ICAP Service as provided by the ICAP server

Setting	Description
Server Local IP	In most cases, leave the default value of 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.

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.



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.

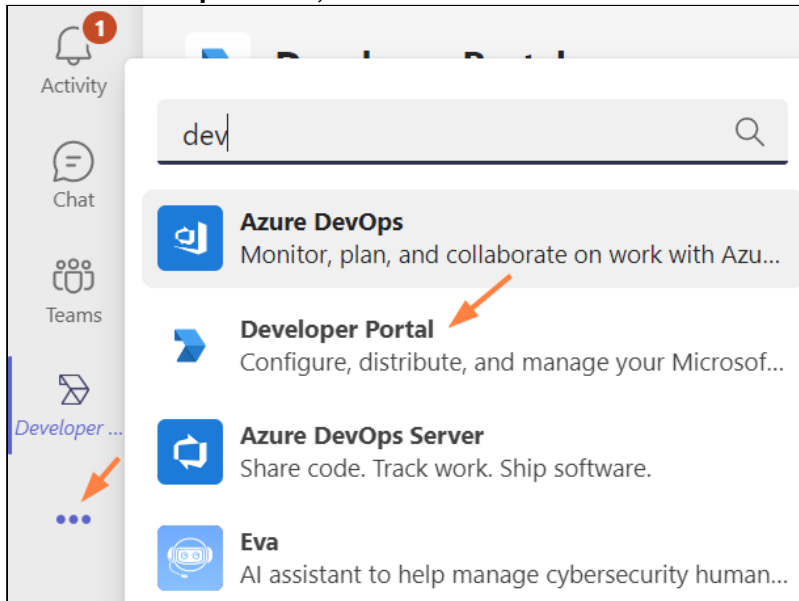
For MS Teams Admins: Configuring FileCloud in Teams

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](#) in the FileCloud Admin portal.

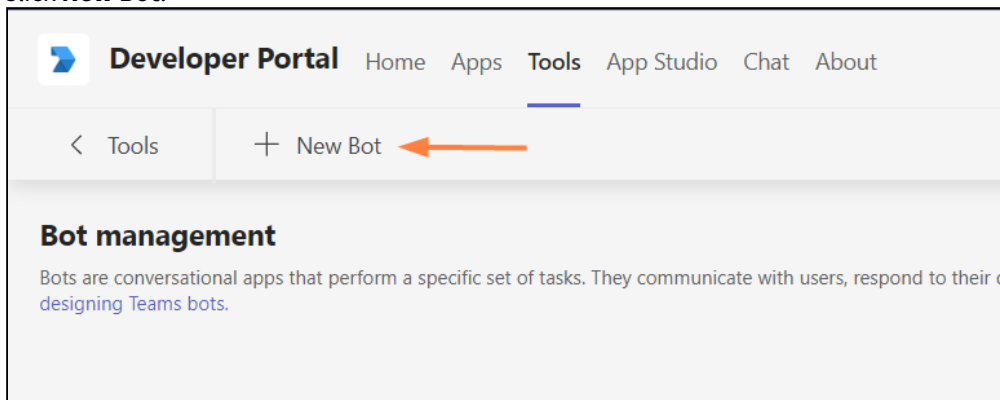
i FileCloud integration with MS Teams is available beginning in FileCloud Version 21.2

1. Confirm that you have FileCloud Version 21.2 or higher installed.
2. Create an MS Teams bot in the Teams' **Developer Portal**:

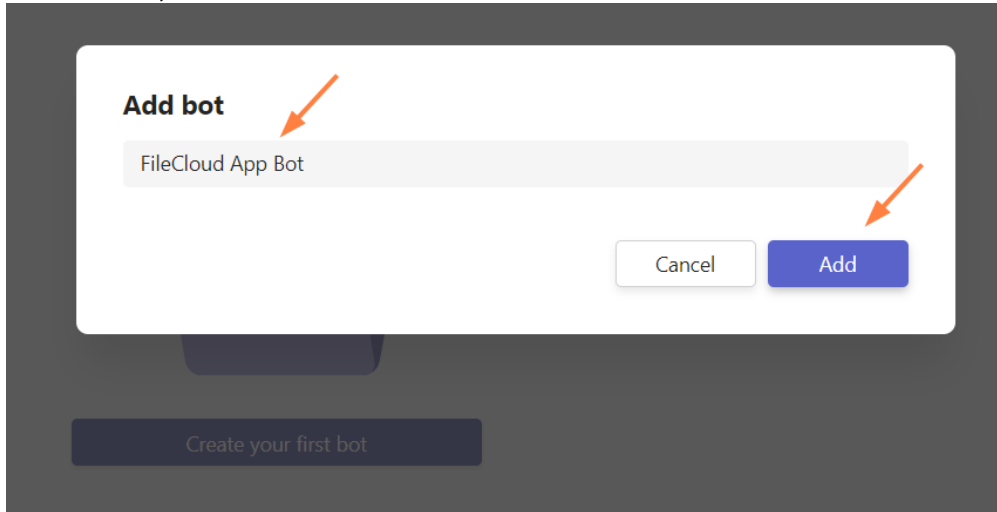
- a. Open **MS Teams**.
- b. If you do not have the **Developer Portal** app installed already, click the **More** icon in the navigation pane, search for **Developer Portal**, and add it.



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

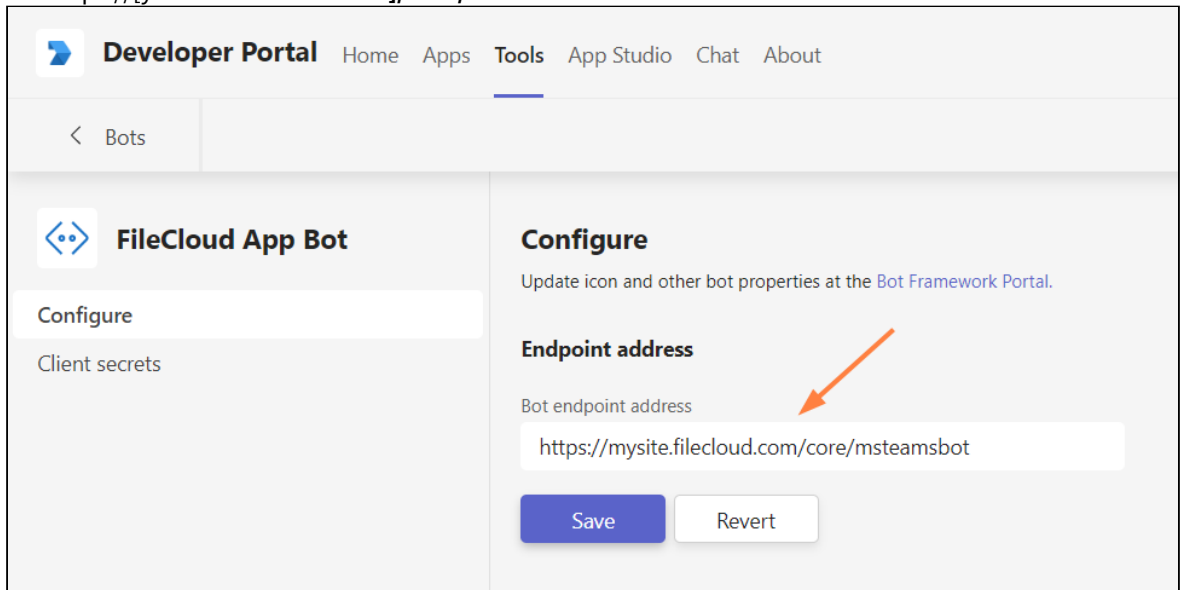


- e. Name the bot ,and click **Add**.



