# FileCloud Server Version 23.232

# Third Party Integration Settings

Printed on 02/06/2024

# Copyright Notice

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

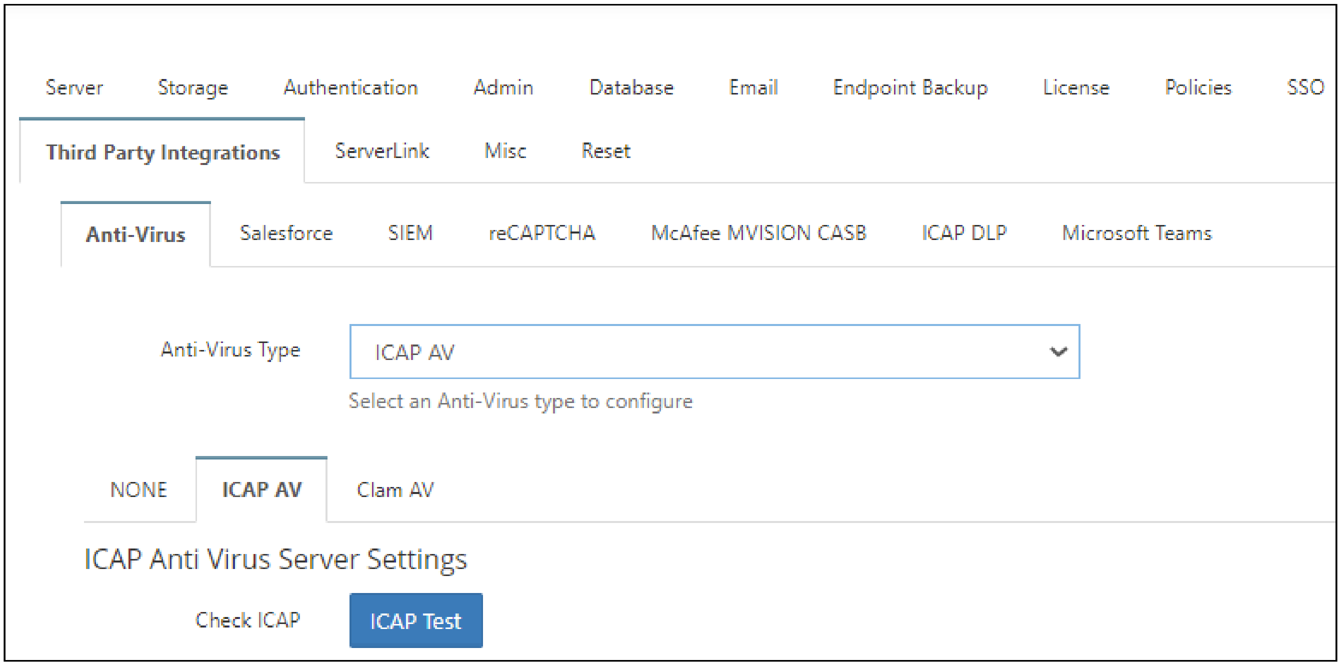
Fax: +1 (866) 824-9584

Email: support@filecloud.com

# Table of Contents

# 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.



Anti-Virus Type: ICAP AV

Select an Anti-Virus type to configure

ICAP Anti Virus Server Settings

Check ICAP

**In this section**:

- Enable Antivirus Scanning
- Integrating FileCloud with Salesforce
- SIEM Integration
- reCaptcha Settings
- CASB integration
- ICAP DLP
- Microsoft Teams
- Setting Up AutoCAD File Preview with Autodesk Viewer
- AI Integration

# Enable Antivirus Scanning

ⓘ Internet Content Adaptation Protocol (ICAP) antivirus integration is available in FileCloud version 18.2
Notes:

- The antivirus security feature works on both Linux and Windows.
- The antivirus product may or may not be deployed on the same server as the one running the FileCloud instance.

- Antivirus scanning applies when files are uploaded to FileCloud.
- Virus scanning of a file is scheduled as soon as file upload is complete.
- Virus scanning is managed by FileCloud.

You must address virus scanning as it is a critical security feature, especially when file storage is involved.

- FileCloud allows users to upload files with arbitrary content.
- It is of utmost importance to make sure that the uploaded files are checked for malicious content in the form of viruses, trojans, malware, etc.
- FileCloud readily integrates with a variety non-commercial and commercially licensed antivirus solutions available in the market.

You can configure FileCloud to scan uploaded files in the following ways:

- Use ClamAV, an open source antivirus software that is included with FileCloud.
- Use ICAP to integrate your own choice of antivirus scanning software with FileCloud.

### What is ICAP?

Internet Content Adaptation Protocol (ICAP) is a generic protocol that allows web servers to offload specialized tasks. This delegation is helpful when the tasks require custom-built servers.

Examples of such specialized tasks include:

- DLP (data loss prevention) based content scanning
- URL filtering
- antivirus scanning

### Which do I use, ClamAV or ICAP?

If you have already purchased your own anti-virus solution and want to use it, then choose ICAP.

If you do not want to use ClamAV for various reasons, then choose ICAP.

If you want to use antivirus scanning included with FileCloud, then choose ClamAV.

# Which solution do you want to use?

⚠ Neither of these options provides protection for the server on which FileCloud is deployed. The antivirus solution configured here applies only for the uploaded files.

➡ ClamAV

➡ ICAP

# Use ClamAV Antivirus Scanning

FileCloud does not provide support for ClamAV, which is third-party software. If you need assistance with your ClamAV configuration or setup please check the ClamAV Troubleshooting FAQ.

ClamAV integration with Azure/S3 external networks is not supported.

You can configure FileCloud to scan uploaded files using ClamAV, an open source antivirus software.

ClamAV is available for:

- Windows
- Linux

When a virus is detected in an uploaded file, the following actions occur:

1. The incoming file is deleted.
2. An alert is displayed in the admin portal.
3. A toast is displayed in the user portal.
4. An entry is added in the audit log about virus detection in the file and subsequent deletion of the file.

## To Use ClamAV

**Install ClamAV in Ubuntu**

These instructions are for Ubuntu Linux, but they can be used for other Linux systems using equivalent commands.

To install ClamAV in Ubuntu:

1. Install the ClamAV package

   ```
   sudo apt-get install clamav-daemon
   ```

2. You might need to run 'freshclam' to update the antivirus database files

```
sudo freshclam
```

3. Update the ClamAV-Daemon mode to use TCP, by running the sudo dpkg-reconfigure clamav-base

```
sudo dpkg-reconfigure clamav-daemon
```

4. In the reconfigure wizard, choose Socket Type TCP and Interface as localhost to listen to.

5. After reconfigure finishes, verify the clamd.conf file is setup correctly (/etc/clamav/clamd.conf)

   NOTE: TCPAddr localhost may not work. You can enter the filecloud URL in place of TCPAddr to make it work

```
TCPSocket 3310
TCPAddr localhost
StreamMaxLength 100M
```

6. Additional commands for Ubuntu 16

```
#The Socket Configuration changes are also required as below:


#Edit the file /etc/systemd/system/clamav-daemon.service.d/extend.conf

[Socket]
SocketUser=clamav
ListenStream=/var/run/clamav/clamd.ctl
SocketGroup=clamav
SocketMode=666
ListenStream=xx.xx.xx.xx:3310


# Note that xx.xx.xx.xx = IP address of server or 127.0.0.1


#After that run:


systemctl --system daemon-reload
systemctl restart clamav-daemon.service
```

7. Start ClamAV-Daemon

```
sudo /etc/init.d/clamav-daemon start
```

### Install ClamAV on Windows

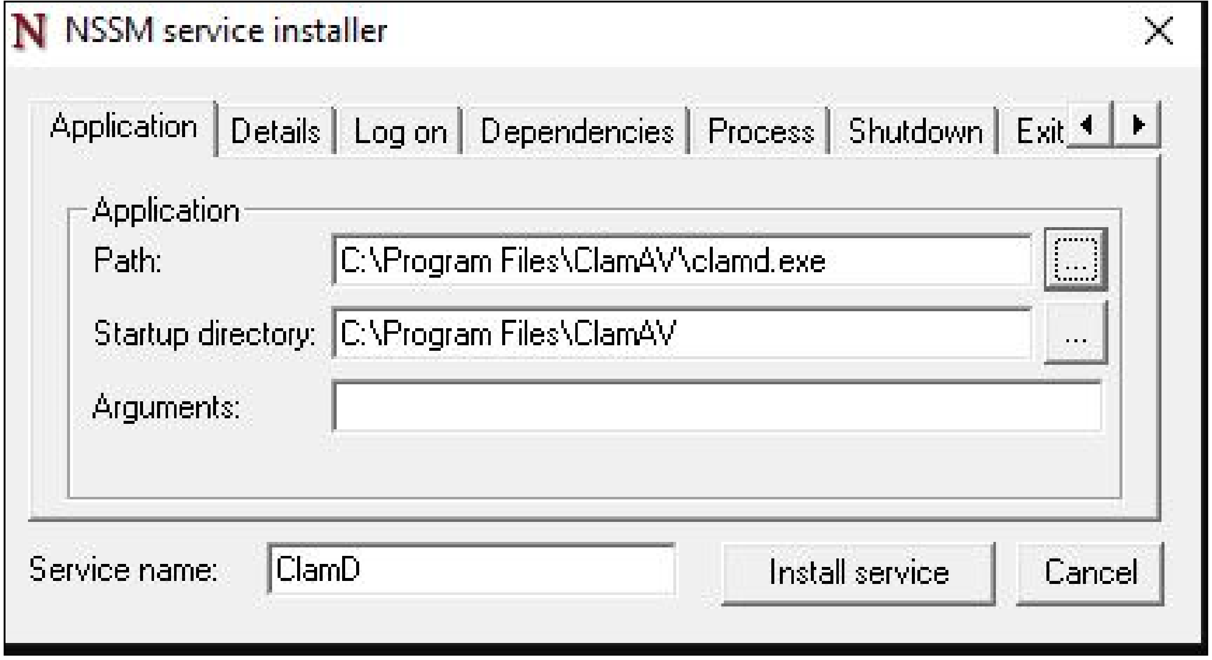
- The native ClamAV version does not have a GUI.
- The virus database definition can be updated using freshclam using a Windows task scheduler.

### To install ClamAV on Windows:

1. Download the latest version of the ClamAV installer from:
   http://www.clamav.net/downloads
2. Install ClamAV by running the latest msi file downloaded.
3. Download the nssm Service Manager from:
   https://patch.codelathe.com/tonidocloud/live/3rdparty/nssm/nssm.zip
4. Unzip the nssm folder and move the nssm folder to the C:\ driveor, if you are installing ClamAV in the FileCloud Server, to the C:\xampp folder.
5. Navigate to the nssm folder in the command line and run the following command:

```
C:\nssm>nssm install ClamD
```

The nssm service install tool window opens:



Path: C:\Program Files\ClamAV\clamd.exe

Startup directory: C:\Program Files\ClamAV

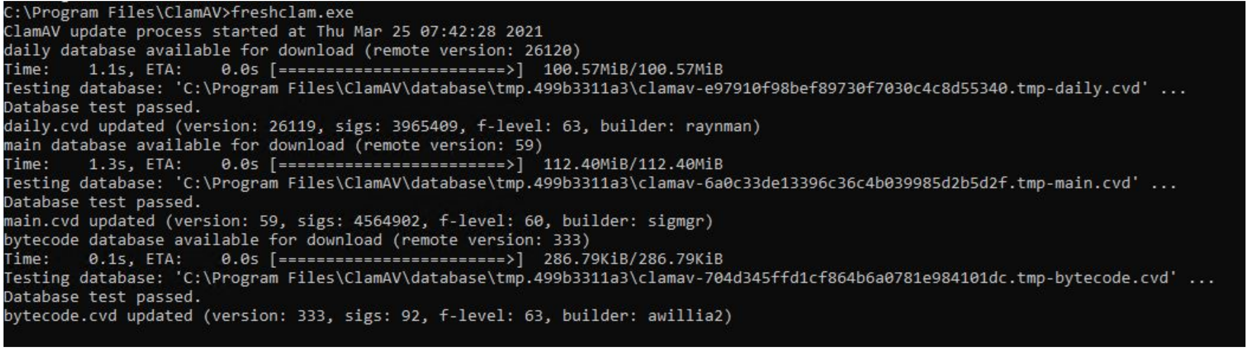
Arguments:

Service name: ClamD

6. To install the service, select the clamd.exe file path in **Application Path** and click **Install Service**.
7. Copy **clamd.conf.sample** and **freshclam.conf.sample** from **C:\Program Files\ClamAV\conf_examples** to **C:\Program Files\ClamAV**, and rename them **clamd.conf** and **freshclam.conf**
8. In **clamd.conf** and **freshclam.conf**, comment out the line beginning with *Example*.
9. If ClamAV is installed on a server other than the FileCloud server:
   Bind the IP address of the server in **clamd.conf** by changing the IP address for **TCPAddr**.
10. To update the ClamD database, enter:

```
cd C:\Program Files\ClamAV
freshclam.exe
```

The console response should appear similar to:



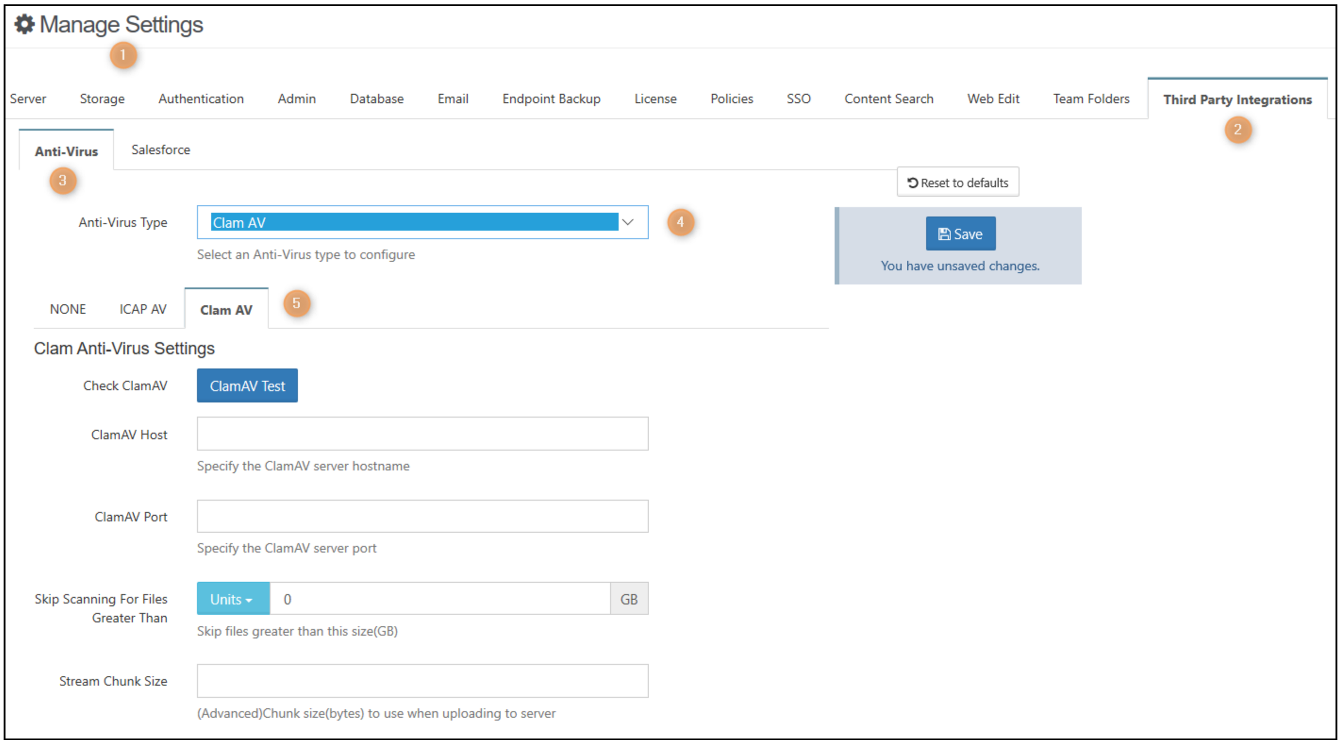
```
C:\Program Files\ClamAV>freshclam.exe
ClamAV update process started at Thu Mar 25 07:42:28 2021
daily database available for download (remote version: 26120)
Time:    1.1s, ETA:    0.0s [========================>]  100.57MiB/100.57MiB
Testing database: 'C:\Program Files\ClamAV\database\tmp.499b3311a3\clamav-e97910f98bef89730f7030c4c8d55340.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 26119, sigs: 3965409, f-level: 63, builder: raynman)
main database available for download (remote version: 59)
Time:    1.3s, ETA:    0.0s [========================>]  112.40MiB/112.40MiB
Testing database: 'C:\Program Files\ClamAV\database\tmp.499b3311a3\clamav-6a0c33de13396c36c4b039985d2b5d2f.tmp-main.cvd' ...
Database test passed.
main.cvd updated (version: 59, sigs: 4564902, f-level: 60, builder: sigmgr)
bytecode database available for download (remote version: 333)
Time:    0.1s, ETA:    0.0s [========================>]  286.79KiB/286.79KiB
Testing database: 'C:\Program Files\ClamAV\database\tmp.499b3311a3\clamav-704d345ffd1cf864b6a0781e984101dc.tmp-bytecode.cvd' ...
Database test passed.
bytecode.cvd updated (version: 333, sigs: 92, f-level: 63, builder: awillia2)
```

11. Start the service **ClamD** from Windows Services.
12. Verify the service is running and bind it to the localhost IP address or the IP address of the ClamAV server by running the following command:

```
netstat -ano |findstr 3310
```

### Integrate ClamAV with FileCloud

Once ClamAV is setup and started, the next step is to add details of the ClamAV service to FileCloud server.



Anti-Virus Type: Clam AV

Select an Anti-Virus type to configure

Clam Anti-Virus Settings

Check ClamAV

ClamAV Host

Specify the ClamAV server hostname

ClamAV Port

Specify the ClamAV server port

Skip Scanning For Files Greater Than: 0

Skip files greater than this size(GB)

Stream Chunk Size

(Advanced)Chunk size(bytes) to use when uploading to server

### To integrate ClamAV with FileCloud:

1. Open a browser, log in to the Admin Portal, and from the left navigation panel, click ***Settings*****.**
2. On the *Manage Settings* screen, select the ***Third Party Integrations*** **tab.**
3. **On the *Third Party Integrations* tab, select the *Anti-Virus*** sub-tab.
4. **On the *Anti-Virus*** sub-tab, in *Anti-Virus Type*, select *Clam AV*.
5. Select the *Clam AV* sub-tab.
6. On the *Clam AV* tab, select the checkbox for *Enable ClamAV Scan*.
7. Enter the following information:

| Setting | Description |
|---|---|
| **Enable ClamAV Scan** | Check this setting to enable AV scanning |
| **ClamAV Host** | Enter the URL or IP of the system where Clam AV is running. This can be local or remote system. |
| **ClamAV Port** | The port used by ClamAV (This is set when ClamAV is installed in the previous section) |
| **Skip scanning for files greater than** | This is the file limit in bytes that will be scanned. For example, very large files can be excluded from scanning. Default value is 25MB |
| **Stream Chunk Size** | This is a advanced setting used to stream the file content to ClamAV for scanning. Default is 8KB. |

8. Click ***Save***.
9. To verify connectivity, click the ***ClamAV Test*** button.

⚠ Once the ClamAV configuration is set up, every file uploaded to FileCloud will be scanned before being added to FileCloud storage.

- If a file fails AV check (i.e. a virus detected) then the file will be deleted and an entry will be added to the Audit log with the details of the file.

## If scanning fails

If scanning fails because the ClamAV server is down, a message appears on your screen, and your Manage Alerts page displays the warning:
**Unable to communicate with ClamAV Server. Check immediately.**

By default, if ClamAV fails to scan a file because the ClamAV server is down, the file is not deleted.

**To automatically delete files if ClamAV scan fails because the ClamAV server is unavailable**:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

   ```
   define("TONIDOCLOUD_CLAMAV_DELETE_ON_SCAN_FAIL", "1");
   ```

   Now, when scan fails, the file is deleted, and the audit log displays the message: *ClamAV removed [FILE_PATH] due to scan fail.*
   If TONIDOCLOUD_CLAMAV_DELETE_ON_SCAN_FAIL is enabled and the CLAMAV server is not available, FileCloud does not allow files to be uploaded.

## Use ICAP Antivirus Scanning

> ICAP antivirus integration is available in FileCloud version 18.2.

> ICAP scans are noted in audit logs beginning with version 19.3.

FileCloud uses Internet Content Adaption Protocol (ICAP) to integrate with any antivirus product currently supporting ICAP.

### 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.

FileCloud's ICAP integration feature:

- Works on both Linux and Windows servers
- Is part of FileCloud server itself
- Provides flexibility and scalability - the ICAP antivirus server does not have to be deployed on the same server as the one running the FileCloud server instance.
- Triggers virus scanning only when files are uploaded to FileCloud.
- Scanning is scheduled "inline" as soon as the file upload is completed

> If you have already purchased your own antivirus solution and want to use it, or if you do not want to use ClamAV for various reasons, we highly recommended using this feature.

We also recommend that the ICAP Antivirus server administrator consult the antivirus product documentation to understand the operational and configuration parameters, capabilities and limitations. As virus scanning is a critical feature for maintaining water-tight security and smooth functioning of any workplace, consulting the documentation is important before configuring FileCloud's ICAP integration settings, it would also help in troubleshooting and maintenance.