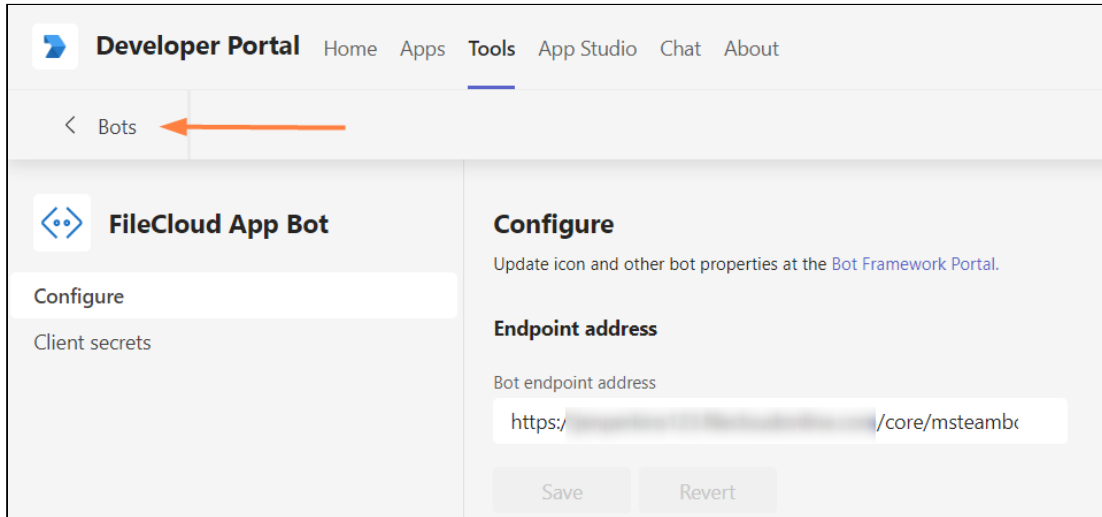
The bot appears opened on the **Tools** screen.

- f. Change the **Endpoint address** to point to the bot in your FileCloud server, and click Save. Use `https://[your FileCloud server]/core/msteamsbot`



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

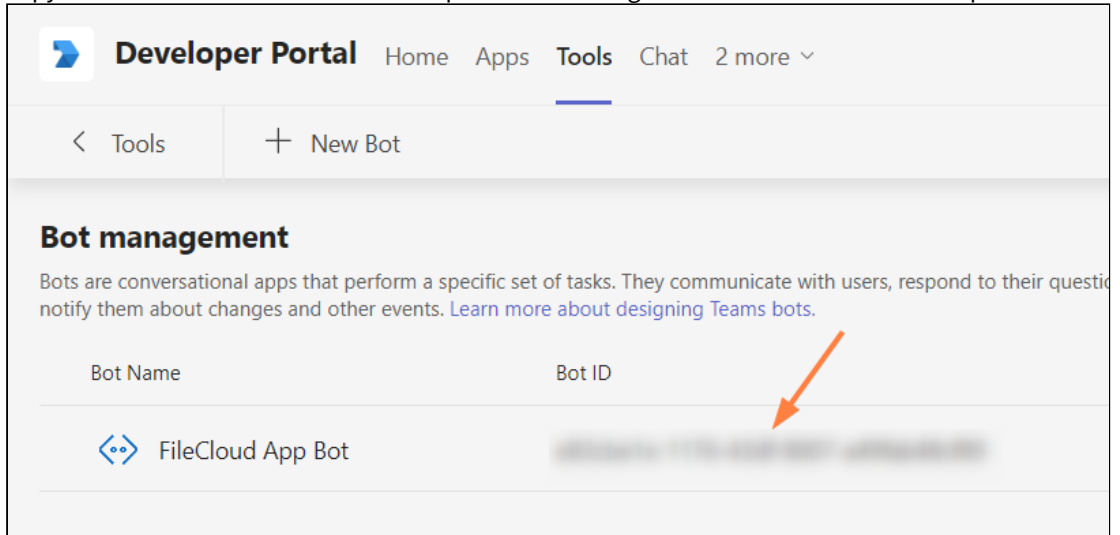
g. Click **Bots**.



The screenshot shows the 'Developer Portal' interface. The top navigation bar includes 'Home', 'Apps', 'Tools', 'App Studio', 'Chat', and 'About'. The 'Tools' tab is active. Below the navigation, there is a breadcrumb trail: '< Bots'. An orange arrow points to the 'Bots' link. The main content area is titled 'FileCloud App Bot' and has a sub-header 'Configure'. Below this, there is a 'Client secrets' section. To the right, there is a 'Configure' section with a description: 'Update icon and other bot properties at the Bot Framework Portal.' Below this is the 'Endpoint address' section, which contains a text input field with the value 'https://[redacted]/core/msteambc'. At the bottom of this section are 'Save' and 'Revert' buttons.

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

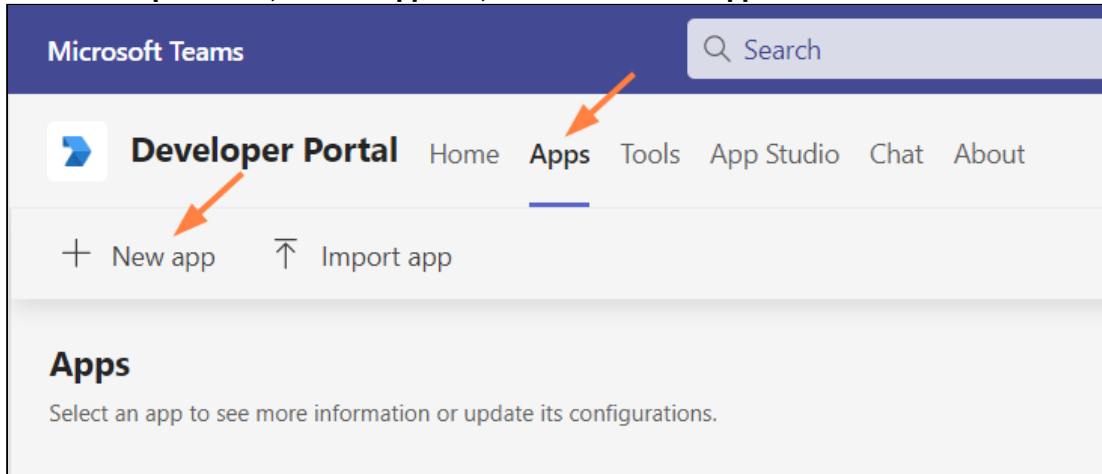
h. Copy the **Bot ID**. You will need it to set up MS Teams integration in the FileCloud admin portal.



The screenshot shows the 'Developer Portal' interface. The top navigation bar includes 'Home', 'Apps', 'Tools', 'Chat', and '2 more'. The 'Tools' tab is active. Below the navigation, there is a breadcrumb trail: '< Tools'. To the right of the breadcrumb is a '+ New Bot' button. The main content area is titled 'Bot management' and has a description: 'Bots are conversational apps that perform a specific set of tasks. They communicate with users, respond to their questions, and notify them about changes and other events. Learn more about designing Teams bots.' Below this is a table with two columns: 'Bot Name' and 'Bot ID'. The table contains one row for the 'FileCloud App Bot'. An orange arrow points to the 'Bot ID' cell, which contains a long alphanumeric string.

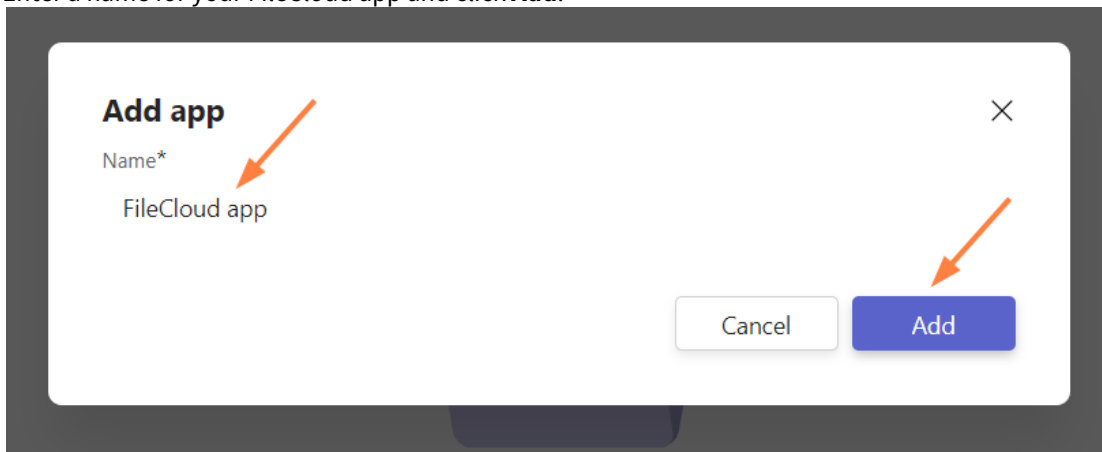
3. Create the MS Teams application in Teams' **Developer Portal**.

- 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.

The screenshot shows the 'FileCloud app' configuration page in Microsoft Teams. The left navigation pane is expanded to 'Basic information'. The main content area is titled 'Basic information' and contains the following sections:

- App names:** A short name (30 characters or less) is required. A longer version is optional. The 'Short name - 30 characters or less*' field contains 'FileCloud app'. The 'Full name - up to 100 characters (optional)' field contains '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. The field is obscured by a blurred grey box with a copy icon.
- Descriptions:** Short and long descriptions must be different. The 'Short description - 80 characters or less*' field contains 'FileCloud app for MS Teams'.

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

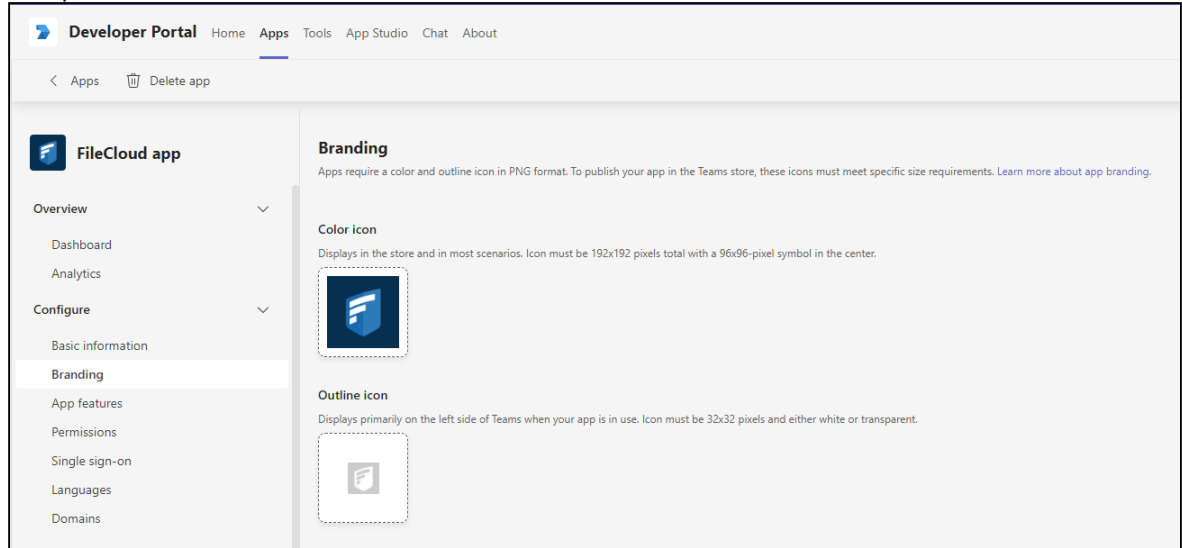
The screenshot shows the 'FileCloud app' configuration page in Microsoft Teams, now on the 'Branding' section. The left navigation pane is expanded to 'Branding'. The main content area is titled 'Branding' and contains the following sections:

- Color icon:** Displays in the store and in most scenarios. Icon must be 192x192 pixels total with a 96x96-pixel symbol in the center. A blue arrow icon is shown in a dashed box.
- 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. A grey square icon with a white symbol is shown in a dashed box.
- Accent color:** Displays for primary actions and other app UI components. A grey square is shown in a dashed box.

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

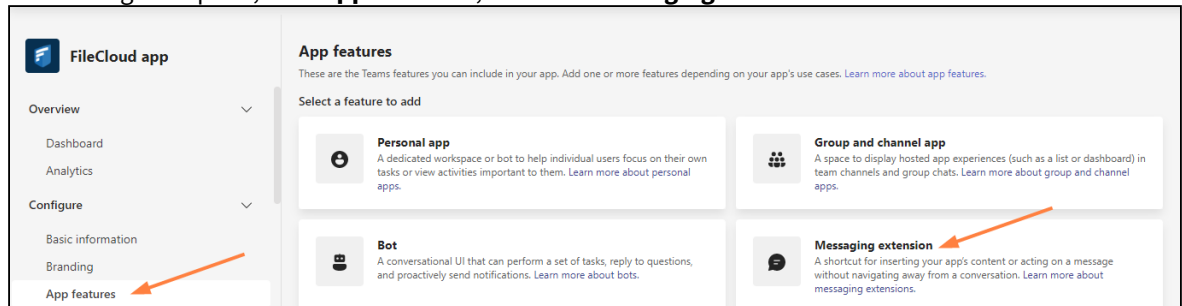


- f. Upload the first image for **Color icon**, and the second image for **Outline icon**.
You may use custom images, but they must be 192px X 192px for the color image and 32px X 32px for the transparent outline.



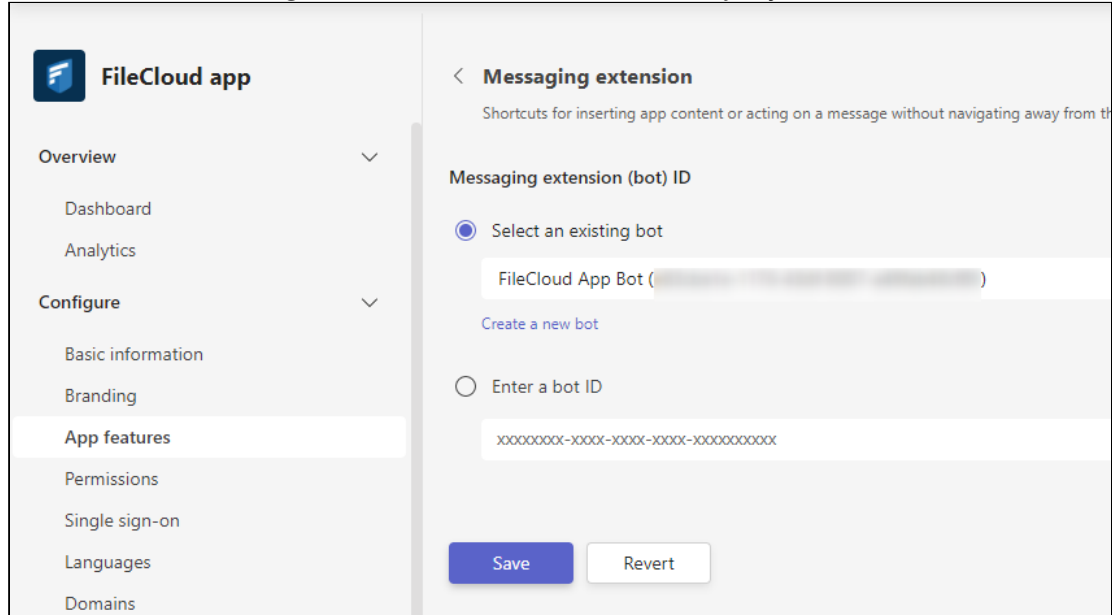
4. Set up your MS Teams bot.