## How ICAP detects a virus

After a file is scanned, FileCloud checks for the following response headers on the file scanning result:

- X-Infection-Found
- X-Violations-Found
- X-Virus-ID

If any of these headers are found, FileCloud performs the actions listed below, under **When ICAP detects a virus**.

## When ICAP detects a virus

Similar to the case of ClamAV, if FileCloud's ICAP Client has been configured correctly with a properly deployed ICAP AV server, when a virus is detected in an uploaded file, the following actions occur:

1. The incoming file is deleted.
2. An alert is displayed in the Admin Portal.
3. A toast is displayed in the User Portal.
4. An entry is added in the audit log about virus detection in the file and subsequent deletion of the file.

## Integrating ICAP with FileCloud

Using ICAP to integrate Antivirus capabilities into FileCloud requires customers to:

1. Set up an ICAP antivirus server.
2. Configure FileCloud's inbuilt ICAP client to access your antivirus server.

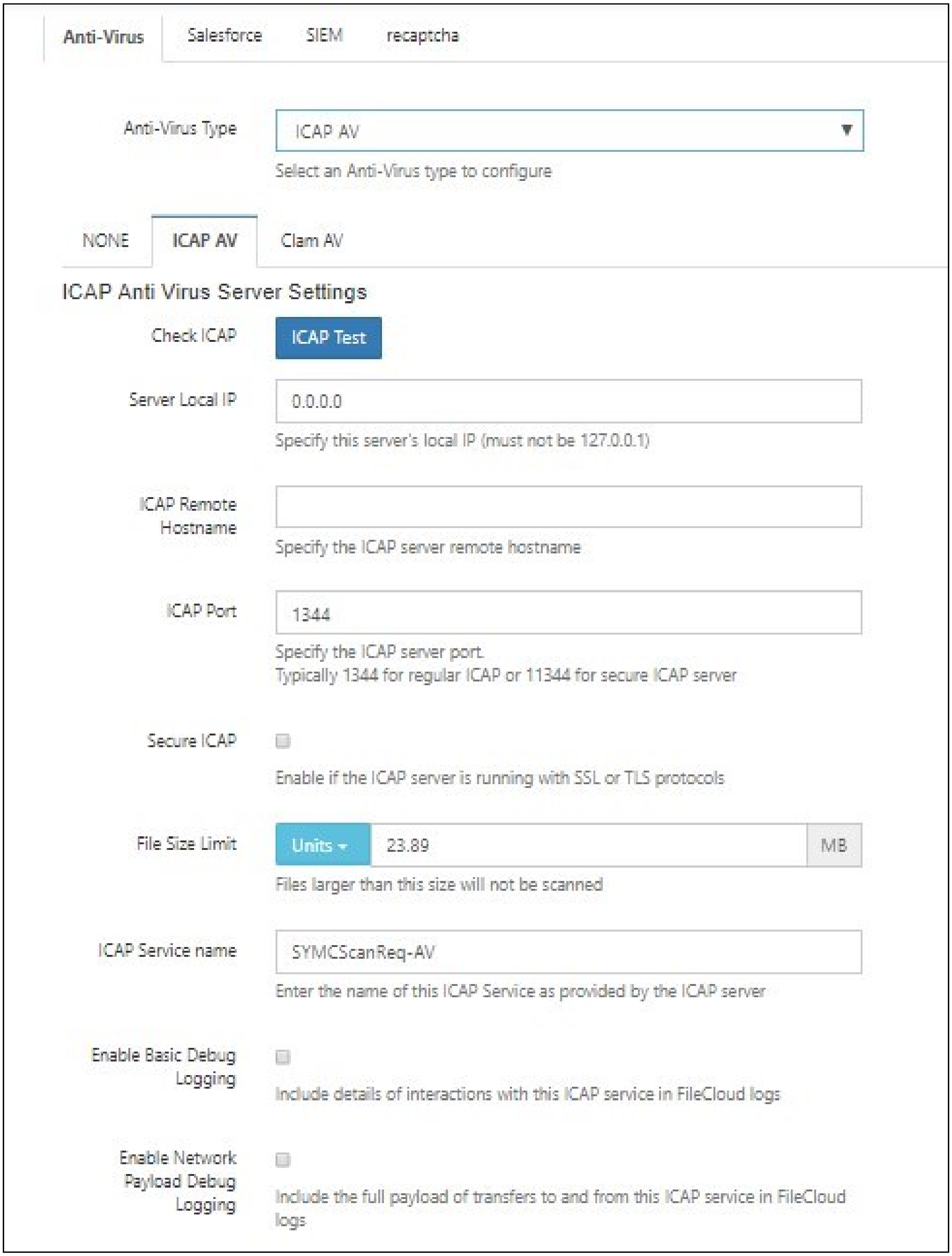
FileCloud has made it easy for administrators to connect FileCloud to your antivirus server by including an inbuilt ICAP Client.

The easy configuration steps apply to both Windows and Linux servers.

To configure FileCloud to use your antivirus server:

1. Open a browser and log on to the *Admin Portal*.
2. On the left navigation panel, click *Settings*.
3. Select the *Third Party Integrations* tab.
4. In the *Anti-Virus* tab, from the Anti-Virus type drop down list, select *ICAP AV*.
5. Configure the various parameters for the ICAP Client as described in the Table 1.
6. To save your changes, click *Save*.
7. To confirm if the configuration has been done correctly, click the ICAP Test button.

8. A positive reply will confirm proper connectivity with the ICAP AV Server.



Anti-Virus Type: ICAP AV ▼

Select an Anti-Virus type to configure

ICAP Anti Virus Server Settings

Check ICAP: ICAP Test

Server Local IP: 0.0.0.0

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

ICAP Remote Hostname:

Specify the ICAP server remote hostname

ICAP Port: 1344

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 ▾ 23.89 MB

Files larger than this size will not be scanned

ICAP Service name: SYMCScanReq-AV

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

Enable Basic Debug Logging: □

Include details of interactions with this ICAP service in FileCloud logs

Enable Network Payload Debug Logging: □

Include the full payload of transfers to and from this ICAP service in FileCloud logs

Table 1. ICAP Client Parameters

| 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 AV is deployed. |
| **ICAP Port** | Leave the default value of 1344 as it is. In rare cases, this might need to be changed to whatever port the ICAP AV server is listening on. |
| **Secure ICAP** | Enable if the ICAP server is running with SSL or TLS protocols. |
| **File Size Limit** | This is the file limit in bytes that will be scanned. For example, very large files can be excluded from scanning. Default value is 25MB |
| **ICAP Service Name** | Consult the ICAP AV server product documentation to know this value. It must be set correctly otherwise integration wont work. |
| **Enable Basic Debug Logging** | Check this to enable logging of detailed operational debug messages in the (error) logs. |
| **Enable Network Payload Debug Logging** | Check this to enable logging of detailed network communication related debug messages in the (error) logs. |

## User details sent with scan requests

To help the ICAP server determine if a scan is required, the following headers are sent with every scan request:

Header X-FILECLOUD-USER-NAME - name of user performing the upload.
Header X-FILECLOUD-USER-EMAIL -  email of user performing the upload.
Header X-FILECLOUD-USER-TYPE - type of user performing the upload. Possible values are "full", "guest", and "external".
Header X-FILECLOUD-GROUP-NAMES - comma-separated list of group names that user performing the upload is a member of.

To disable sending of these headers:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

```
define("TONIDOCLOUD_ICAPAV_DISABLE_ADDITIONALHEADERS", "1");
```

## If scanning fails

If scanning fails because the ICAP server is down, a message appears on your screen, and your Manage Alerts page displays the message:

□ 2020-Jul-29 07:06 PM Warning Unable to communicate with ICAP/AV Server. Check immediately.

By default, if ICAP fails to scan a file because the ICAP server is down, the file is not deleted.

**To automatically delete files if ICAP scan fails because the ICAP server is unavailable**:

1. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
2. Add the line:

   ```
   define("TONIDOCLOUD_ICAP_DELETE_ON_SCAN_FAIL",1);
   ```

   Now, when scan fails, the file is deleted, and the audit log displays the message: *ICAP removed [FILE_PATH] due to scan fail.*

   > ⚠ If TONIDOCLOUD_ICAP_DELETE_ON_SCAN_FAIL is enabled and the ICAP server is not available, FileCloud does not allow files to be uploaded.

# 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:

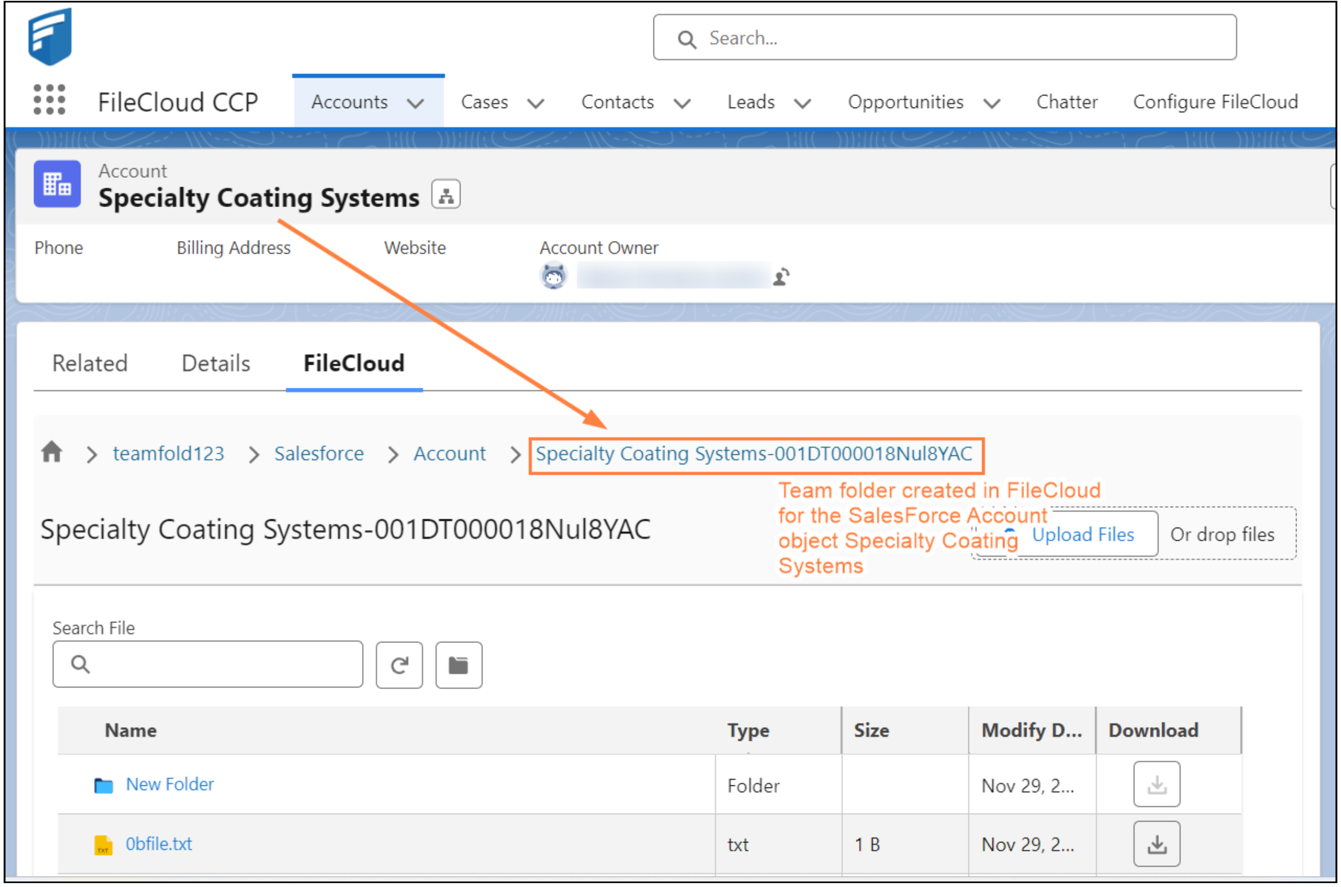
- Upload, download, access and share remote files from within Salesforce.
- Store files on-premises or in the public cloud (Amazon AWS, Microsoft Azure). Access files securely inside Salesforce from anywhere.
- Share files and collaborate with team members, even if they are not Salesforce users.
- Integrate 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.



Specialty Coating Systems-001DT000018Nul8YAC

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

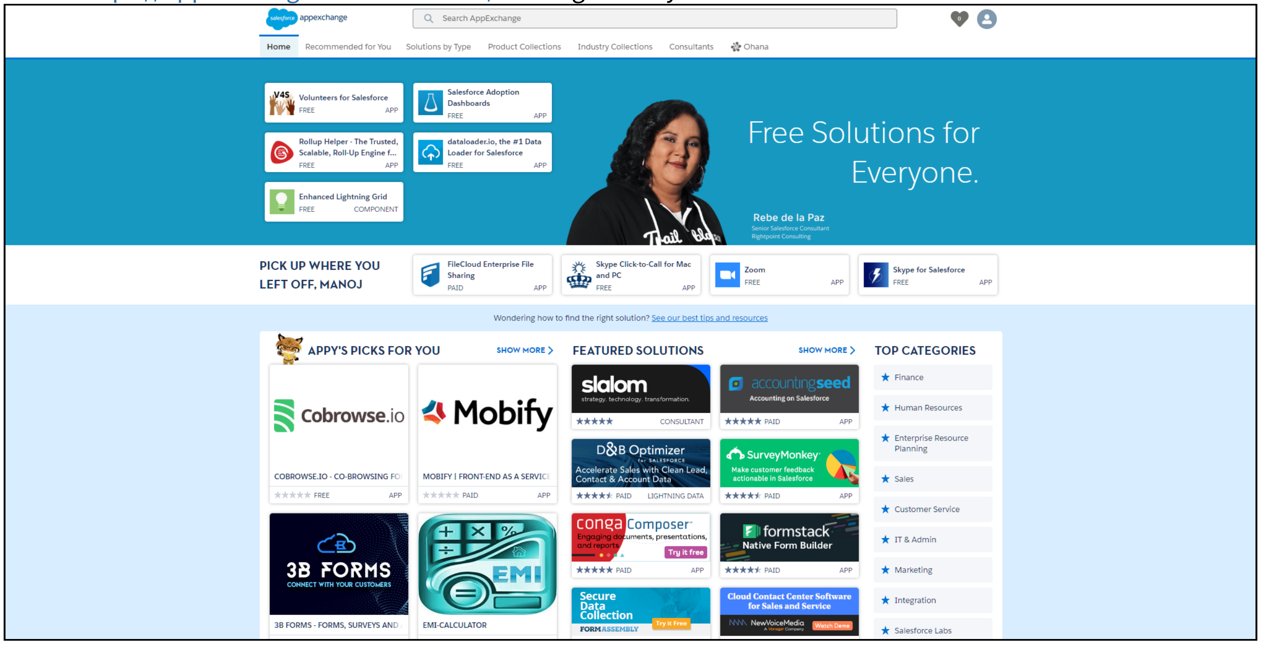
| Name | Type | Size | Modify D... | Download |
|---|---|---|---|---|
| New Folder | Folder | | Nov 29, 2... | |
| 0bfile.txt | txt | 1 B | Nov 29, 2... | |

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.

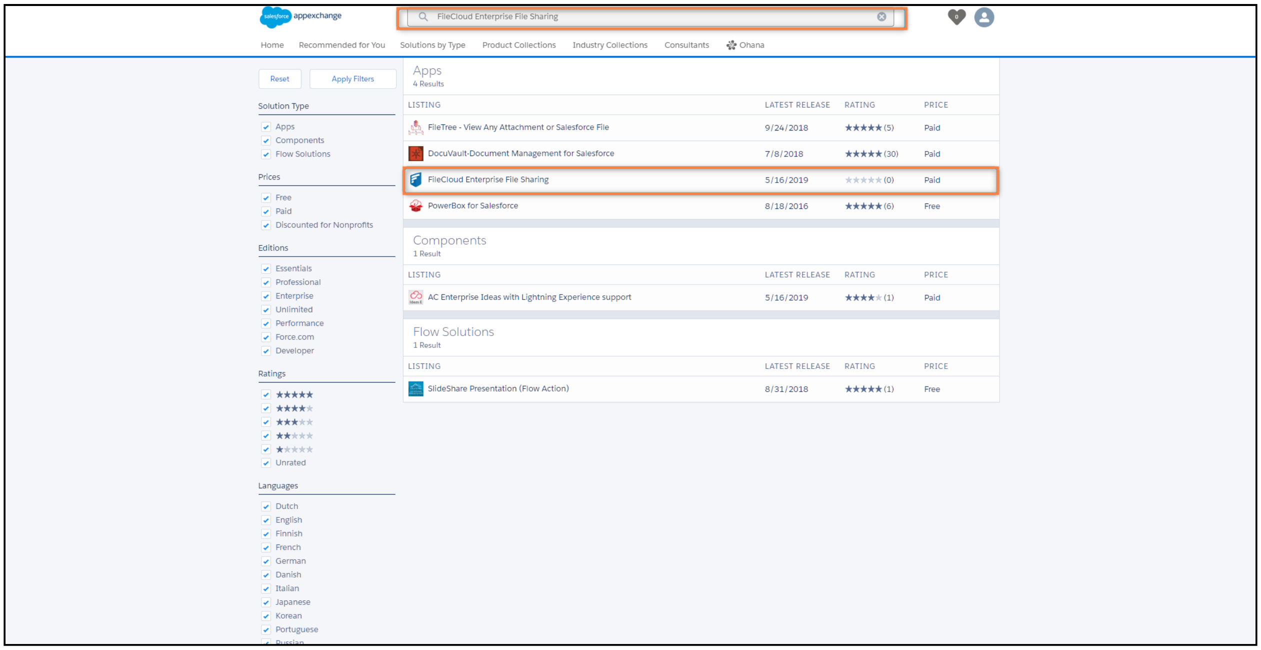
## Adding FileCloud to Salesforce

**To integrate FileCloud with Salesforce:**

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


appexchange
Search AppExchange
Home
Recommended for You
Solutions by Type
Product Collections
Industry Collections
Consultants
Ohana
Volunteers for Salesforce FREE APP
Salesforce Adoption Dashboards FREE APP
Rollup Helper - The Trusted, Scalable, Roll-Up Engine f... FREE APP
dataloader.io, the #1 Data Loader for Salesforce FREE APP
Enhanced Lightning Grid FREE COMPONENT
Free Solutions for Everyone.
Rebe de la Paz
Senior Salesforce Consultant
Rightpoint Consulting
PICK UP WHERE YOU LEFT OFF, MANOJ
FileCloud Enterprise File Sharing PAID APP
Skype Click-to-Call for Mac and PC FREE APP
Zoom FREE APP
Skype for Salesforce FREE APP
Wondering how to find the right solution? See our best tips and resources
APPY'S PICKS FOR YOU
SHOW MORE
FEATURED SOLUTIONS
SHOW MORE
TOP CATEGORIES
Cobrowse.io
COBROWSE.IO - CO-BROWSING FO
FREE APP
Mobify
MOBIFY | FRONT-END AS A SERVIC
PAID APP
slalom
CONSULTANT
accountingseed
Accounting on Salesforce
PAID APP
D&B Optimizer
Accelerate Sales with Clean Lead, Contact & Account Data
PAID LIGHTNING DATA
SurveyMonkey
Make customer feedback actionable in Salesforce
PAID APP
3B FORMS
CONNECT WITH YOUR CUSTOMERS
3B FORMS - FORMS, SURVEYS AND
EMI
EMI-CALCULATOR
conga Composer
Try it free
PAID APP
formstack
Native Form Builder
PAID APP
Secure Data Collection
FORMASSEMBLY
Cloud Contact Center Software for Sales and Service
NewVoiceMedia
Finance
Human Resources
Enterprise Resource Planning
Sales
Customer Service
IT & Admin
Marketing
Integration
Salesforce Labs

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



Apps
4 Results

| LISTING | LATEST RELEASE | RATING | PRICE |
|---|---|---|---|
| FileTree - View Any Attachment or Salesforce File | 9/24/2018 | ★★★★★ (5) | Paid |
| DocuVault-Document Management for Salesforce | 7/8/2018 | ★★★★★ (30) | Paid |
| FileCloud Enterprise File Sharing | 5/16/2019 | ☆☆☆☆☆ (0) | Paid |
| PowerBox for Salesforce | 8/18/2016 | ★★★★★ (6) | Free |

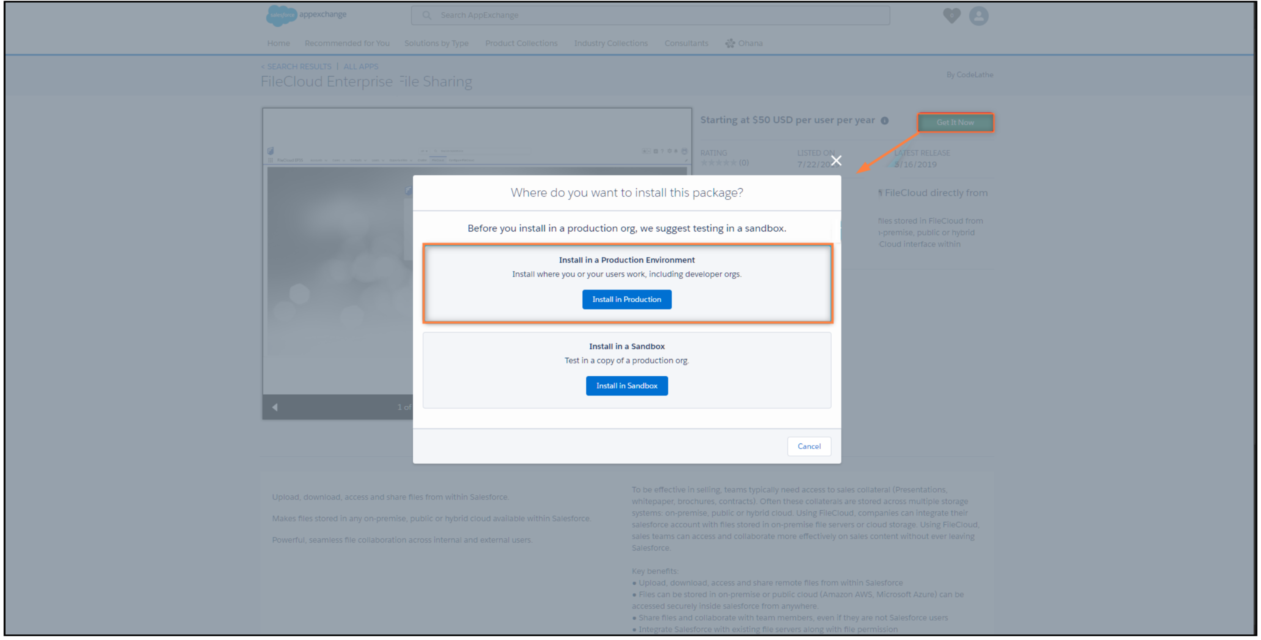
Components
1 Result

| LISTING | LATEST RELEASE | RATING | PRICE |
|---|---|---|---|
| AC Enterprise Ideas with Lightning Experience support | 5/16/2019 | ★★★★☆ (1) | Paid |

Flow Solutions
1 Result

| LISTING | LATEST RELEASE | RATING | PRICE |
|---|---|---|---|
| SlideShare Presentation (Flow Action) | 8/31/2018 | ★★★★★ (1) | Free |

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



FileCloud Enterprise File Sharing

Starting at $50 USD per user per year

Where do you want to install this package?