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

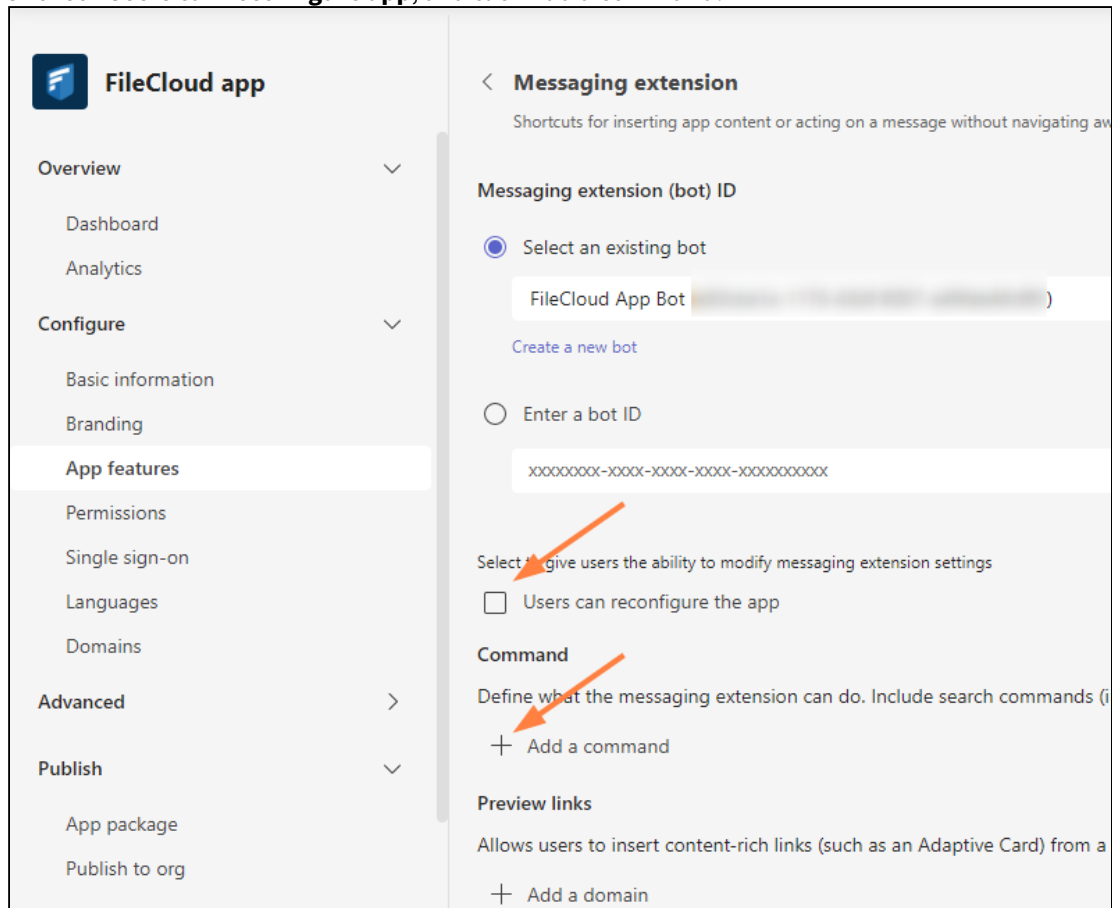


The **Messaging Extension** screen opens.

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



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



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

Cancel Save

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:// /core/msteamsbot

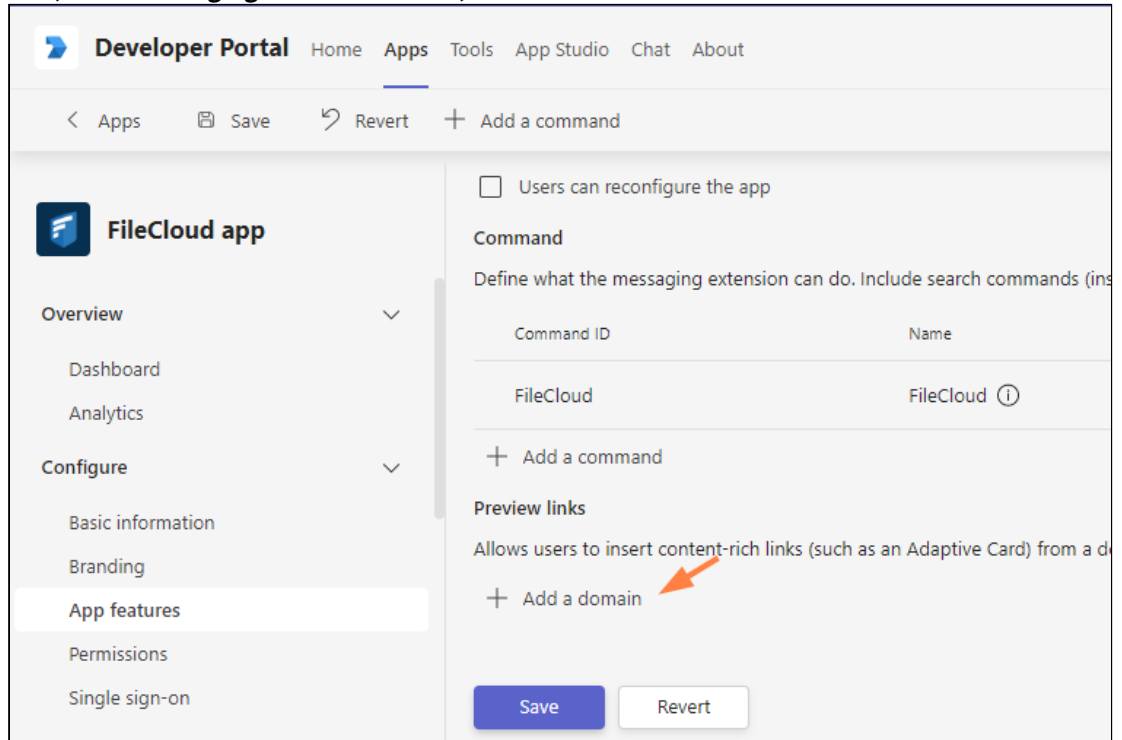
Cancel Save

- e. Click **Save**.
You are returned to the **Messaging Extension** screen.
- f. Click **Save** again, or the command will not be saved.