Before you install in a production org, we suggest testing in a sandbox.

Install in a Production Environment

Install where you or your users work, including developer orgs.

Install in Production

Install in a Sandbox

Test in a copy of a production org.

Install in Sandbox

Cancel

Upload, download, access and share files from within Salesforce.

Makes files stored in any on-premise, public or hybrid cloud available within Salesforce.

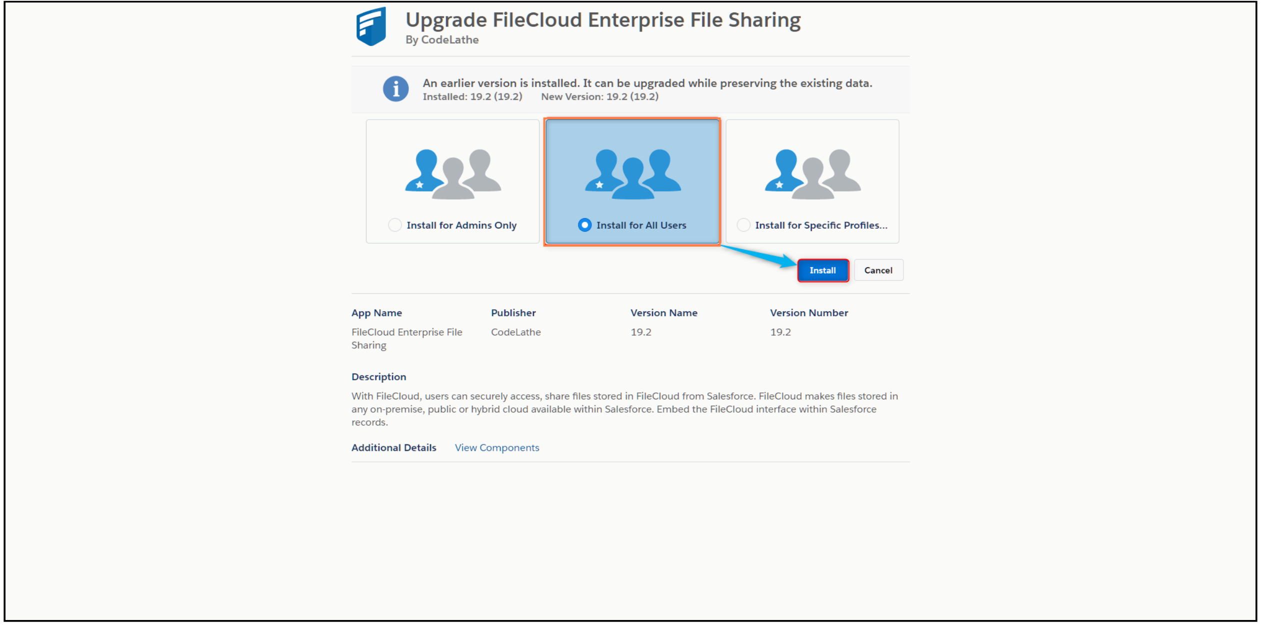
Powerful, seamless file collaboration across internal and external users.

To be effective in selling, teams typically need access to sales collateral (Presentations, whitepaper, brochures, contracts). Often these collaterals are stored across multiple storage systems: on-premise, public or hybrid cloud. Using FileCloud, companies can integrate their salesforce account with files stored in on-premise file servers or cloud storage. Using FileCloud, sales teams can access and collaborate more effectively on sales content without ever leaving Salesforce.

Key benefits:

- Upload, download, access and share remote files from within Salesforce
- Files can be stored in on-premise or public cloud (Amazon AWS, Microsoft Azure) can be accessed 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 along with file permission

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



Upgrade FileCloud Enterprise File Sharing

By CodeLathe

An earlier version is installed. It can be upgraded while preserving the existing data.

Installed: 19.2 (19.2)     New Version: 19.2 (19.2)

○ Install for Admins Only

● Install for All Users

○ Install for Specific Profiles...

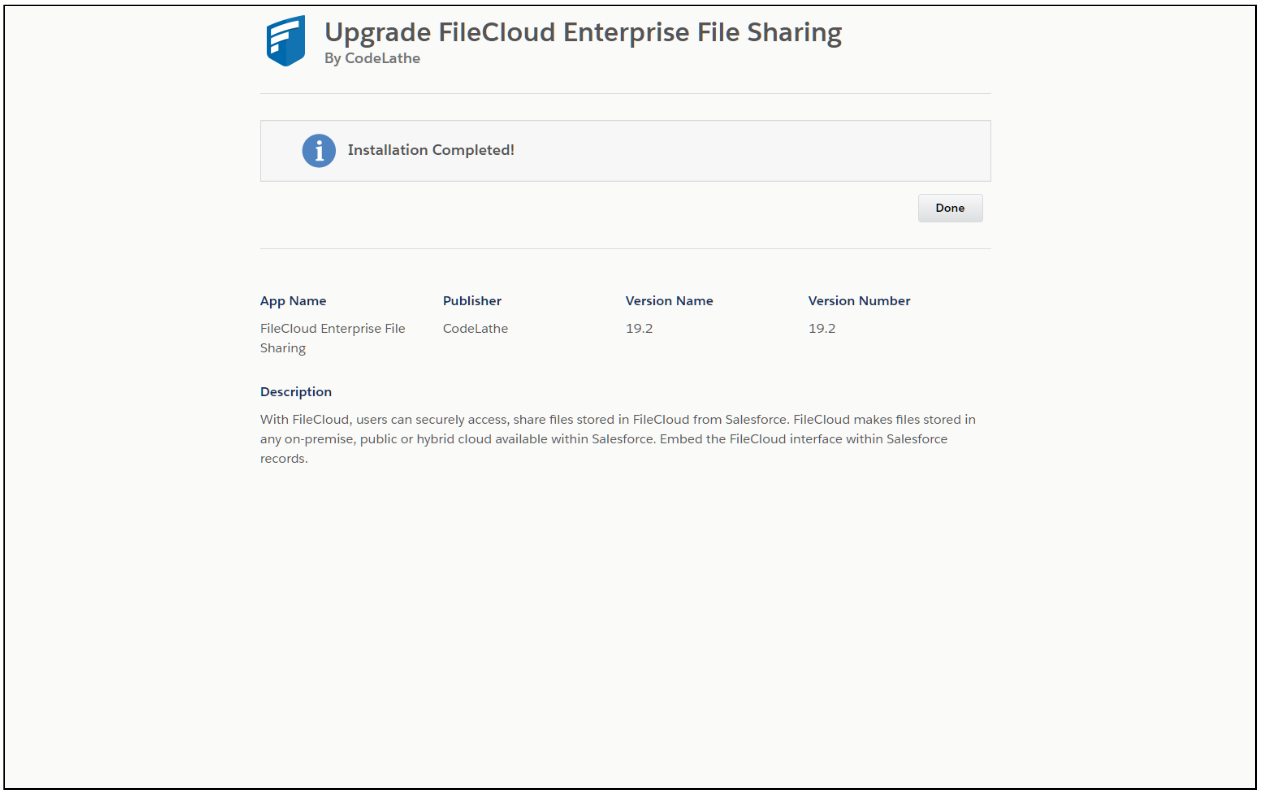
Install  Cancel

| 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.

Additional Details    View Components



Upgrade FileCloud Enterprise File Sharing

By CodeLathe

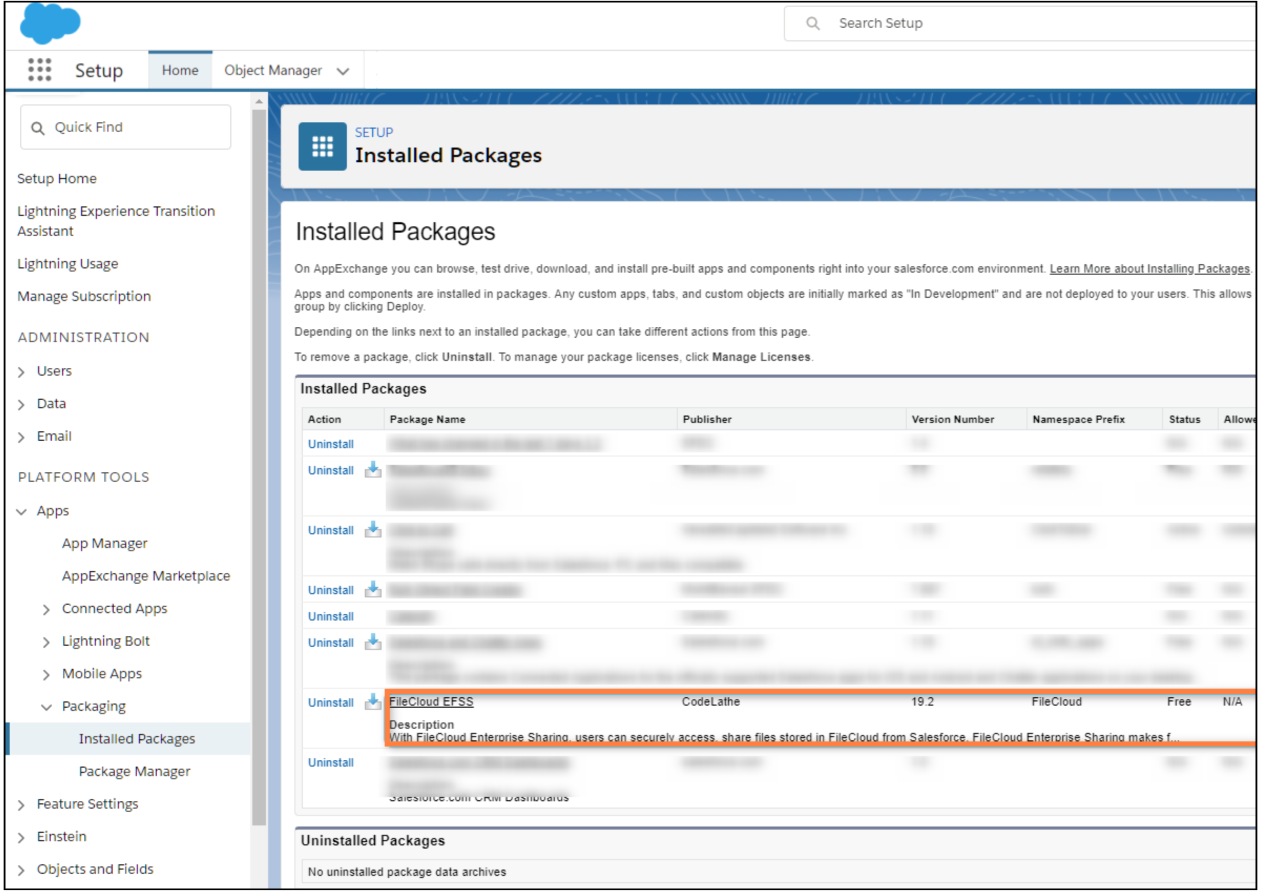
Installation Completed!

| 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**.



Installed Packages

On AppExchange you can browse, test drive, download, and install pre-built apps and components right into your salesforce.com environment. Learn More about Installing Packages.

Apps and components are installed in packages. Any custom apps, tabs, and custom objects are initially marked as "In Development" and are not deployed to your users. This allows group by clicking Deploy.

Depending on the links next to an installed package, you can take different actions from this page.

To remove a package, click **Uninstall**. To manage your package licenses, click **Manage Licenses**.

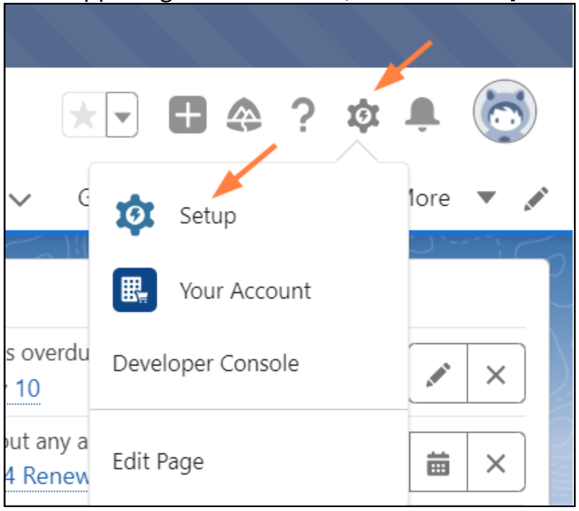
Installed Packages

| Action | Package Name | Publisher | Version Number | Namespace Prefix | Status | Allowe |
|---|---|---|---|---|---|---|
| Uninstall | [redacted] | [redacted] | [redacted] |  | [redacted] | [redacted] |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Uninstall | [redacted] | [redacted] | [redacted] |  | [redacted] | [redacted] |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Uninstall | FileCloud EFSS<br>Description<br>With FileCloud Enterprise Sharing, users can securely access, share files stored in FileCloud from Salesforce. FileCloud Enterprise Sharing makes f... | CodeLathe | 19.2 | FileCloud | Free | N/A |
| Uninstall | [redacted] | [redacted] | [redacted] |  | [redacted] | [redacted] |

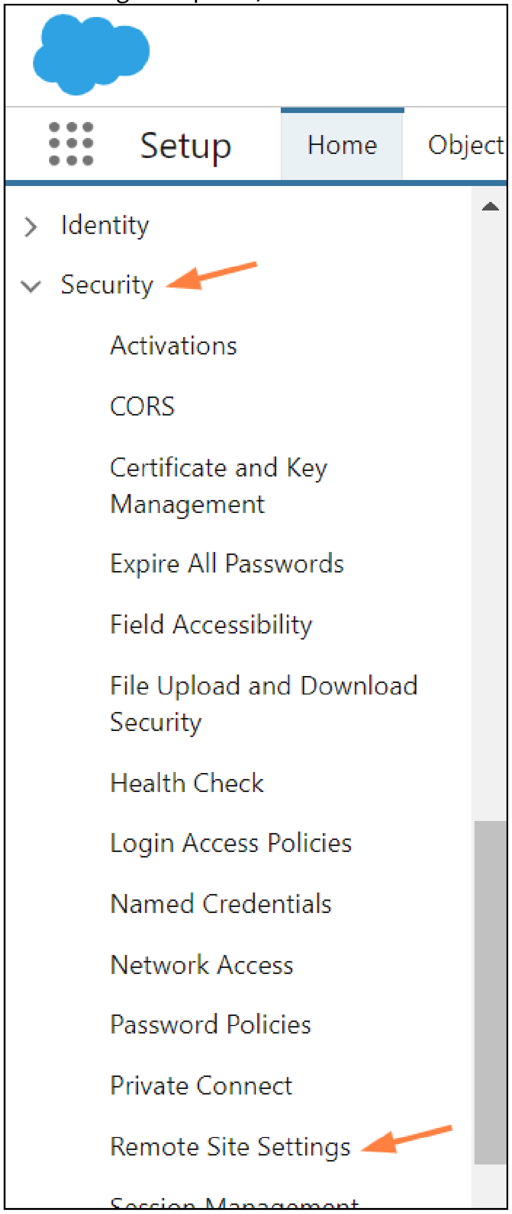
Uninstalled Packages

No uninstalled package data archives

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

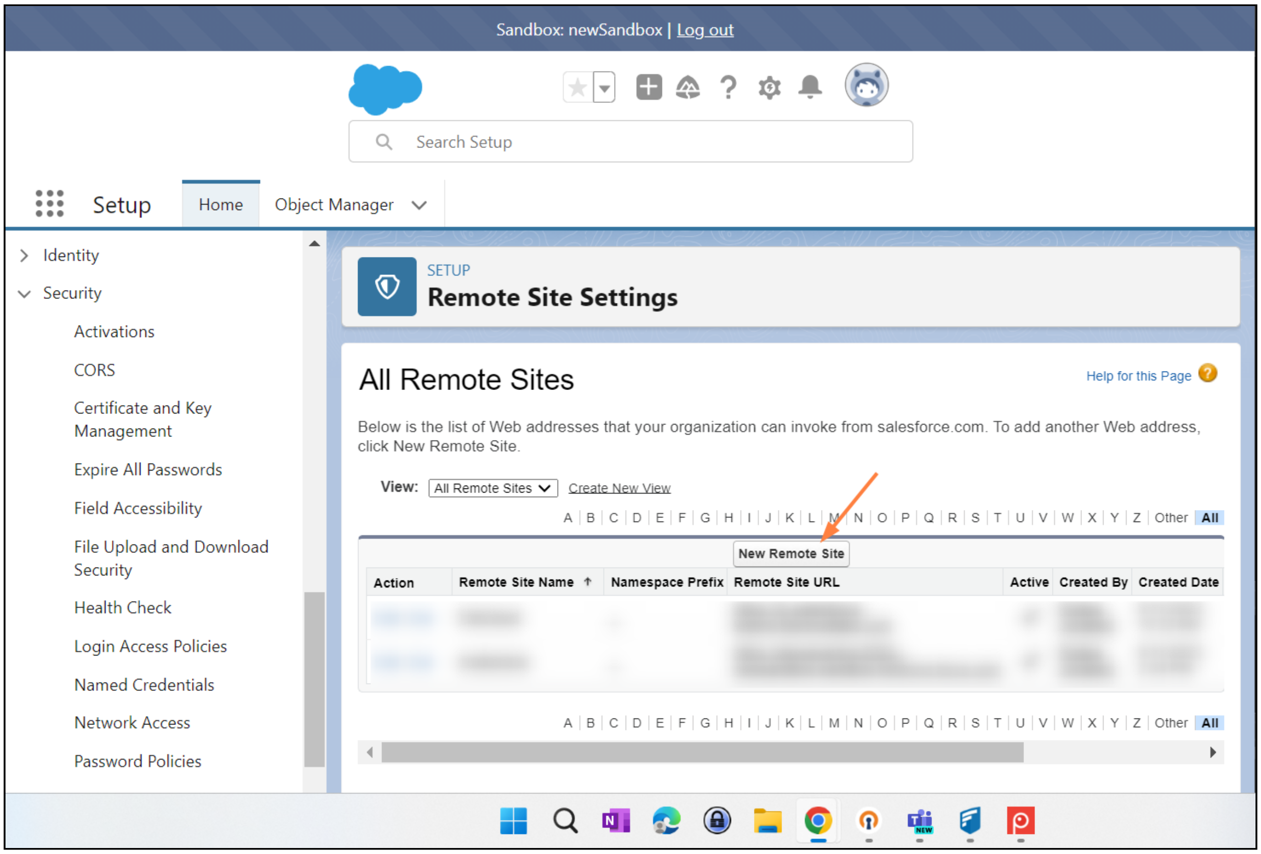


6. In the navigation panel, scroll down to **Security** and expand it. Click **Remote Site Settings**.



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

7. Click **New Remote Site**.

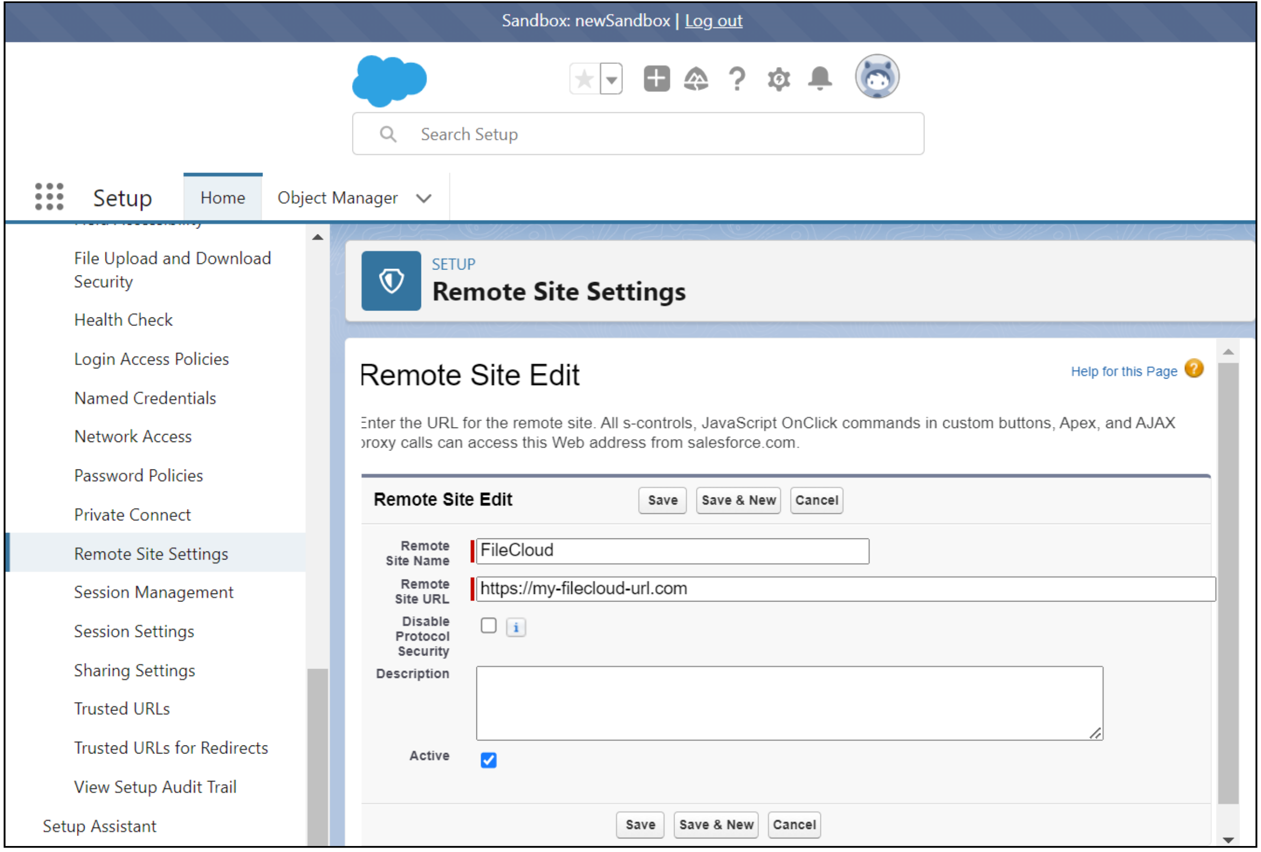


All Remote Sites

Below is the list of Web addresses that your organization can invoke from salesforce.com. To add another Web address, click New Remote Site.