+ Add a domain

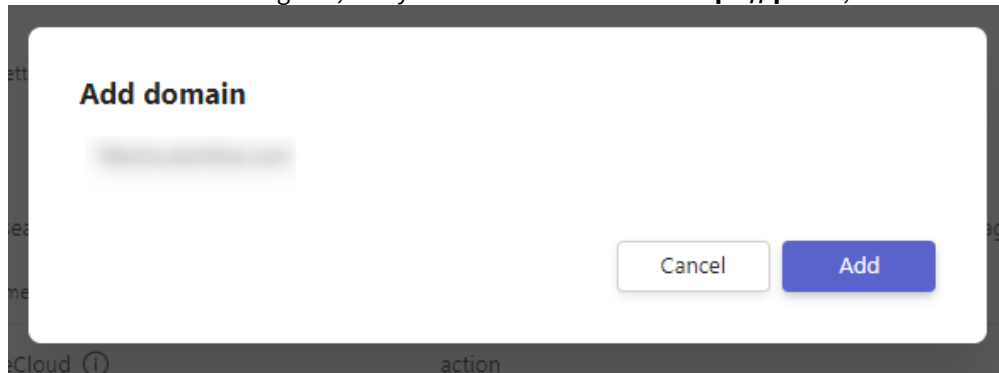
Save Revert

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



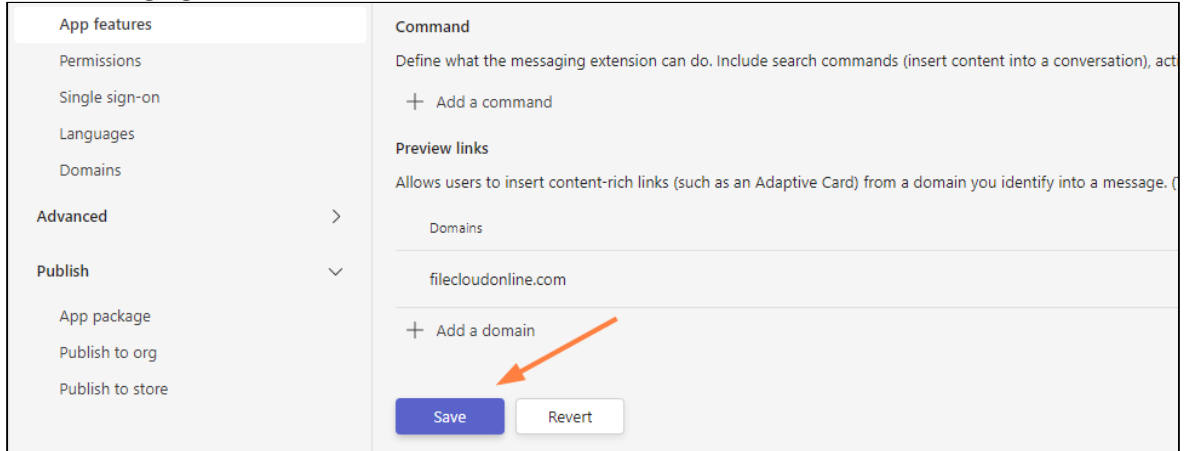
The screenshot shows the 'Developer Portal' interface for the 'FileCloud app'. The left sidebar contains navigation options: Overview, Dashboard, Analytics, Configure, Basic information, Branding, App features (highlighted), Permissions, and Single sign-on. The main content area shows the 'App features' configuration. A checkbox 'Users can reconfigure the app' is unchecked. Below it, the 'Command' section is titled 'Define what the messaging extension can do. Include search commands (ins)'. A table lists the command 'FileCloud' with ID 'FileCloud' and Name 'FileCloud'. Below the table is a '+ Add a command' button. The 'Preview links' section is titled 'Allows users to insert content-rich links (such as an Adaptive Card) from a d'. Below it is a '+ Add a domain' button, which is highlighted with an orange arrow. At the bottom are 'Save' and 'Revert' buttons.

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

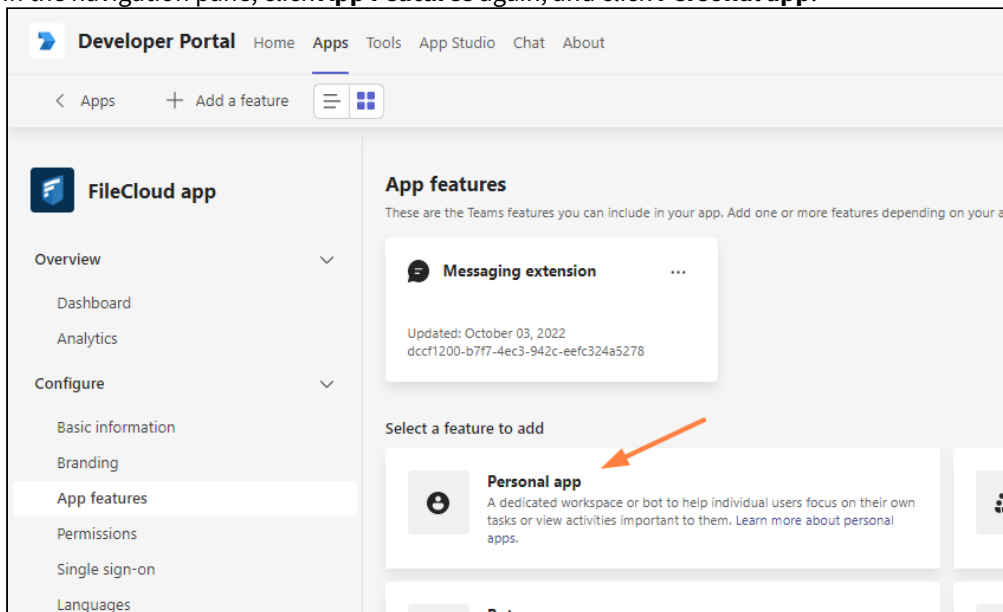


The screenshot shows a modal dialog box titled 'Add domain'. It contains a text input field with a blurred placeholder. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

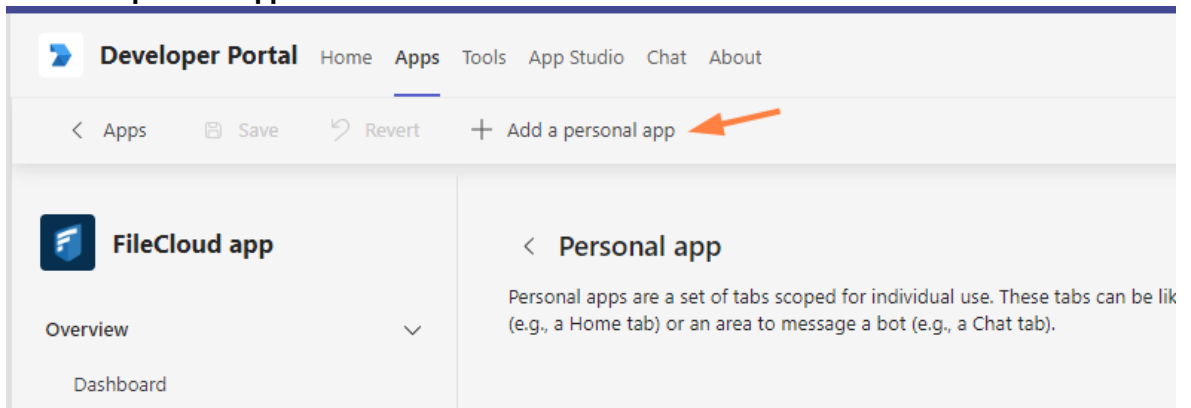
- i. In the **Messaging Extension** screen, click **Save**.