| Action | Remote Site Name ↑ | Namespace Prefix | Remote Site URL | Active | Created By | Created Date |
|---|---|---|---|---|---|---|
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |

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



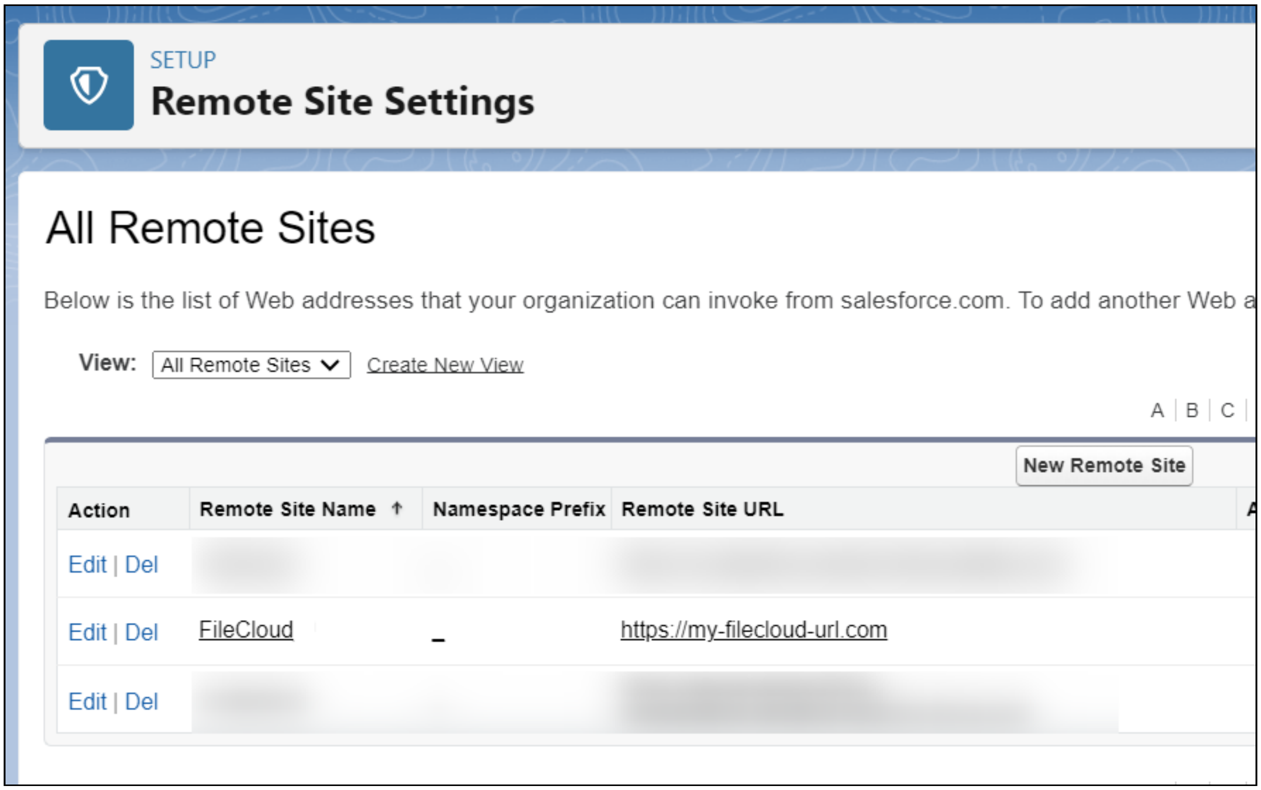
Remote Site Edit

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.

Remote Site Edit

| | |
|---|---|
| Remote Site Name | FileCloud |
| Remote Site URL | https://my-filecloud-url.com |
| Disable Protocol Security | □ |
| Description | |
| Active | ☑ |

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



## All Remote Sites

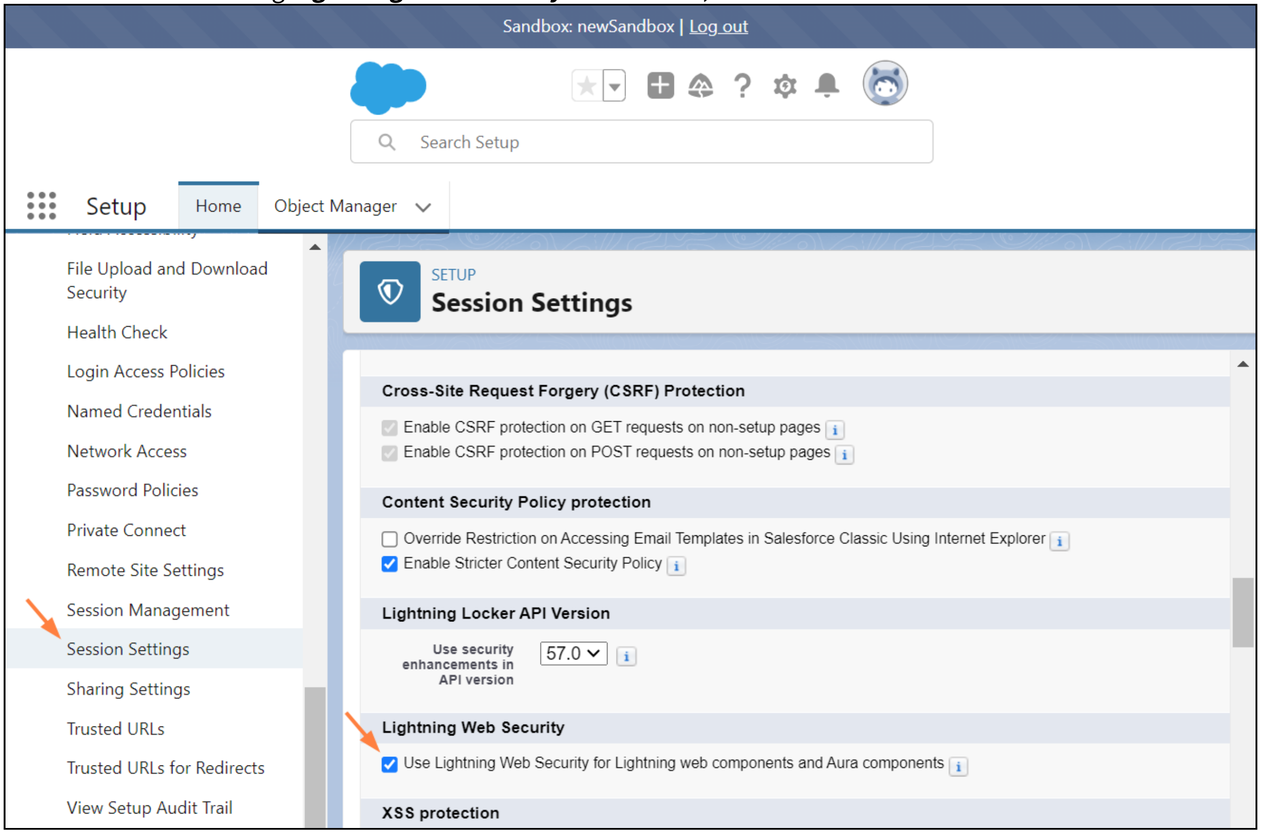
Below is the list of Web addresses that your organization can invoke from salesforce.com. To add another Web a

View: All Remote Sites Create New View

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

9. 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.



Cross-Site Request Forgery (CSRF) Protection

☑ Enable CSRF protection on GET requests on non-setup pages

☑ Enable CSRF protection on POST requests on non-setup pages

Content Security Policy protection

☐ Override Restriction on Accessing Email Templates in Salesforce Classic Using Internet Explorer

☑ Enable Stricter Content Security Policy

Lightning Locker API Version

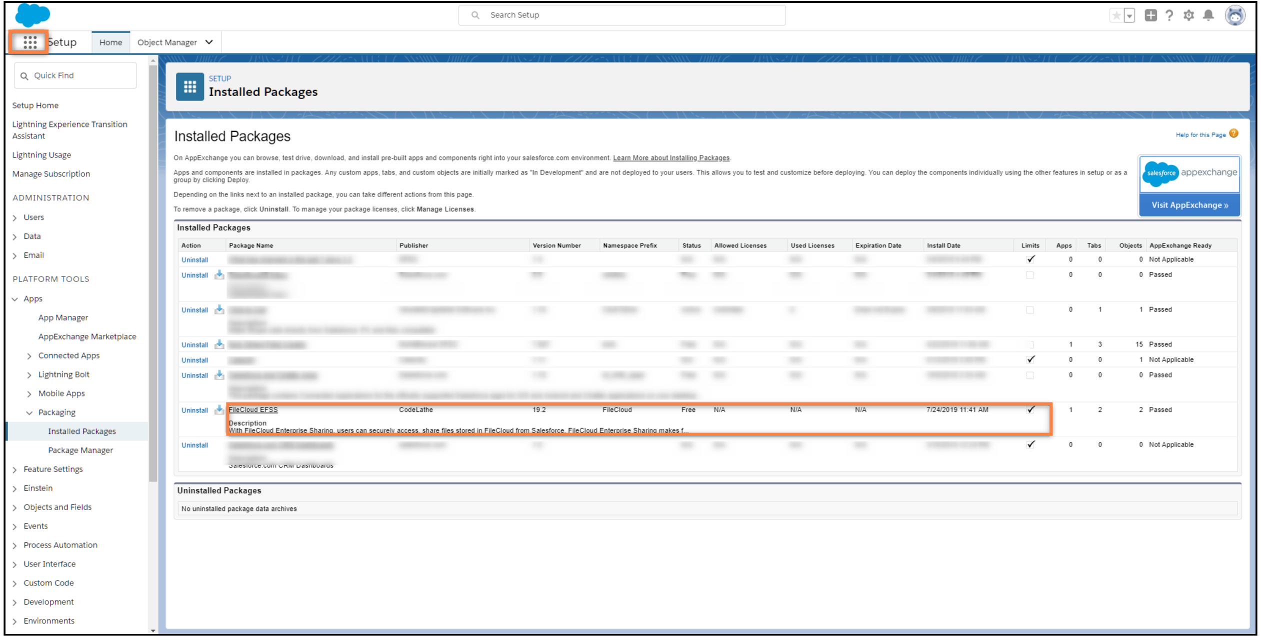
Use security enhancements in API version: 57.0

Lightning Web Security

☑ Use Lightning Web Security for Lightning web components and Aura components

XSS protection

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



Installed Packages

On AppExchange you can browse, test drive, download, and install pre-built apps and components right into your salesforce.com environment. Learn More about Installing Packages.

Apps and components are installed in packages. Any custom apps, tabs, and custom objects are initially marked as "In Development" and are not deployed to your users. This allows you to test and customize before deploying. You can deploy the components individually using the other features in setup or as a group by clicking Deploy.

Depending on the links next to an installed package, you can take different actions from this page.

To remove a package, click **Uninstall**. To manage your package licenses, click **Manage Licenses**.

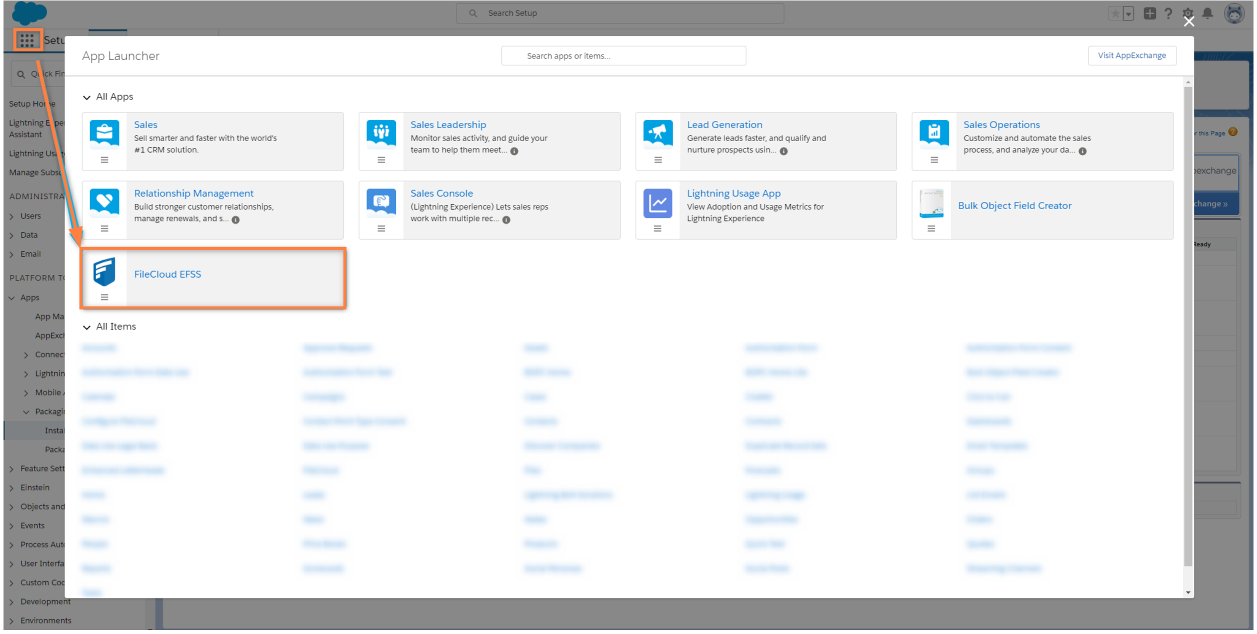
Installed Packages

| Action | Package Name | Publisher | Version Number | Namespace Prefix | Status | Allowed Licenses | Used Licenses | Expiration Date | Install Date | Limits | Apps | Tabs | Objects | AppExchange Ready |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Uninstall | [redacted] | [redacted] | [redacted] |  | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ✓ | 0 | 0 | 0 | Not Applicable |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ☐ | 0 | 0 | 0 | Passed |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ☐ | 0 | 1 | 1 | Passed |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ☐ | 1 | 3 | 15 | Passed |
| Uninstall | [redacted] | [redacted] | [redacted] |  | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ✓ | 0 | 0 | 1 | Not Applicable |
| Uninstall | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ☐ | 0 | 0 | 0 | Passed |
| Uninstall | FileCloud EFSS<br>Description<br>With FileCloud Enterprise Sharing, users can securely access, share files stored in FileCloud from Salesforce. FileCloud Enterprise Sharing makes f... | CodeLathe | 19.2 | FileCloud | Free | N/A | N/A | N/A | 7/24/2019 11:41 AM | ✓ | 1 | 2 | 2 | Passed |
| Uninstall | [redacted]<br>Salesforce.com CRM Dashboards | [redacted] | [redacted] |  | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | ✓ | 0 | 0 | 0 | Not Applicable |

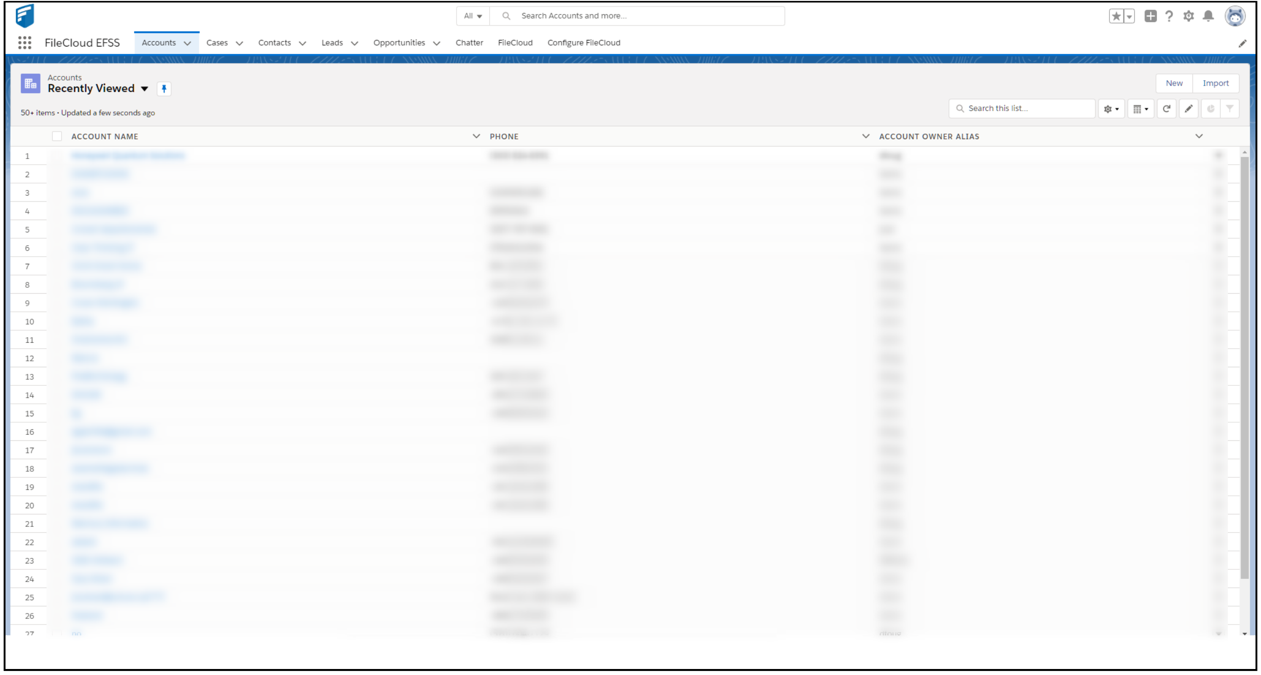
Uninstalled Packages

No uninstalled package data archives

12. From the App Launcher, click FileCloud EFSS.


Search Setup
App Launcher
Search apps or items...
Visit AppExchange
All Apps
Sales
Sell smarter and faster with the world's #1 CRM solution.
Sales Leadership
Monitor sales activity, and guide your team to help them meet...
Lead Generation
Generate leads faster, and qualify and nurture prospects usin...
Sales Operations
Customize and automate the sales process, and analyze your da...
Relationship Management
Build stronger customer relationships, manage renewals, and s...
Sales Console
(Lightning Experience) Lets sales reps work with multiple rec...
Lightning Usage App
View Adoption and Usage Metrics for Lightning Experience
Bulk Object Field Creator
FileCloud EFSS
All Items

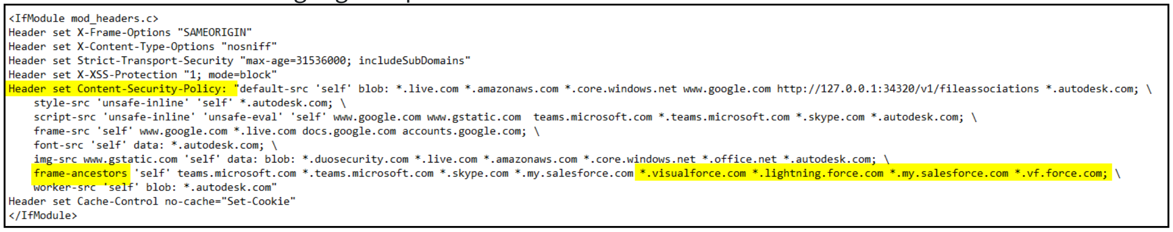
Installation is complete.



## Configuring FileCloud with Salesforce

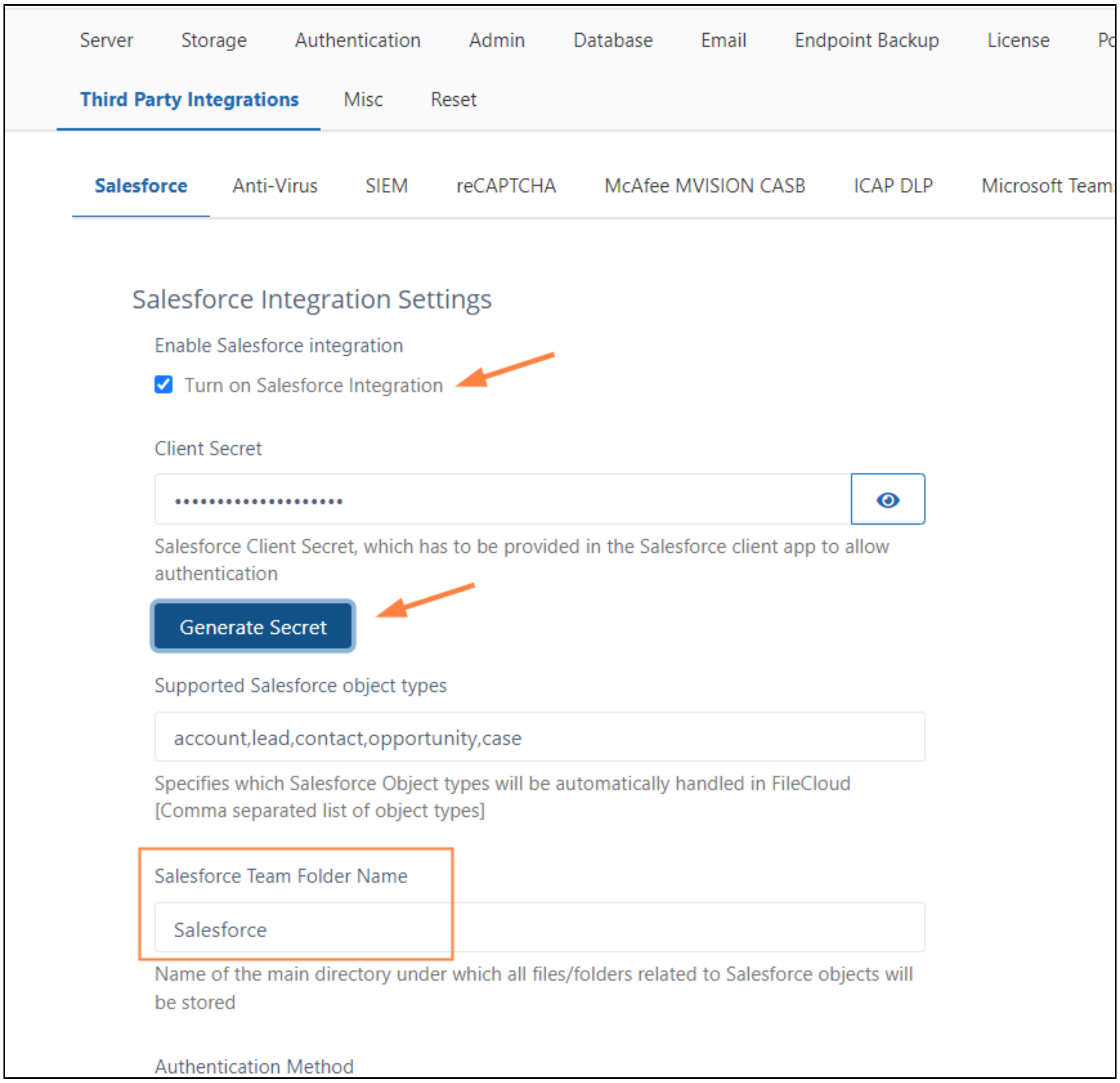
After you install/integrate FileCloud with Salesforce, complete the following:

1. Edit the **.htaccess** file.
    a. Windows: go to **C:\xampp\htdocs**
    Linux: go to: **/var/www/html/config**
    b. Open the file **.htaccess**
    c. Locate **Header set Content-Security-Policy** and in the list following **frame-ancestors**, append ***.**visualforce.com ***.**lightning.force.com ***.**my.salesforce.com**, *.**vf.force.com**;**
    The edit is shown in the highlighted portion below:



```
<IfModule mod_headers.c>
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header set Content-Security-Policy: "default-src 'self' blob: *.live.com *.amazonaws.com *.core.windows.net www.google.com http://127.0.0.1:34320/v1/fileassociations *.autodesk.com; \
    style-src 'unsafe-inline' 'self' *.autodesk.com; \
    script-src 'unsafe-inline' 'unsafe-eval' 'self' www.google.com www.gstatic.com  teams.microsoft.com *.teams.microsoft.com *.skype.com *.autodesk.com; \
    frame-src 'self' www.google.com *.live.com docs.google.com accounts.google.com; \
    font-src 'self' data: *.autodesk.com; \
    img-src www.gstatic.com 'self' data: blob: *.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net *.autodesk.com; \
    frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com *.my.salesforce.com *.visualforce.com *.lightning.force.com *.my.salesforce.com *.vf.force.com; \
    worker-src 'self' blob: *.autodesk.com"
Header set Cache-Control no-cache="Set-Cookie"
</IfModule>
```

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.)



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

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

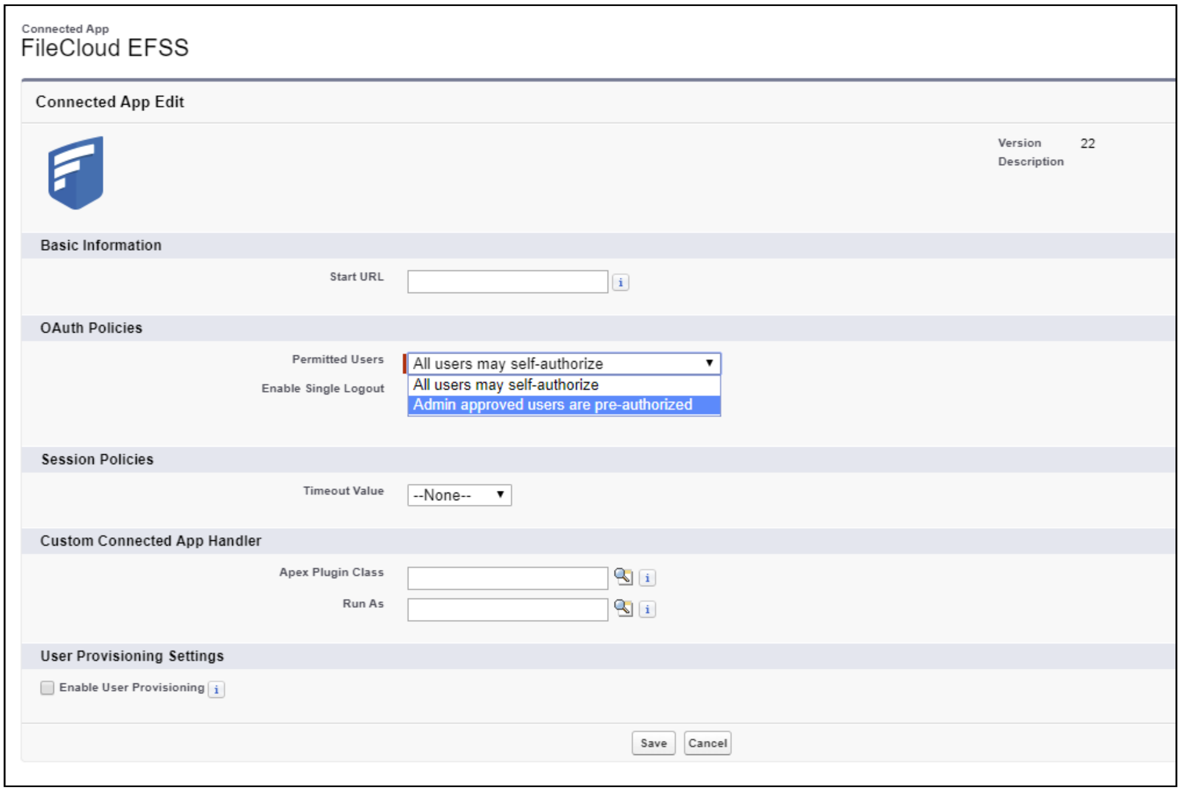
Salesforce

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

Authentication Method

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: All users may self-authorize

All users may self-authorize

Admin approved users are pre-authorized

Enable Single Logout

Session Policies

Timeout Value: --None--

Custom Connected App Handler

Apex Plugin Class

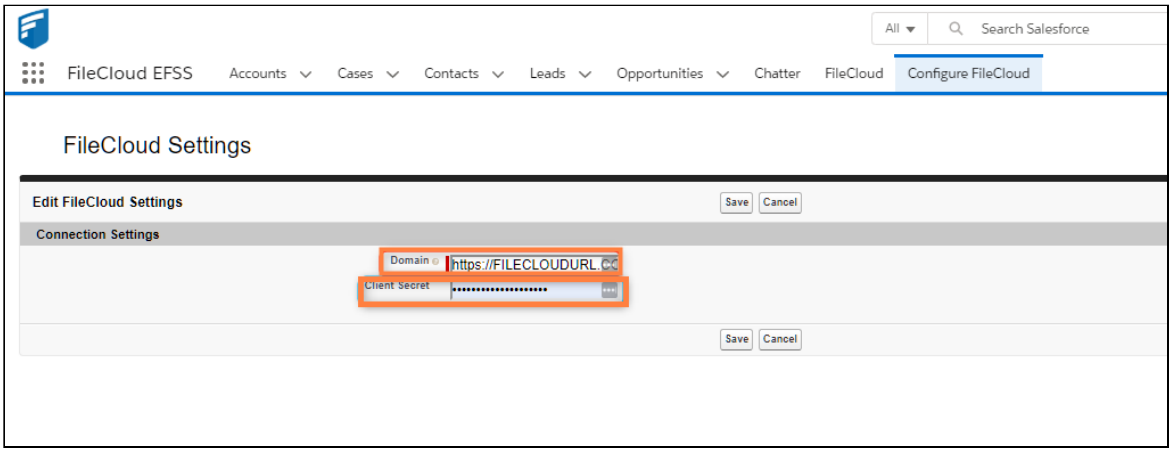
Run As

User Provisioning Settings

□ Enable User Provisioning

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 Settings

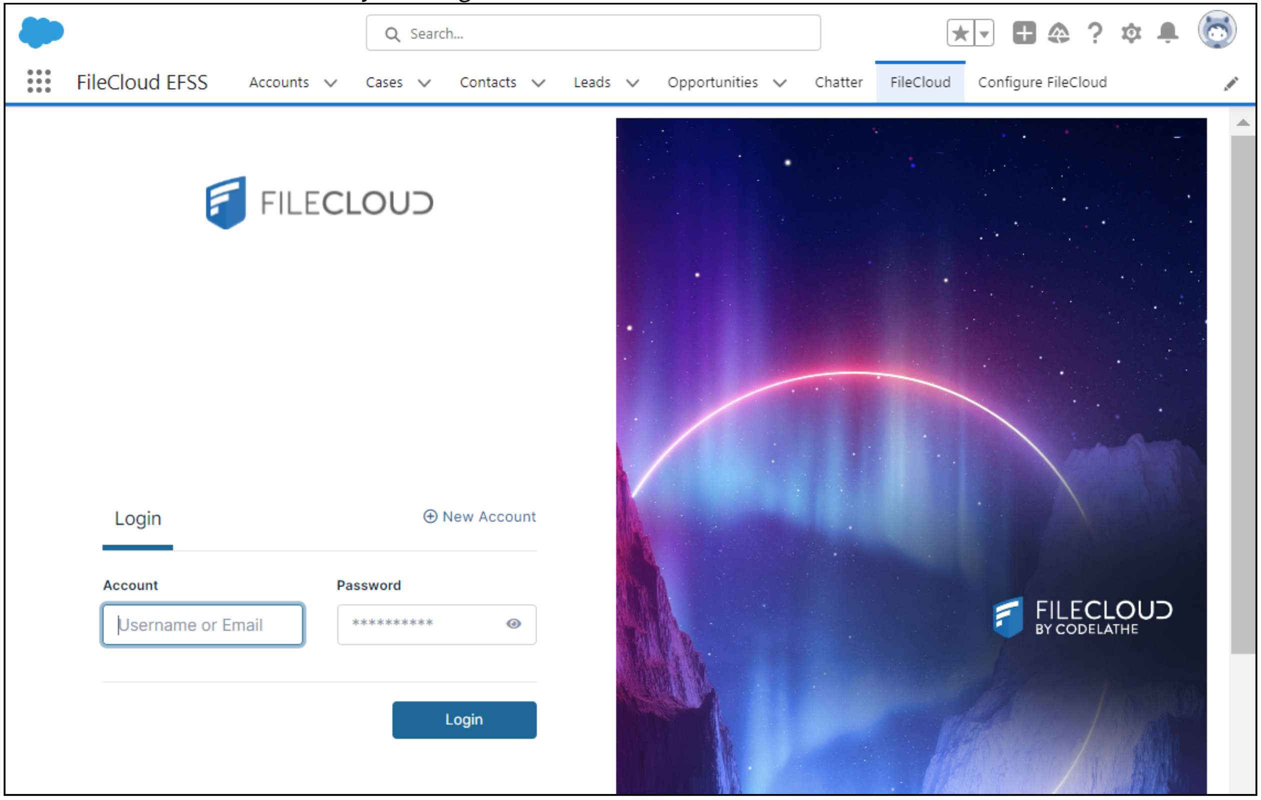
Edit FileCloud Settings

Connection Settings

Domain: https://FILECLOUDURL.CC

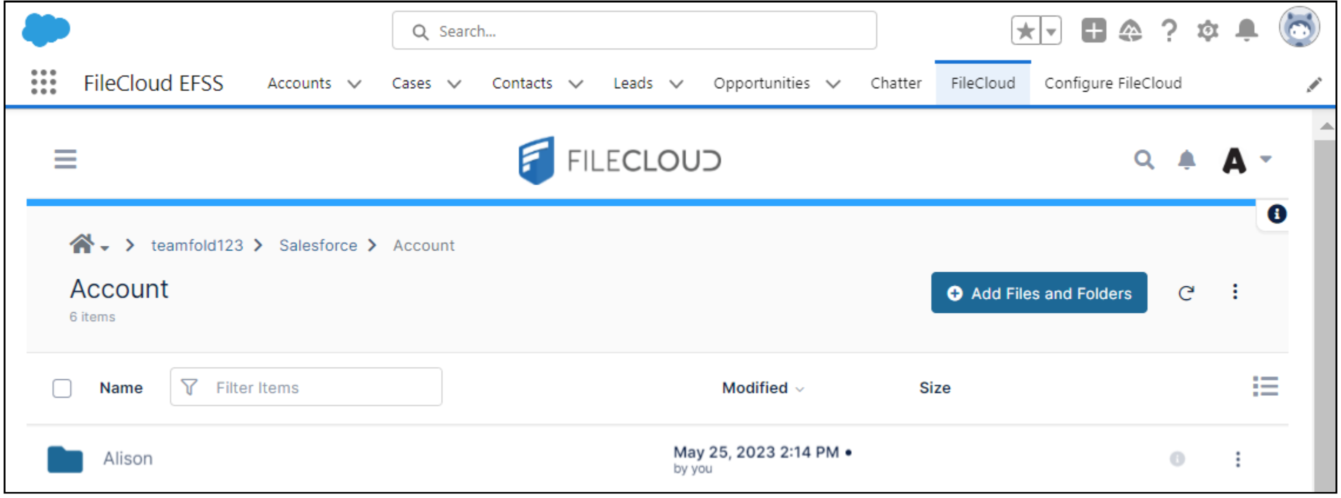
Client Secret: ••••••••••••••••••••

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



## Restricting Permissions on Salesforce Team Folders

Now that you have integrated FileCloud and Salesforce, when you create an object in Salesforce, a sub-folder in the Salesforce Team Folder in FileCloud is created for the object.



teamfold123 > Salesforce > Account

Account
6 items

| Name | Modified | Size |
|---|---|---|
| Alison | May 25, 2023 2:14 PM • by you | |

Since you may want more restrictive permissions on each object's folder when it is created, you can configure FileCloud to only enable the owner (creator) of the object and a group of users that you designate as managers to have access to the object folder.

**To configure more restrictive default permissions on Team Folders for Salesforce objects:**

1. If you have not already shared the Salesforce Team Folder with all FileCloud users or groups who may want to access an object sub-folder, give them access to the Salesforce Team Folder in FileCloud now.
2. Open the configuration file:
   Windows: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux: /var/www/config/cloudconfig.php
3. Add the following lines, listing the emails of users who you want to be able to access all Salesforce object folders in the second setting:

```
define('TONIDOCLOUD_SALESFORCE_RESTRICT_ACCESS_ENABLED', '1');
define('TONIDOCLOUD_SALESFORCE_MANAGER_USERS_EMAILS', ['email1@filecloud.com',
'email2@filecloud.com']);
```

4. Save your changes.
   **Note**: To turn off these restrictions, set TONIDOCLOUD_SALESFORCE_RESTRICT_ACCESS_ENABLED to 0.

# SIEM Integration

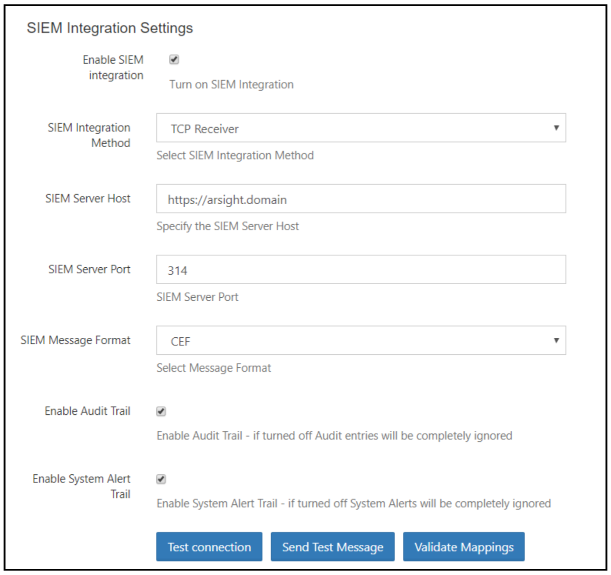
ⓘ **SIEM Integration**

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: TCP Receiver
Select SIEM Integration Method

SIEM Server Host: https://arsight.domain
Specify the SIEM Server Host

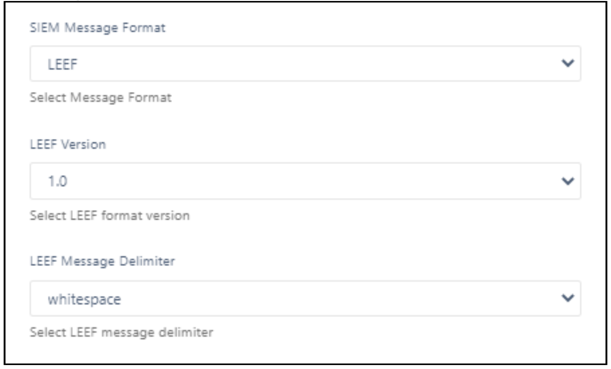
SIEM Server Port: 314
SIEM Server Port

SIEM Message Format: CEF
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

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: LEEF
Select Message Format

LEEF Version: 1.0
Select LEEF format version

LEEF Message Delimiter: whitespace
Select LEEF message delimiter

## 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*.

The following options are available:

| **Option** | **Description** |
|---|---|
| Enable SIEM Integration | Turns SIEM integration ON or OFF |

| Option | Description |
|---|---|
| SIEM Integration method | Specifies the SIEM Integration method. Following options are available:<br>▪ TCP Receiver - messages are sent to the specified SIEM server endpoint (host and port) via TCP socket connection<br>▪ UDP Receiver - messages are sent to the specified SIEM server endpoint (host and port) via UDP socket connection<br>▪ Syslog - messages are written directly to the Syslog, which can be imported by the SIEM server<br>**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:<br>▪ CEF - Common Event Format<br>▪ LEEF - Log Event Extended Format<br>NOTE: SIEM software provider should specify supported formats in the SIEM documentation. |
| LEEF Version (LEEF Format only) | Specifies the version of the LEEF format message. Available versions:<br>▪ 1.0<br>▪ 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.<br>**NOTE: All settings have to be saved first. Connection tests are based on the *currently* saved settings.** |

| 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.<br>**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. |

## Syslog Integration

In order to provide more flexibility, FileCloud allows admins to specify two important Syslog parameters - ident and facility. **Ident** specifies the name of the application logged in Syslog. **Facility** specifies where all FileCloud messages are sent and can be utilized by the system level Syslog configuration (e.g. in "rsyslog"). Both settings can be overridden in the *cloudconfig.php* configuration file by inputting the following settings:

- Ident - to specify ident value, add the following setting to *cloudconfig.php*

  ```
  define('TONIDOCLOUD_SIEM_SYSLOG_IDENT', 'IDENT_VALUE');
  ```

  If no value is provided, by default it will be set to 'SIEM'.
- Facility -to specify ident value please add the following setting: to the *cloudconfig.php*

  ```
  define('TONIDOCLOUD_SIEM_SYSLOG_FACILITY', LOG_LOCAL2);
  ```

  If no value is provided, by default it will be set to LOG_LOCAL5.  Below is a full list of supported values.

| | |
|---|---|
| `LOG_AUTH` | Security/authorization messages (use `LOG_AUTHPRIV` instead in systems where that constant is defined) |
| `LOG_AUTHPRIV` | Security/authorization messages (private) |
| `LOG_CRON` | Clock daemon (cron and at) |
| `LOG_DAEMON` | Other system daemons |
| `LOG_KERN` | Kernel messages |

| | |
|---|---|
| `LOG_LOCAL0` ... `LOG_LOCAL7` | Reserved for local use. These are not available in Windows |
| `LOG_LPR` | Line printer subsystem |
| `LOG_MAIL` | Mail subsystem |
| `LOG_NEWS` | USENET news subsystem |
| `LOG_SYSLOG` | Messages generated internally by syslogd |
| `LOG_USER` | Generic user-level messages |
| `LOG_UUCP` | UUCP subsystem |

LOG Values can also be seen in the official PHP documentation.