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



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



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*

Entity ID*

Content URL*

Website URL

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

FileCloud app

Overview ▼

Dashboard

Analytics

Configure ▼

Basic information

Branding

App features

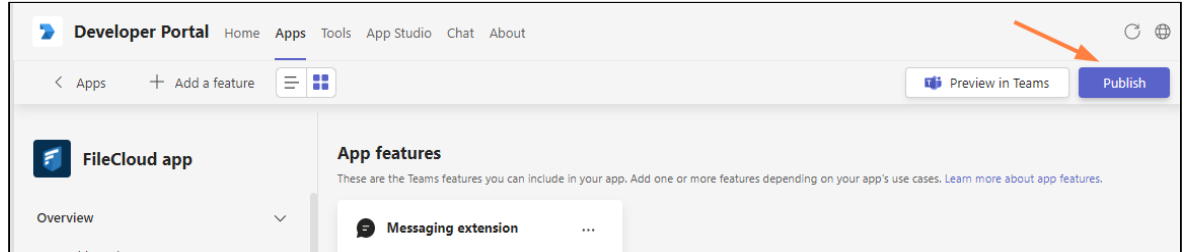
< Personal app

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	

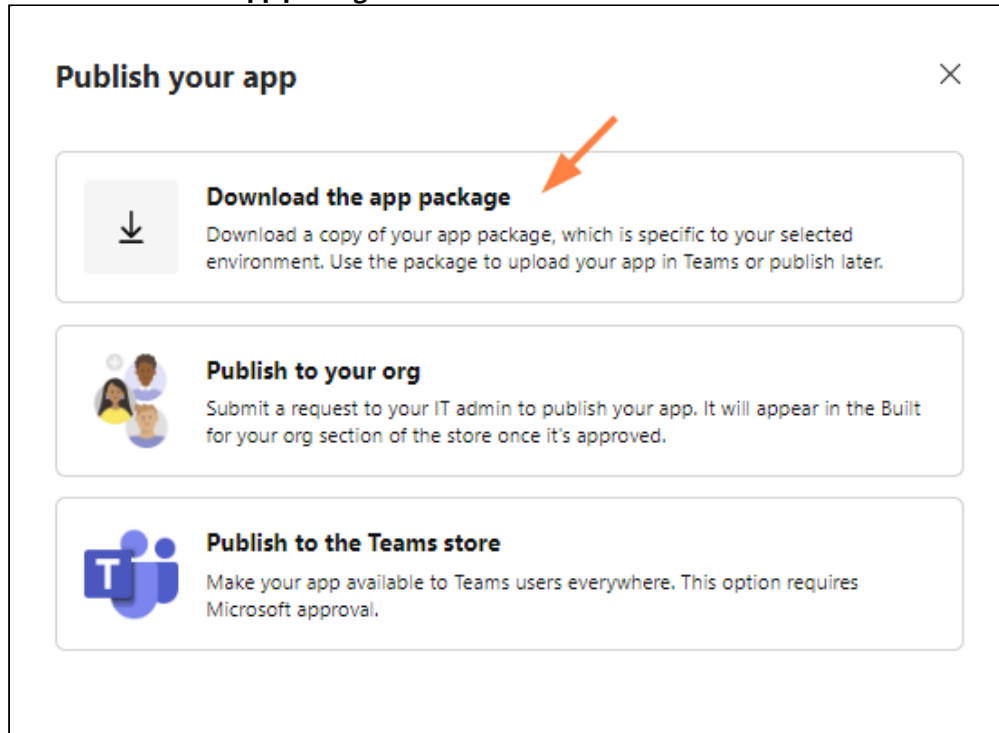
5. Export the application manifest zip file from Teams' **Developer Portal**.

- a. Click **Publish**.



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

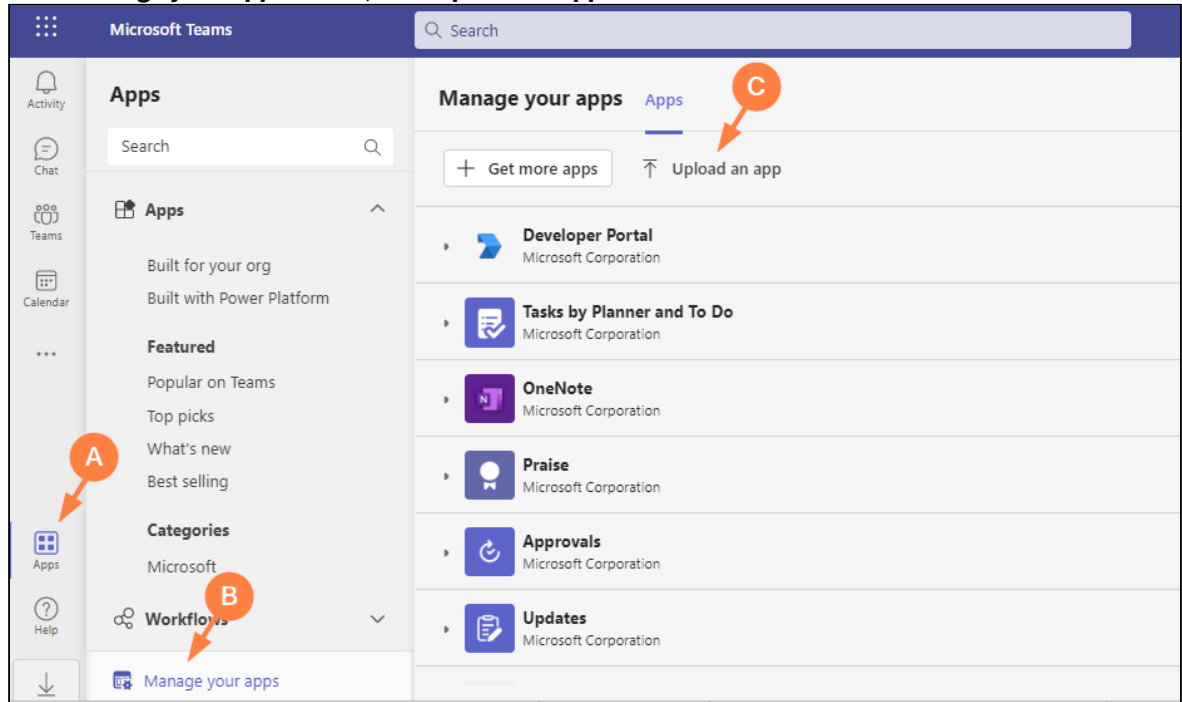
- b. Click **Download the app package**.



- c. Save the downloaded app package zip file.

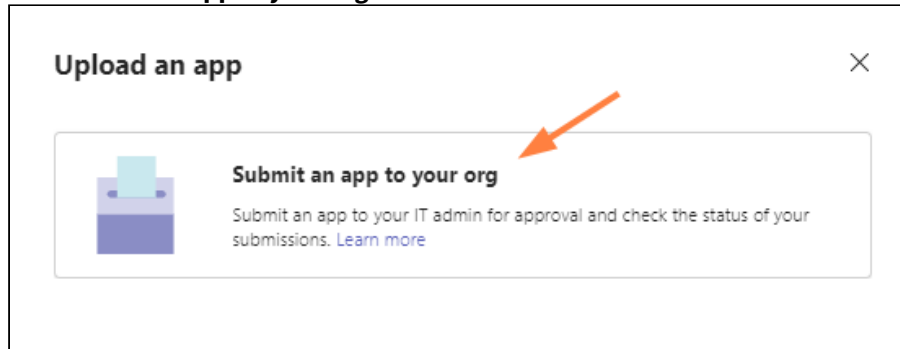
6. Upload the application and submit it for approval in MS Teams.
- In the MS Teams navigation pane, click **Apps**.
 - In the left panel click **Manage your apps**.

- c. In the **Manage your apps** screen, click **Upload an app**.