> ⚠ Please note that there are no quotation marks used for LOG values, as these have to be set to one of the PHP constants.

## Managing SIEM Mappings

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

**1. Accessing SIEM mappings files**

NOTE:

For this step you will need to access **WWWROOT.** It is typically located at:

| **Windows** | **Linux**<br>**(later than Ubuntu 14.04)** | **Linux**<br>**(earlier than Ubuntu 14.04)** |
|---|---|---|
| **c:\xampp\htdocs** | **/var/www/html** | **/var/www** |

Create and access SIEM mappings files:

Navigate to the following directory:

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

It contains the following files:

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

which store mapping samples for audit and system alerts respectively.

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

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

> ⓘ When you upgrade FileCloud, if you previously integrated with SIEM and already have auditmap.php and systemalertsmap.php files, you do not have to recreate or edit them unless you want to change existing mappings.

### SIEM mapping format:

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

**id** (Required) - identifies the SystemAlert/Audit entry this map refers to. **NOTE: It can be a string literal which 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 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 (TBD - add lists of properties)
- 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 as to contain the following four fields:

- eventClass - class of the event in the SIEM system.
- eventName - 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. user that performed the action, ip address of the request, etc.). The key can be any arbitrary string.

To allow a very flexible way to resolve those mappings value a special 'language' was created. Values can be provided in any of the following ways:

- As a literal value (i.e. string or number), i.e.

  **Sample System Alert Mappings**

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

- As a property biding that will resolve the value, based on the actual value provided by the FileCloud audit, system alert being processed:

  **Sample System Alert Mappings**

  ```
  'eventClass' => '$siemArea',
  'eventName' => '$description',
  'user' => '$username',
  'ip' => '$ip'
  ```

  Please check a full list of supported properties for more details. (TBD)

- As a method call:

  **Sample System Alert Mappings**

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

  NOTE: Users can create their own methods that can be utilized here. The first parameter is the PHP callback (class, method name) and the second parameter is the array of values (Optional) that will be 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 converts internal System Alerts severity into the 1-10 range required by SIEM integration in the following way:

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

Sample mappings:

System Alerts:

**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'
        ]
    ]
];
```

Audit:

```
//Report all audit events
$mappings[] = [
    'id' => '*',
    'prefilter' => [],
    'map' => [
        'eventClass' => '$operation',
        'eventName' => '$operation',
        'severity' => 2,
        'extension' => [
            'user' => '$userName',
            'userAgent' => '$userAgent',
            'ip' => '$ip',
            'notes' => '$notes'
        ]
    ]
];


//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'
        ]
    ]
];
```

# 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**<br>**(later than Ubuntu 14.04)** | **Linux**<br>**(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.

> 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.<br>The request can be mapped as a full object, and its info will be sent to the SIEM server as a string.<br>For example: `'request' => '$request'`, will be sent as `{"op":"loginguest","userid":"john.doe","password":"xxx"}`<br>Each field can also be sent individually if provided in the mapping: `'loggedUser' => '$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.<br>Each operation has a different response, so it is better to use this for dedicated rules.<br>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)**,<br>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)<br>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 |

| Property | Description | Values |
|---|---|---|
| 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:<br>▪ workflows<br>▪ 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:<br>▪ upload (file upload operation)<br>▪ 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:<br>▪ downloadfilemulti - Download multiple files<br>▪ downloadfile - Download single file<br>▪ getaudio - Play audio file<br>▪ getvideo - Play video file<br>▪ getfsslideimage - View image file<br>▪ docconvert - Open/view file<br>▪ quickshare - Quick share<br>▪ addusertoshare - Add specific users to share<br>▪ addgrouptoshare - Add specific groups to share<br>▪ 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:<br>SiemArea::INFECTED_FILE<br>SiemArea::INVALID_FILE_TYPE<br>SiemArea::AV_CHECK_FAILED<br>SiemArea::UNHANDLED_EXCEPTION<br>SiemArea::SYSTEM_ERROR<br>SiemArea::DISK_SPACE_EXCEEDED<br>SiemArea::INDEX_DB_FAILURE<br>SiemArea::RMC_INVALID_POLICY<br>SiemArea::SEND_EMAIL_FAILED<br>SiemArea::BACKGROUNDING_FAILED<br>SiemArea::METADATA_HEALTH_CHECK<br>SiemArea::WORKFLOW<br>SiemArea::ZIP_BACKUP_FAILURE<br>SiemArea::SIEM_SERVER_CONNECTION<br>SiemArea::DLP_SHARE_KILL |
| level | System alert critical level | One of the following values:<br>SysAlert::SYSALERT_LEVEL_MELTDOWN<br>SysAlert::SYSALERT_LEVEL_CRITICAL<br>SysAlert::SYSALERT_LEVEL_WARNING<br>SysAlert::SYSALERT_LEVEL_INFORMATION |

| Property | Description | Values |
|---|---|---|
| type | Type of system alert | One of the following values:<br>`SysAlert::SYSALERT_TYPE_DLP_SHARE_KILL_FAILED`<br>`SysAlert::SYSALERT_TYPE_DLP_SHARE_KILLED`<br>`SysAlert::SYSALERT_TYPE_CODE_CONFIGURATION_ERRROR`<br>`SysAlert::SYSALERT_TYPE_CODE_AV_FAILURE`<br>`SysAlert::SYSALERT_TYPE_CODE_SIGNATURE_FAILURE`<br>`SysAlert::SYSALERT_TYPE_CODE_EXCEPTION`<br>`SysAlert::SYSALERT_TYPE_CODE_ERROR`<br>`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.<br>For example:<br>**file** - filename for the File version deletion operation<br>**filePath** - file location for the Infected file<br>**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'
        ]
    ]
];
```

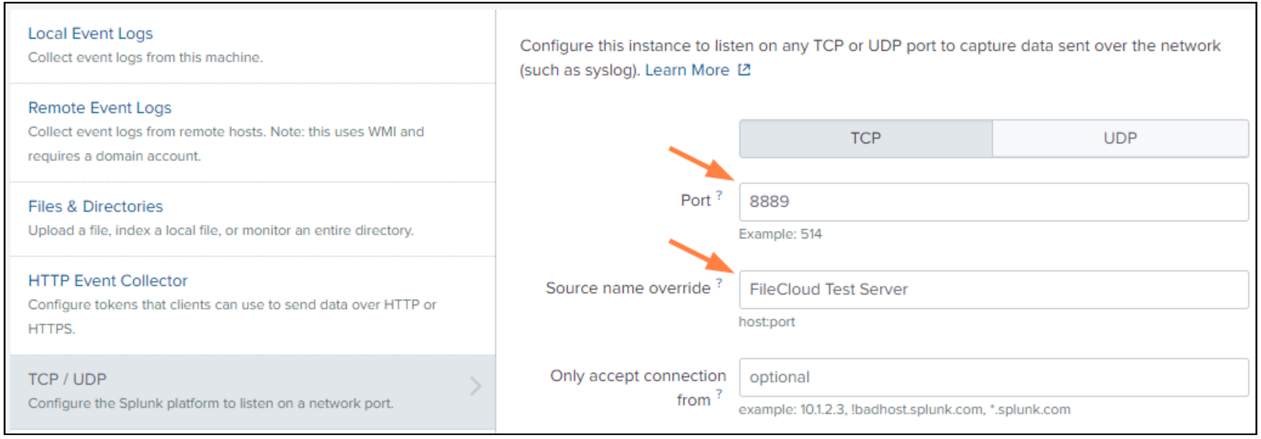
## SIEM Integration with Splunk Enterprise

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

TCP | UDP

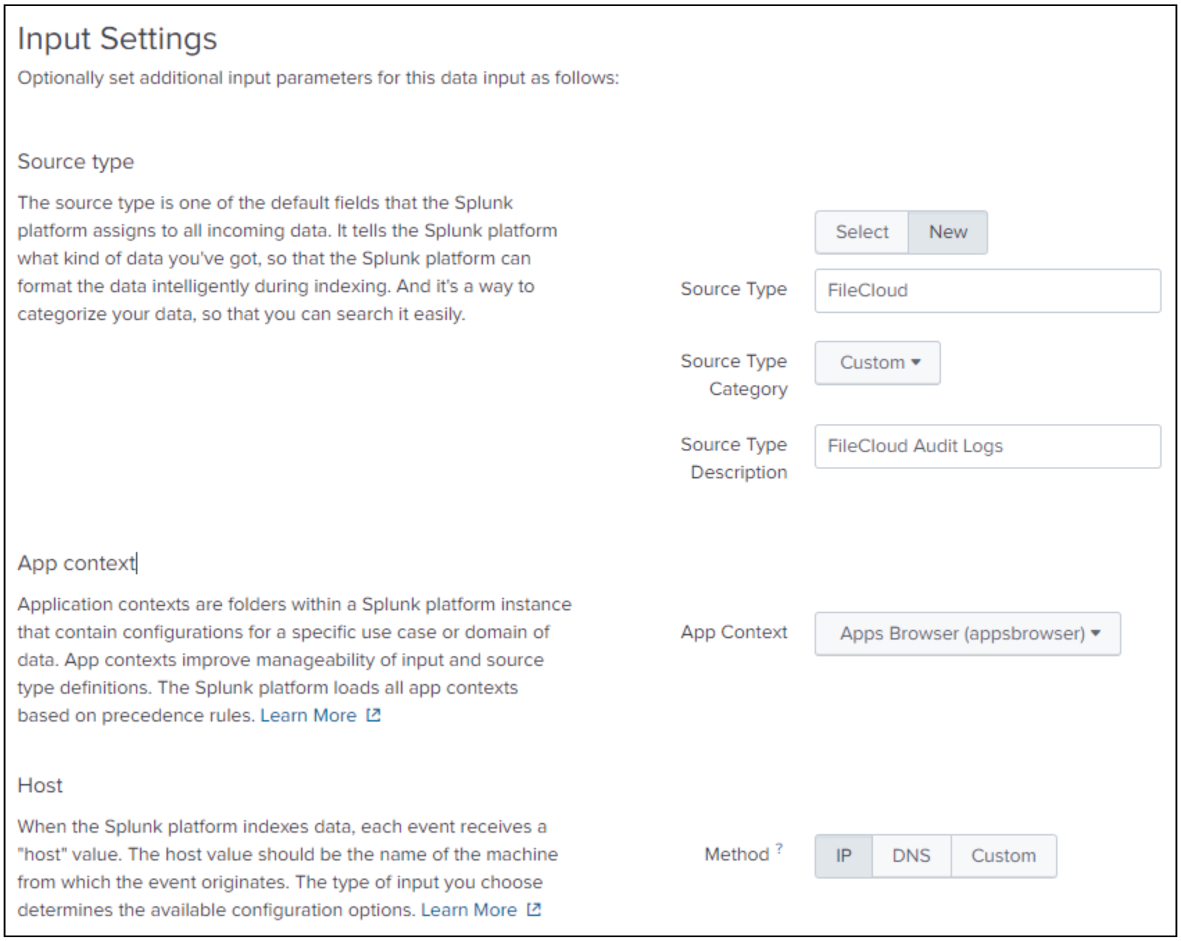
Port ? 8889
Example: 514

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

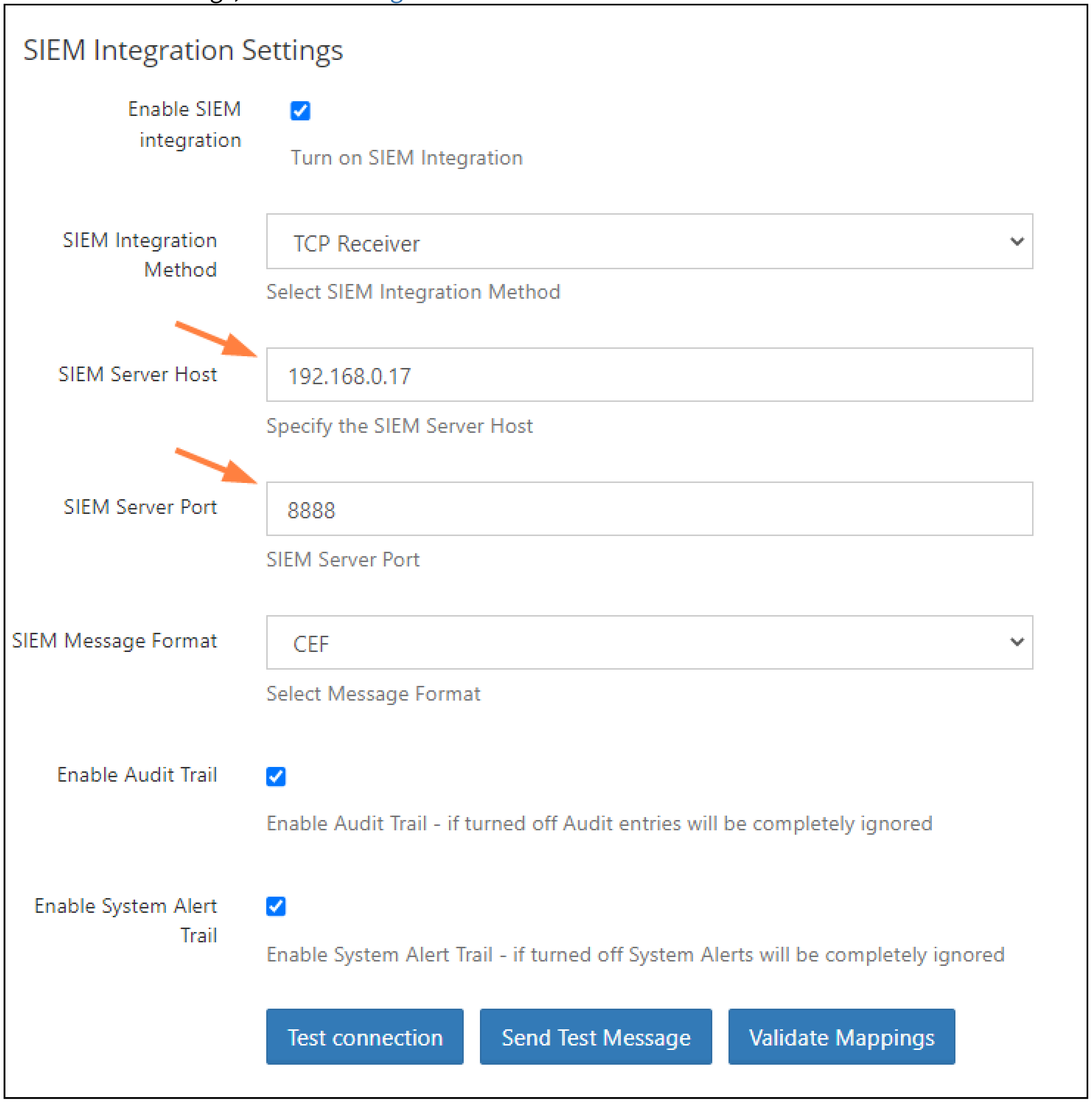
7. Go to the next screen in the wizard, **Review**, and check your settings.
8. Click next to complete your TCP Data Input entry configuration.

## 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: TCP Receiver
Select SIEM Integration Method

SIEM Server Host: 192.168.0.17
Specify the SIEM Server Host

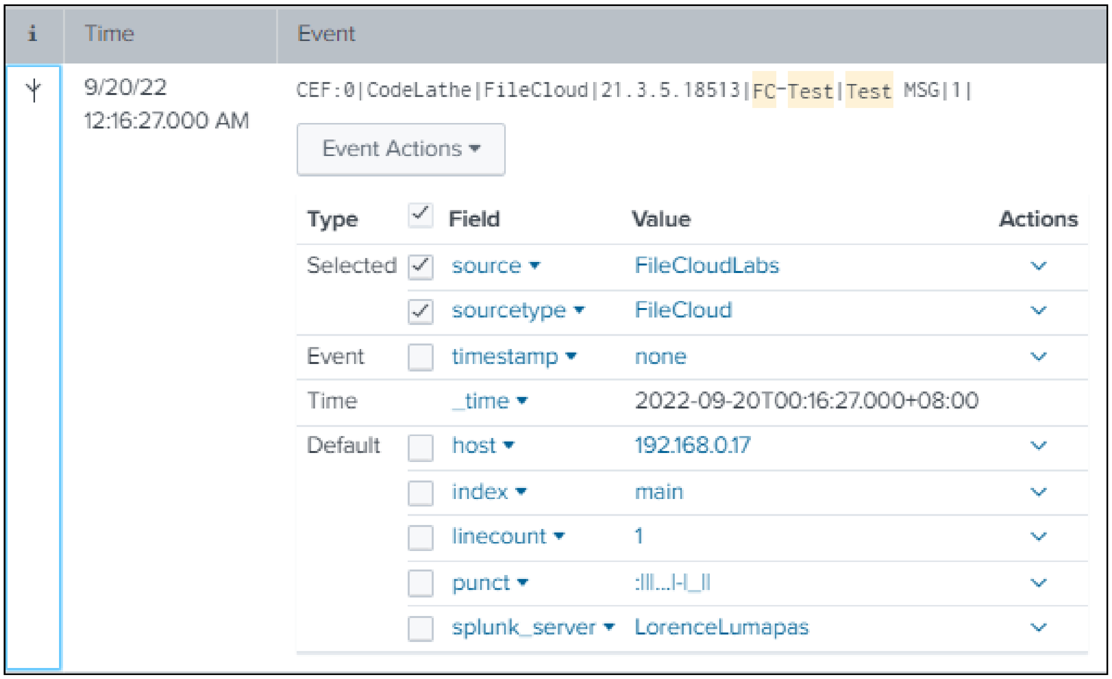
SIEM Server Port: 8888
SIEM Server Port

SIEM Message Format: CEF
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:



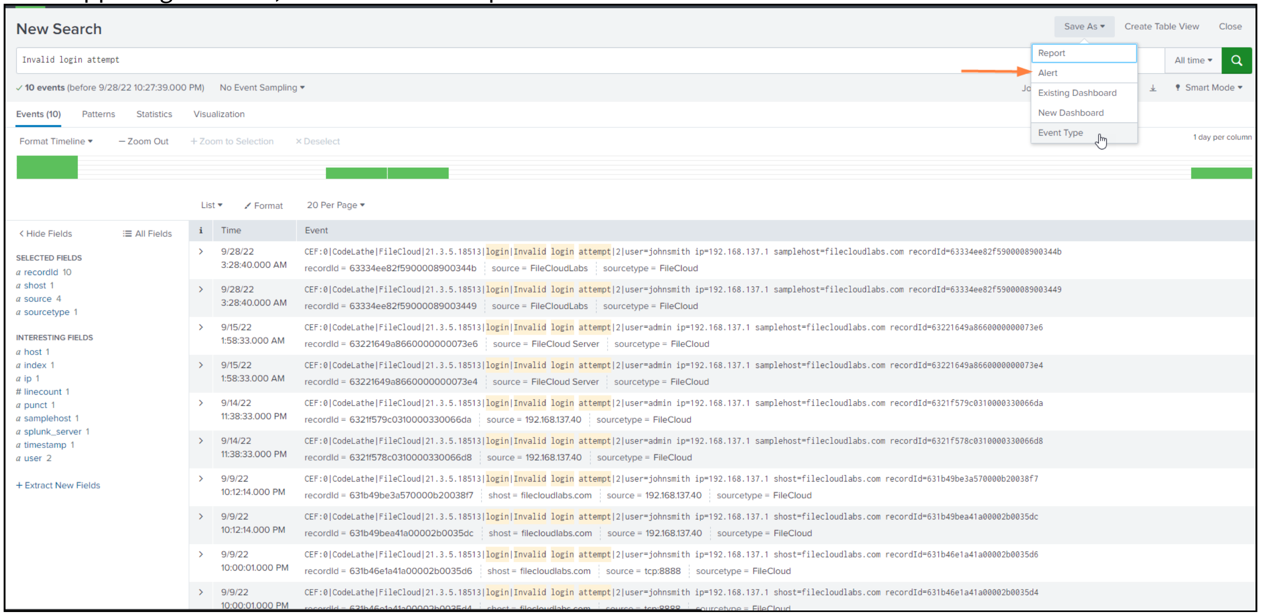
| i | Time | Event |
|---|---|---|
| ᛘ | 9/20/22<br>12:16:27.000 AM | CEF:0\|CodeLathe\|FileCloud\|21.3.5.18513\|FC-Test\|Test MSG\|1\| |

| 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 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) No Event Sampling ▾

SELECTED FIELDS
a recordId 10
a shost 1
a source 4
a sourcetype 1

INTERESTING FIELDS
a host 1
a index 1
a ip 1
# linecount 1
a punct 1
a samplehost 1
a splunk_server 1
a timestamp 1
a user 2

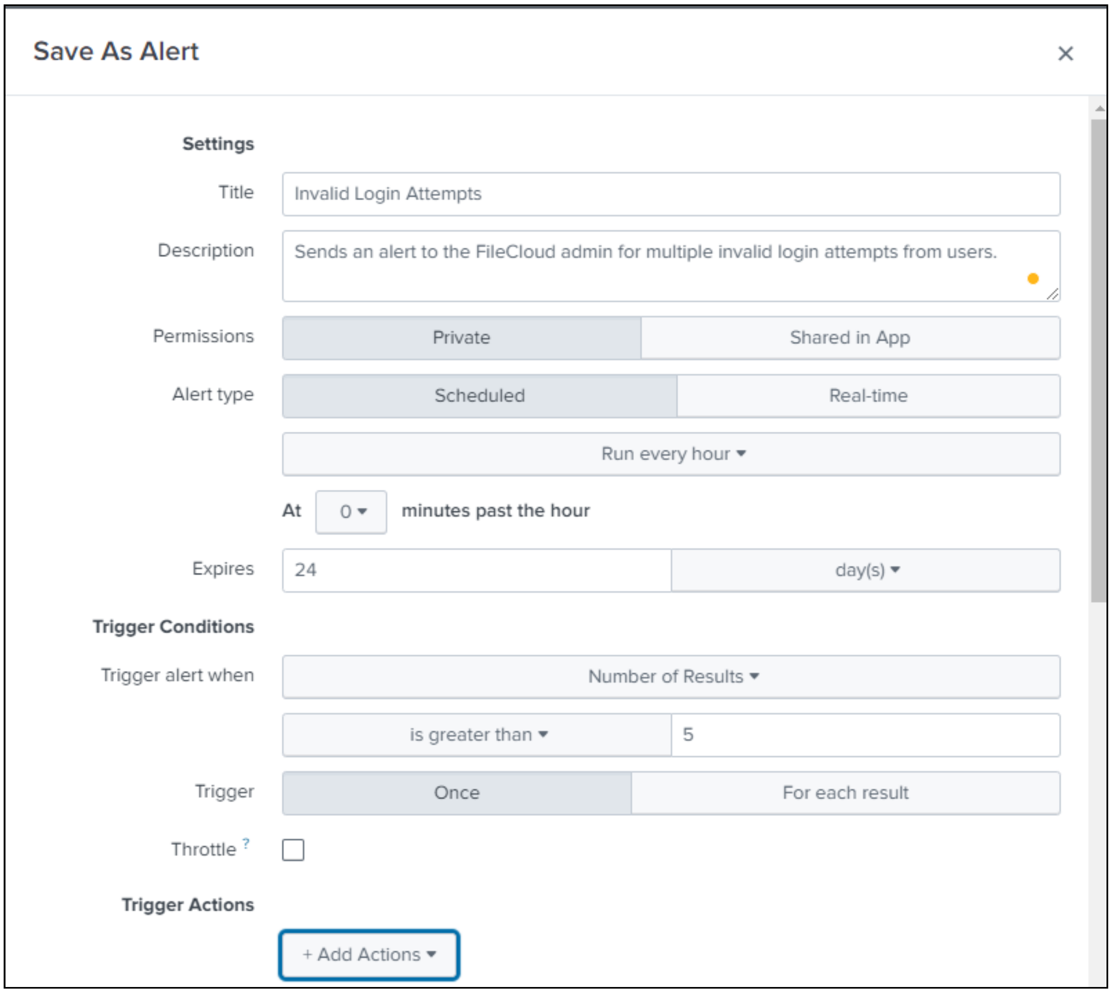
| i | Time | Event |
|---|---|---|
| > | 9/28/22<br>3:28:40.000 AM | CEF:0\|CodeLathe\|FileCloud\|21.3.5.18513\|login\|Invalid login attempt\|2\|user=johnsmith ip=192.168.137.1 samplehost=filecloudlabs.com recordId=63334ee82f5900008900344b<br>recordId = 63334ee82f5900008900344b  source = FileCloudLabs  sourcetype = FileCloud |
| > | 9/28/22<br>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<br>recordId = 63334ee82f59000089003449  source = FileCloudLabs  sourcetype = FileCloud |
| > | 9/15/22<br>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<br>recordId = 63221649a8660000000073e6  source = FileCloud Server  sourcetype = FileCloud |
| > | 9/15/22<br>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<br>recordId = 63221649a8660000000073e4  source = FileCloud Server  sourcetype = FileCloud |
| > | 9/14/22<br>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<br>recordId = 6321f579c0310000330066da  source = 192.168.137.40  sourcetype = FileCloud |
| > | 9/14/22<br>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<br>recordId = 6321f578c0310000330066d8  source = 192.168.137.40  sourcetype = FileCloud |
| > | 9/9/22<br>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<br>recordId = 631b49be3a570000b20038f7  shost = filecloudlabs.com  source = 192.168.137.40  sourcetype = FileCloud |
| > | 9/9/22<br>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<br>recordId = 631b49bea41a00002b0035dc  shost = filecloudlabs.com  source = 192.168.137.40  sourcetype = FileCloud |
| > | 9/9/22<br>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<br>recordId = 631b46e1a41a00002b0035d6  shost = filecloudlabs.com  source = tcp:8888  sourcetype = FileCloud |
| > | 9/9/22<br>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<br>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

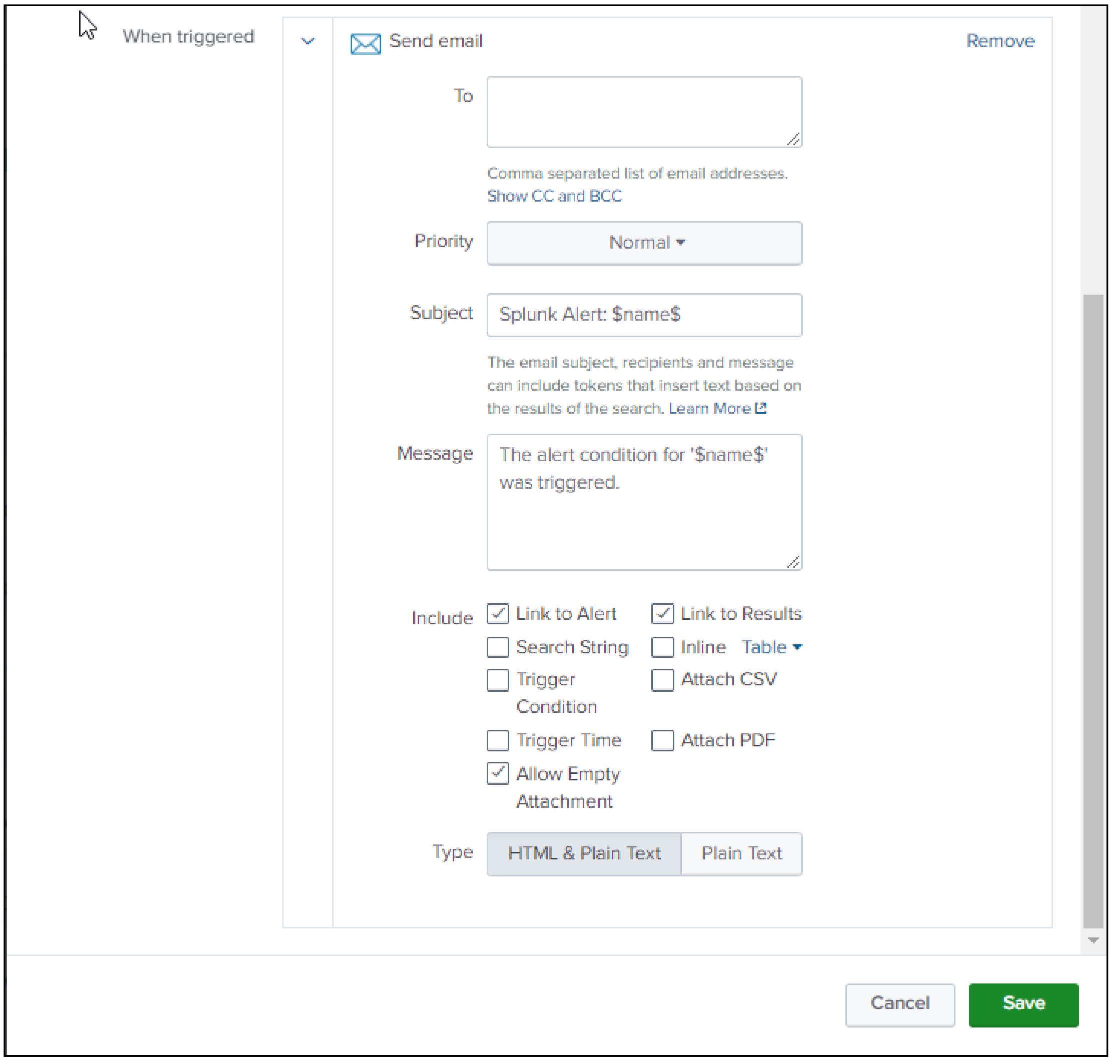
Trigger alert when: Number of Results

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: $name$

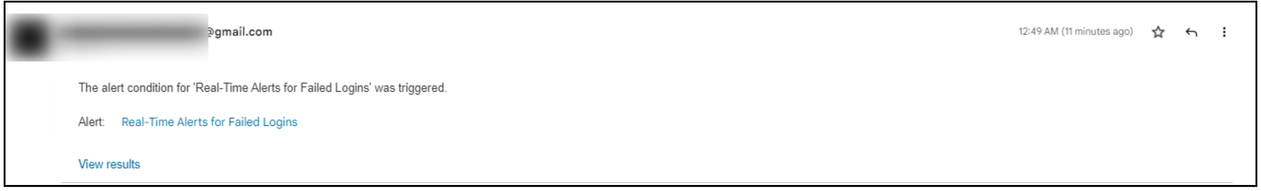
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

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

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

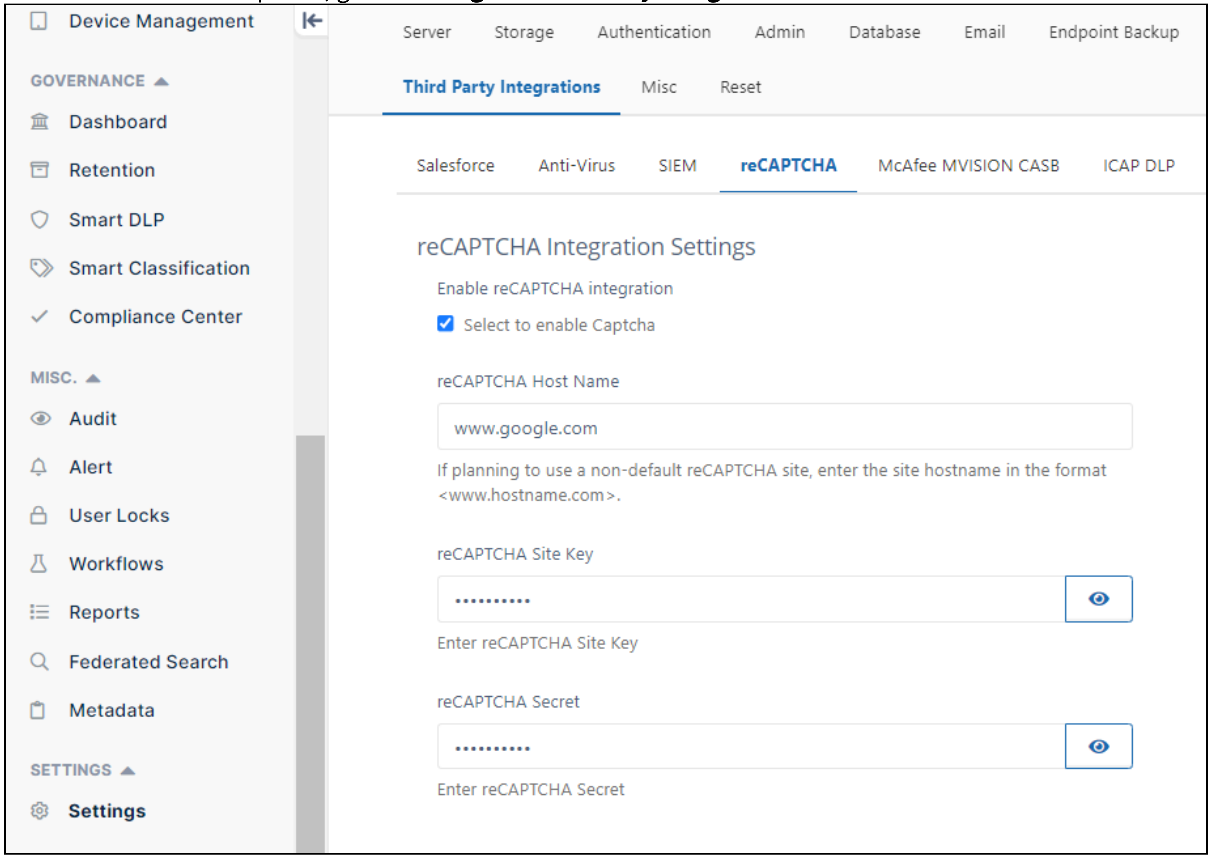
View results

# reCaptcha Settings

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**.



reCAPTCHA Integration Settings

Enable reCAPTCHA integration

☑ Select to enable Captcha

reCAPTCHA Host Name

www.google.com

If planning to use a non-default reCAPTCHA site, enter the site hostname in the format <www.hostname.com>.

reCAPTCHA Site Key

••••••••••

Enter reCAPTCHA Site Key

reCAPTCHA Secret

••••••••••

Enter reCAPTCHA Secret

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.

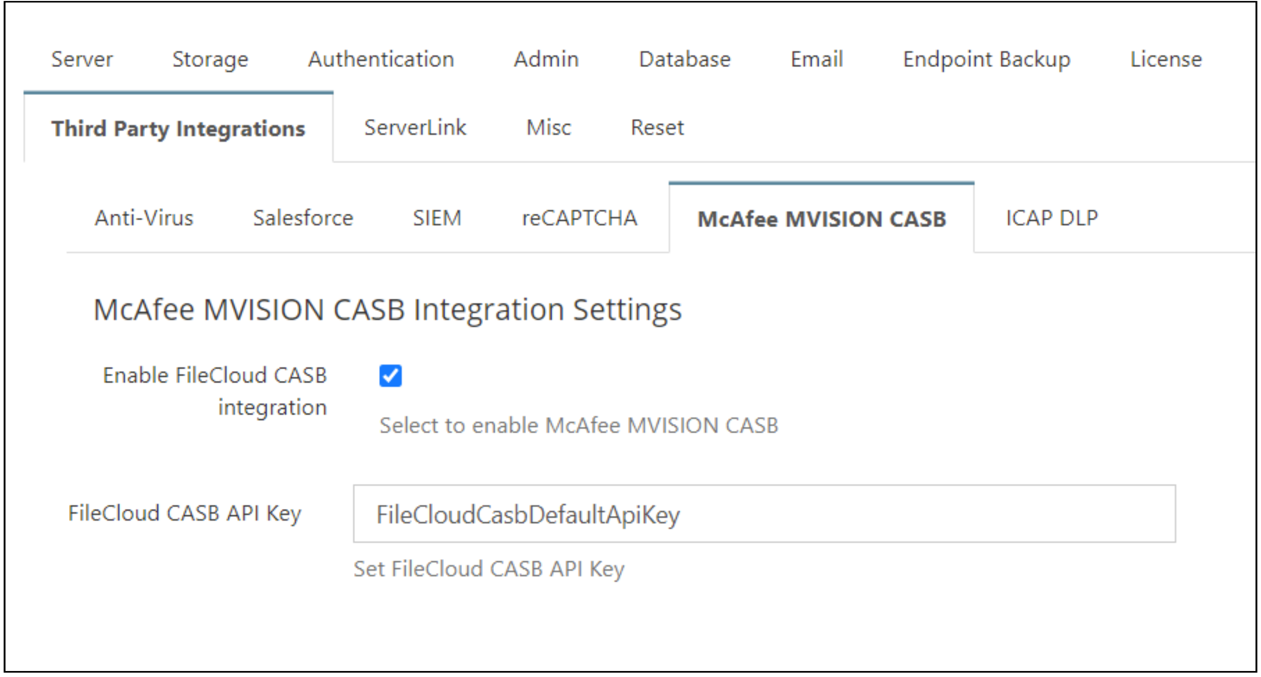
FileCloud includes a smart data leak prevention (DLP) functionality that monitors user actions and and prevents them if they pose a security risk.

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.



McAfee MVISION CASB Integration Settings

Enable FileCloud CASB integration ☑
Select to enable McAfee MVISION CASB

FileCloud CASB API Key: FileCloudCasbDefaultApiKey
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

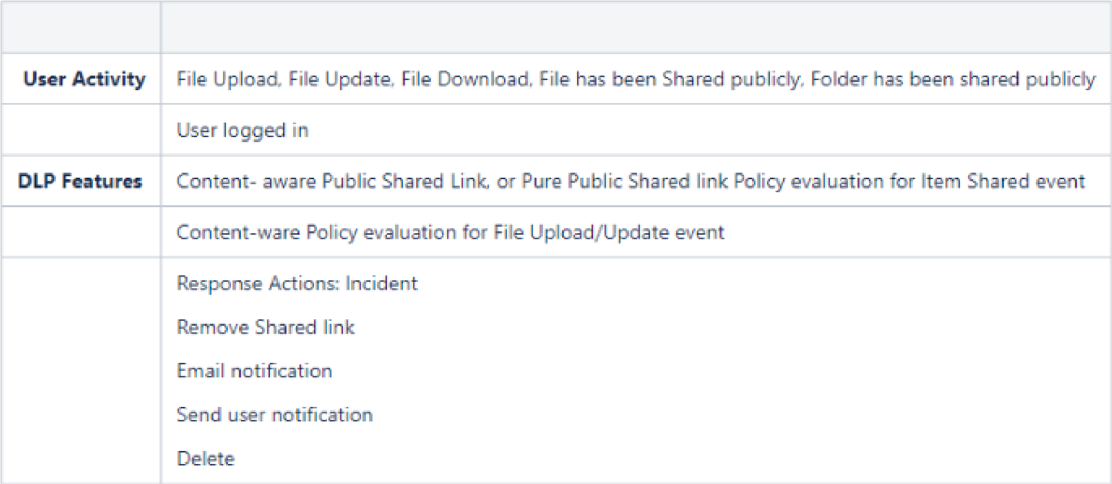
# McAfee CASB integration

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<br>Remove Shared link<br>Email notification<br>Send user notification<br>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.