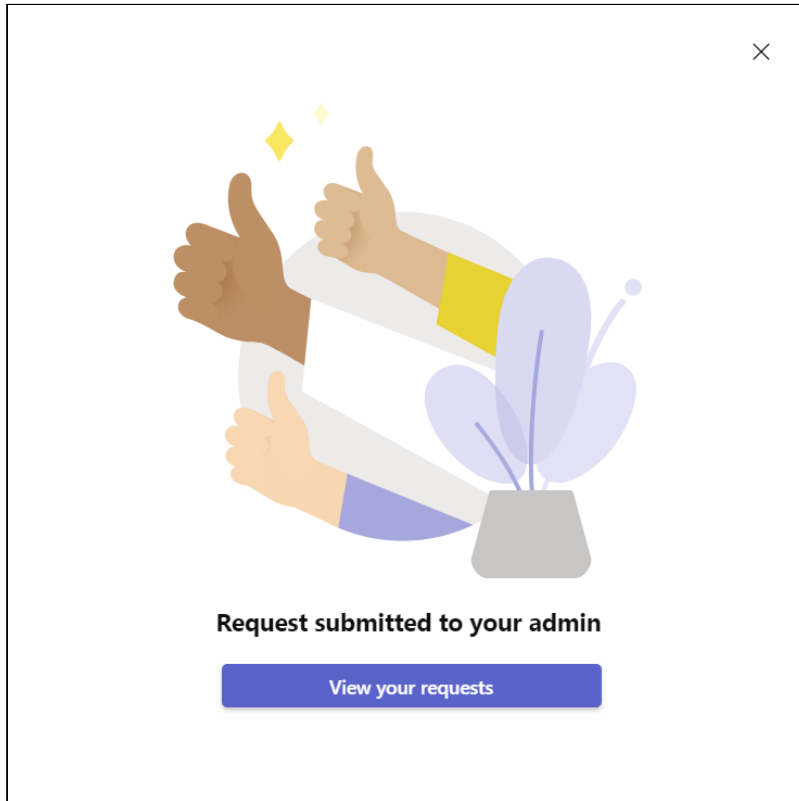
The **Upload an app** dialog box opens.

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



Your file explorer opens.

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



- 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.
7. Next [enable MS Teams integration in FileCloud](#)

For FileCloud Admins: Enabling Integration with MS Teams

After [FileCloud configuration in MS Teams](#) 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> is required, as well as 2-way communication with the domains [teams.microsoft.com](#), [*.teams.microsoft.com](#), and [*.skype.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' FileCloud 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. In the Admin portal, go to **Settings > Third Party Integrations > Microsoft Teams**.
2. Check **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](#)).
4. Check **Use browser session expiry** to use the FileCloud [session timeout setting](#) (located in **Settings** on the **Server** tab).

The screenshot shows the FileCloud Admin portal interface. At the top, there are navigation tabs: Server, Storage, Authentication, Admin, Email, Endpoint Backup, License, and Policies. Below these is a sub-menu for 'Third Party Integrations' with options for Misc and Reset. The 'Microsoft Teams' integration is selected and highlighted. Below the navigation, there are links for Salesforce, SIEM, reCAPTCHA, McAfee MVISION CASB, ICAP DLP, and AutoCAD Viewer. The main content area is titled 'Microsoft Teams Integration Settings' and contains the following options:

- Enable FileCloud MS Teams integration**: A checkbox labeled 'Select to enable FileCloud integration with Microsoft Teams' is checked.
- FileCloud MS Teams Bot Id**: A text input field is present, with a 'Set FileCloud MS Teams Bot Id' link below it.
- Use browser session expiry**: A checkbox labeled 'Use FileCloud browser session timeout only' is checked.

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>

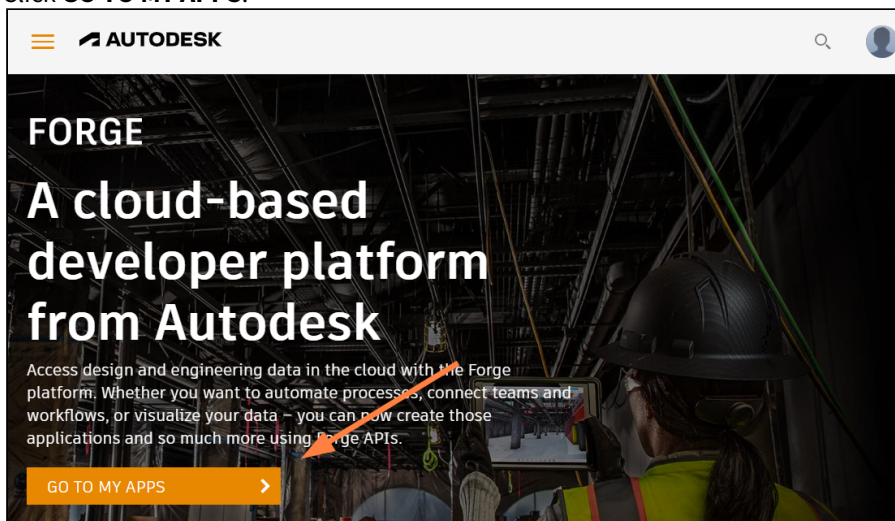
After you configure FileCloud integration with Autodesk Viewer, when users preview 3D and 2D model data file types, they are shown in Autodesk Viewer.

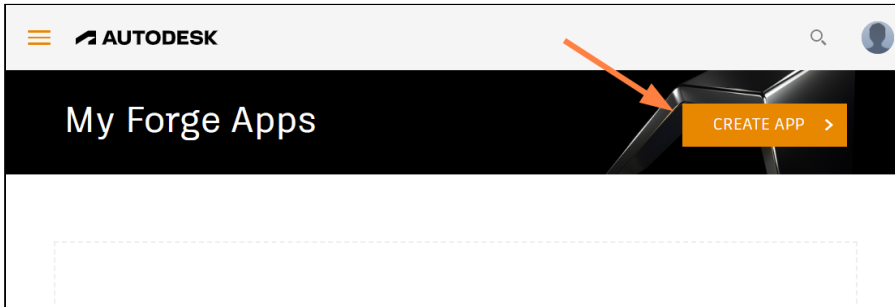
Setting up integration of FileCloud and Autodesk Viewer

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**.



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

Callback URL [What is this ?](#)

Your Website URL 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.

Autodesk Construction Cloud API	BIM 360 API	Data Exchange API	Data Management API
Design Automation API	Model Derivative API	Premium Reporting API	Reality Capture API
Token Flex Usage Data API	Webhooks API		

CREATE 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	AynGeamQTFXywhs76qvL6HeJRrs8GrTx1
Client Secret	<input type="password"/> <input type="button" value="REGENERATE"/>
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, go to **Settings > Third Party Integration > AutoCAD Viewer**.
8. Check **Select to enable FileCloud integration with Autodesk viewer**.
Additional fields appear.
9. In **API Secret**, enter your Autodesk Viewer **Client Secret**.
10. In **API key**, enter your Autodesk Viewer **Client ID**.

Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO

Content Search Web Edit Team Folders **Third Party Integrations** Misc Reset

Salesforce SIEM reCAPTCHA McAfee MVISION CASB ICAP DLP Microsoft Teams **AutoCAD Viewer**

Autodesk viewer

Enable Autodesk integration

Select to enable FileCloud integration with Autodesk viewer

API Secret

Specify the API Secret server remote hostname

API key

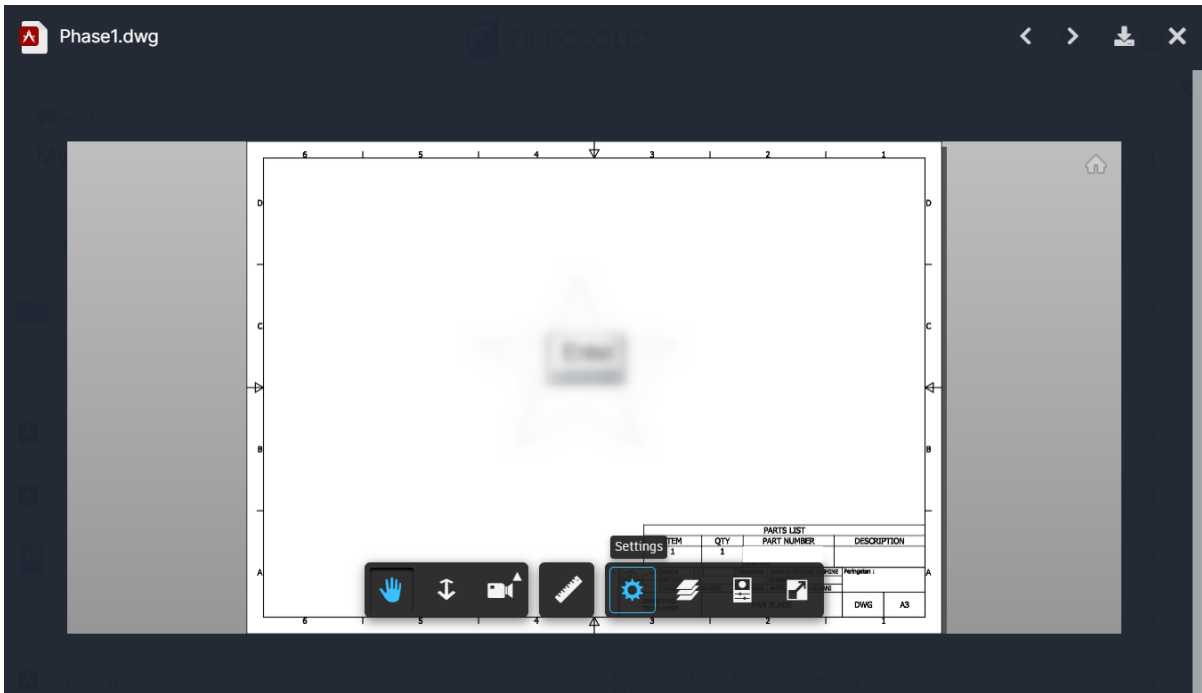
Specify the API key server remote hostname

Region

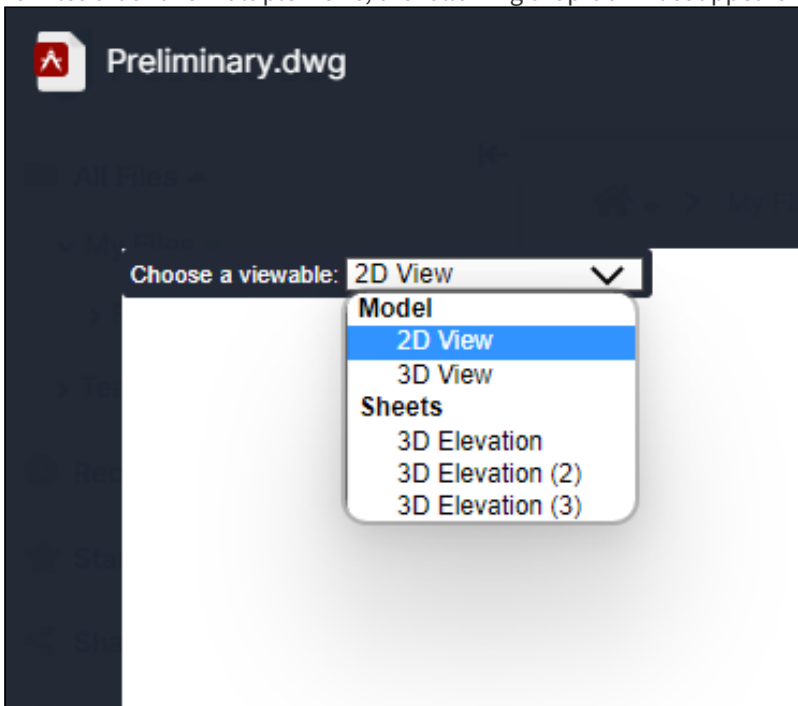
US

Specify the region in wich Autodesk viewer is used

11. Click **Save**.
12. 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 22.232 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. In the admin portal, go to **Settings > Third Party Integrations > AI**.



Server Storage Authentication Admin Email Endpoint Backup License Policies

Third Party Integrations Misc Reset

Salesforce SIEM reCAPTCHA McAfee MVISION CASB ICAP DLP Microsoft Teams

AutoCAD Viewer **AI**

AI Integration Settings

Enable LLM Features

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

Notice

Enabling external AI-based large language model providers such as OpenAI for classification will cause the text content of files classified using this method to be sent to third-party services. This feature should be used in accordance with your organization's Information Security and privacy policies.

Provider

OpenAI

Specify the LLM provider.

API Key

.....

Specify the API key for the LLM provider.

Model

gpt-4-1106-preview

Specify an LLM model to use.

Organization

Optional - Specify the Organization ID.

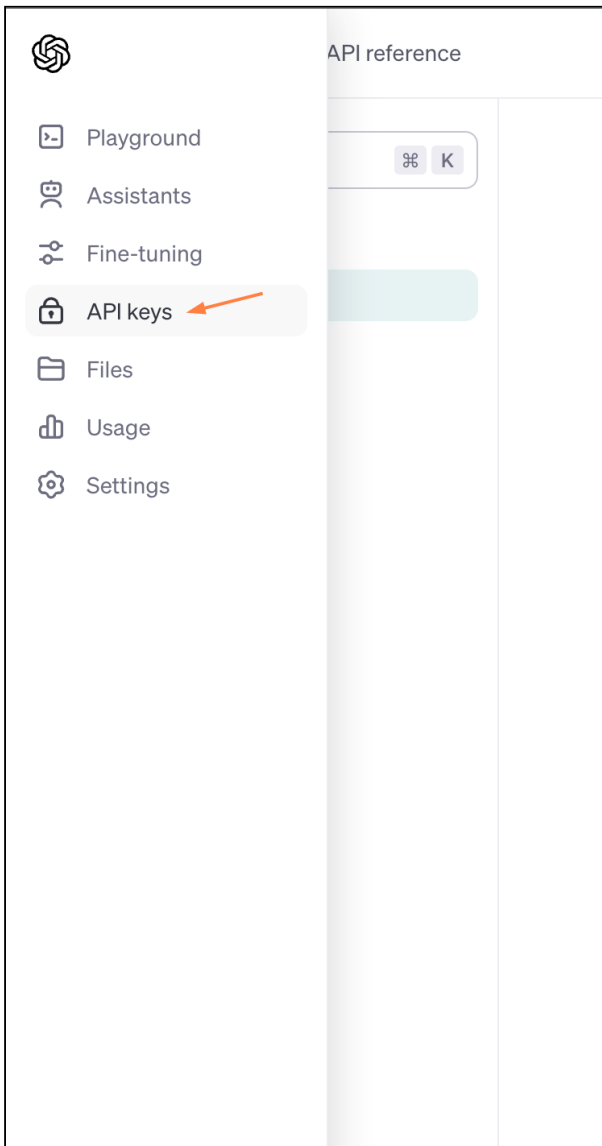
Custom URL

Optional - Specify a custom endpoint URL to use.

Check AI Credentials

[Test Credentials](#)

2. Check **Enable LLM Features**.
3. In **Provider**, choose **OpenAI**.
4. Enter the values for **API Key** and **Organization**.
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:

6. In most cases you are not required to enter a **Custom URL**. It is only necessary if you use a custom OpenAI instance.
7. Click **Test Credentials** to confirm that **FileCloud** and **AI** are properly integrated.