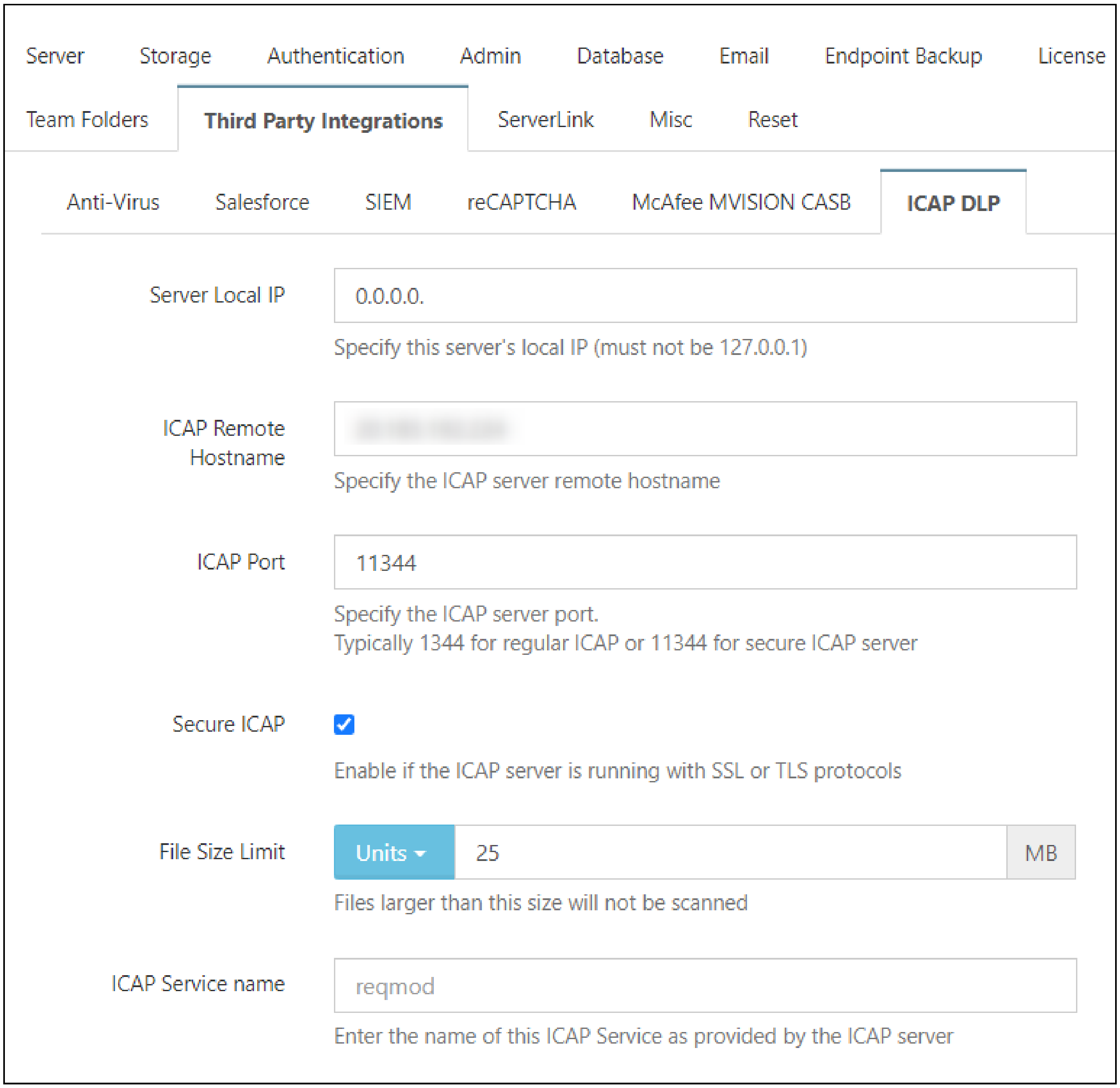
ICAP DLP has been added as a provider for FileCloud's content classification engine (CCE), enabling you set up a content classification rule that flags files for blocking or deletion by DLP rules. You must configure it as a third-party provider in FileCloud to use it with the CCE.

## 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 Local IP: 0.0.0.0.
Specify this server's local IP (must not be 127.0.0.1)

ICAP Remote Hostname: [redacted]
Specify the ICAP server remote hostname

ICAP Port: 11344
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: 25 MB
Files larger than this size will not be scanned

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

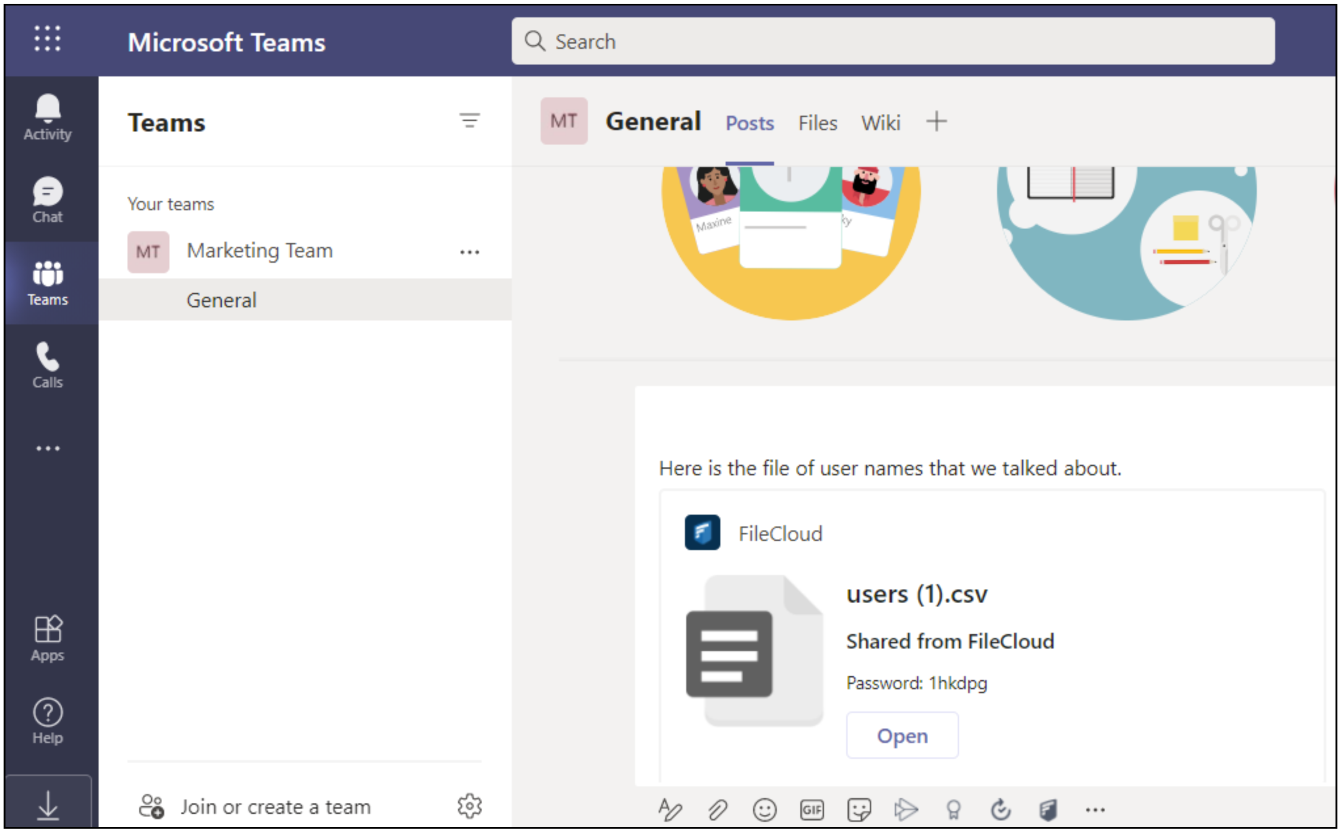
| Setting | Description |
|---|---|
| **Server Local IP** | In most cases, leave the default value of 0.0.0.0. If you are using a separate FileCloud policy with ICAP, enter the Private (LAN) IP of the FileCloud server. |
| **ICAP Remote Hostname** | Enter the hostname or IP of the system where the ICAP 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. |

| Setting | Description |
|---|---|
| **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.



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

users (1).csv

Shared from FileCloud

Password: 1hkdpg

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.

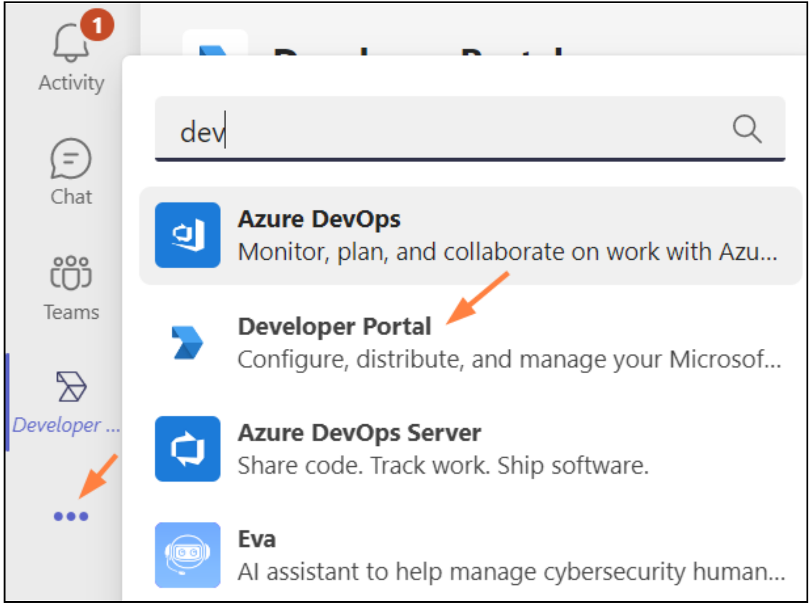
## For MS Teams Admins: Configuring FileCloud in Teams

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.

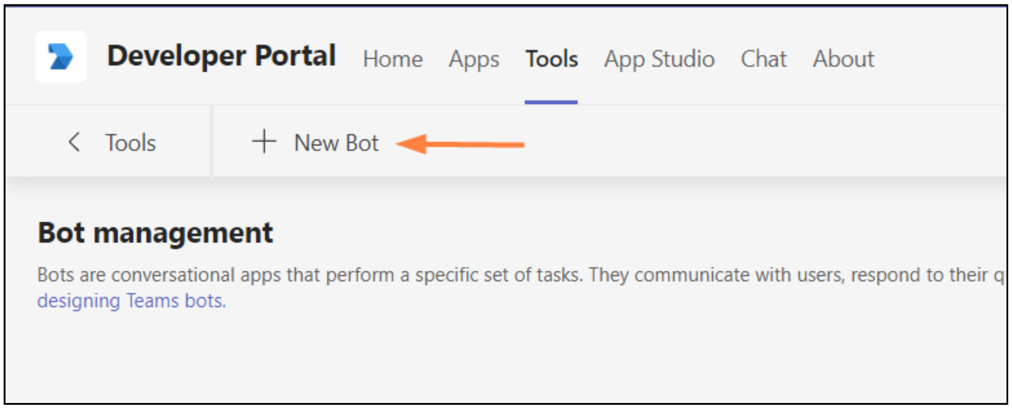
ⓘ FileCloud integration with MS Teams is available beginning in FileCloud Version 21.2

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.


1
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...

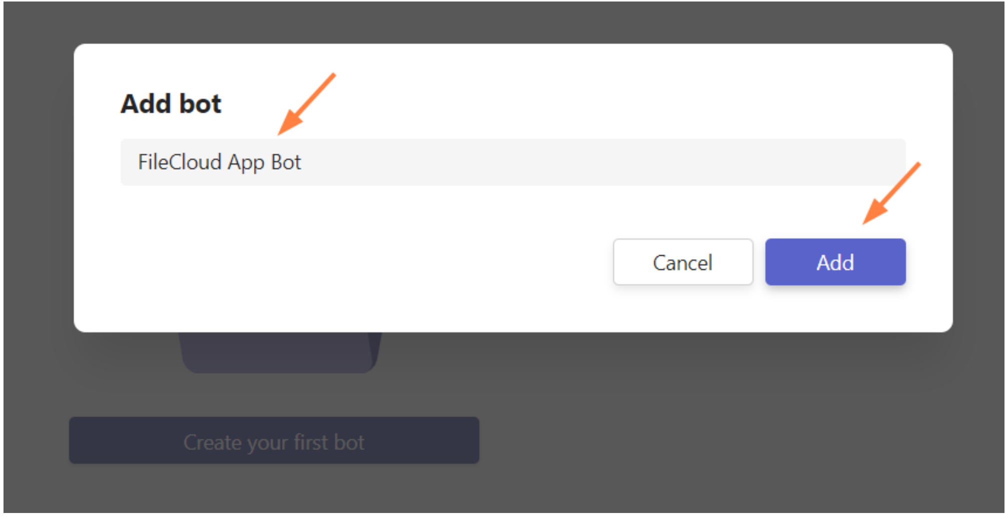
c. Click the **Developer Portal** icon in the navigation pane, and go to **Tools > Bot Management**.
d. Click **New Bot**.



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**.

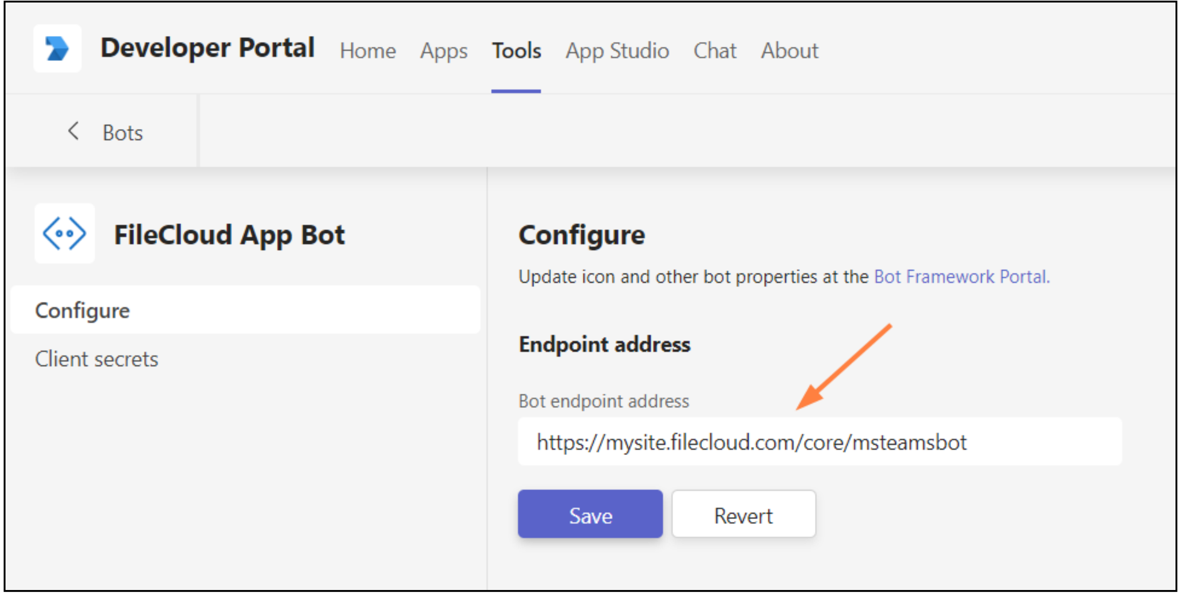


Add bot

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 **FileCloud server]/core/msteamsbot**



Configure

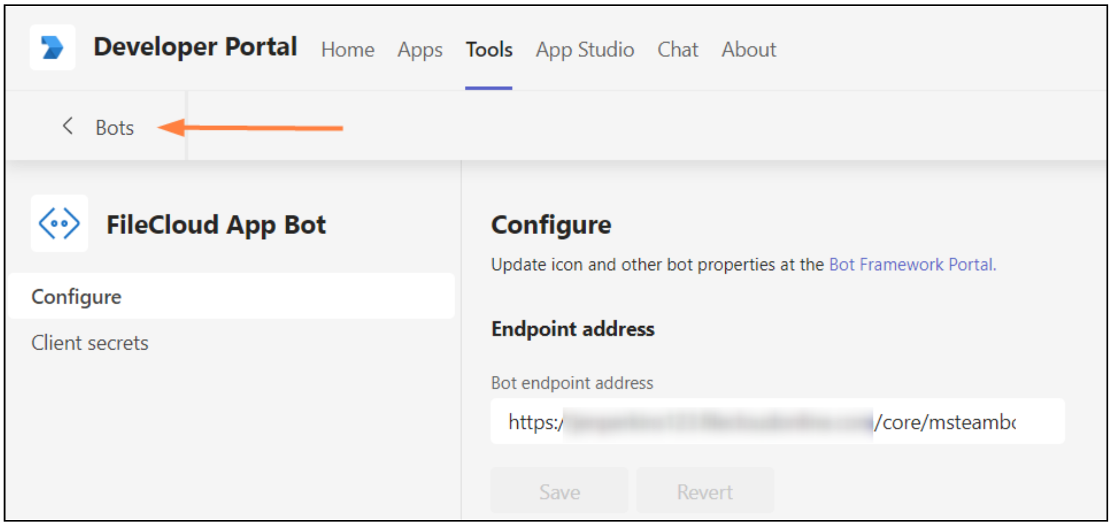
Update icon and other bot properties at the Bot Framework Portal.

Endpoint address

Bot endpoint address: https://mysite.filecloud.com/core/msteamsbot

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

g. Click **Bots**.



Configure

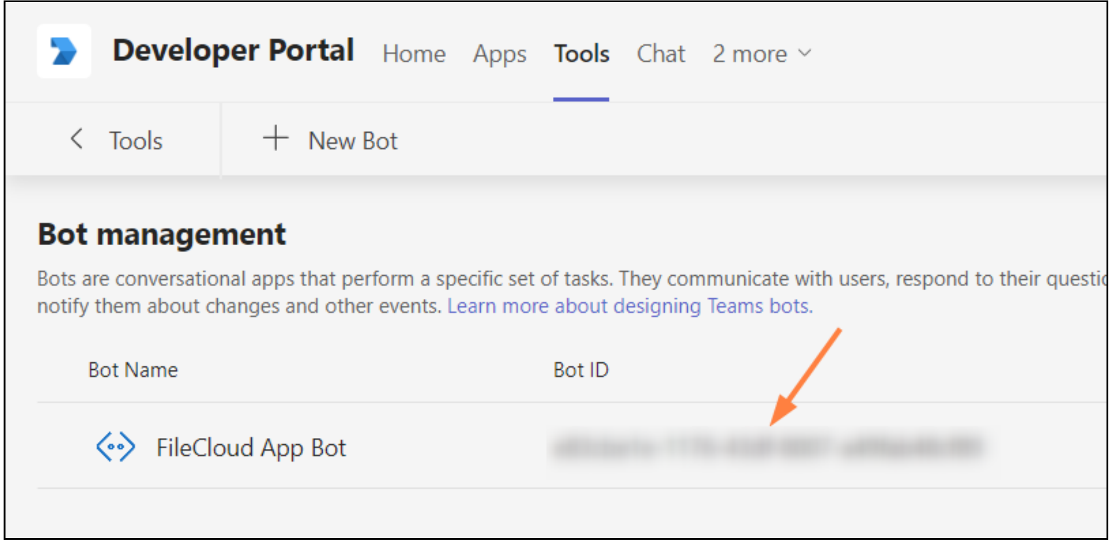
Update icon and other bot properties at the Bot Framework Portal.

Endpoint address

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

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.



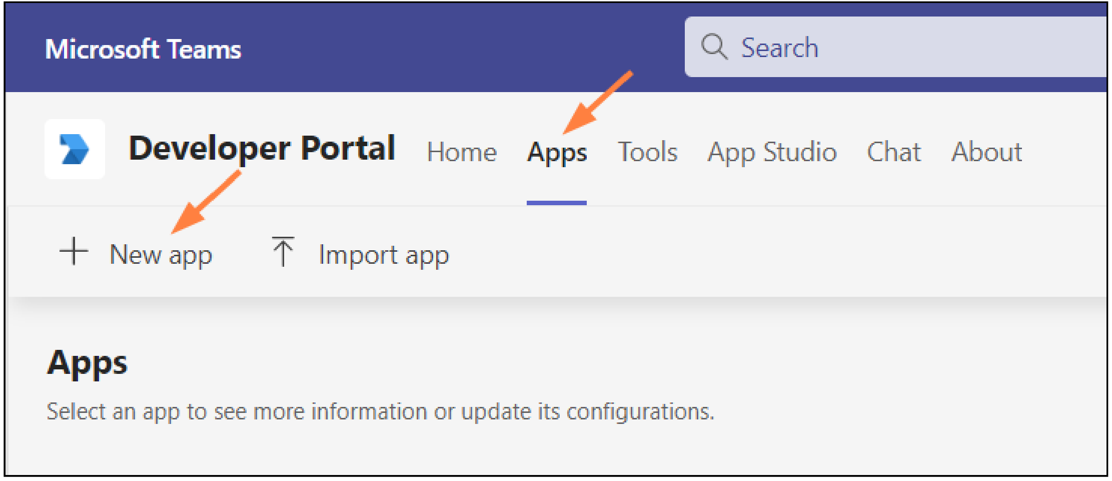
Bot management

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] |

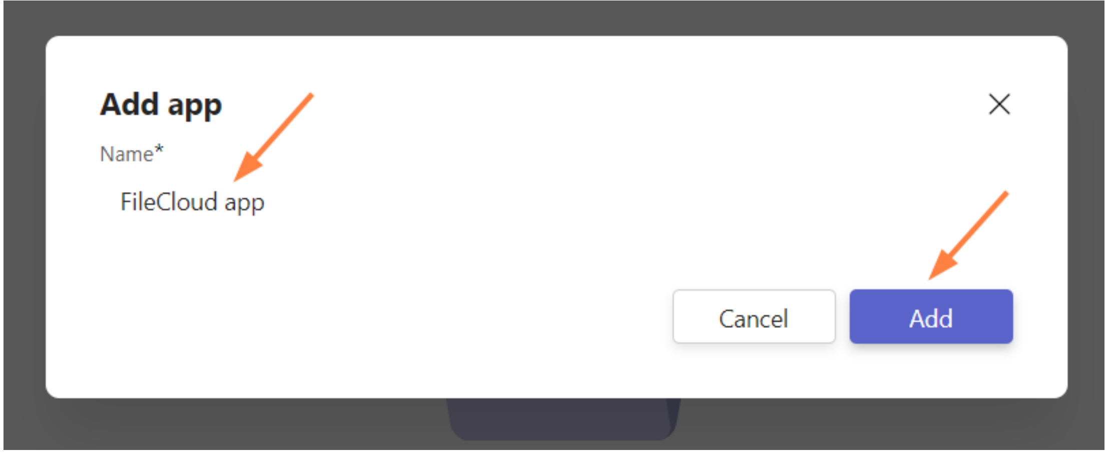
3. Create the MS Teams application in Teams' **Developer Portal**.

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**.

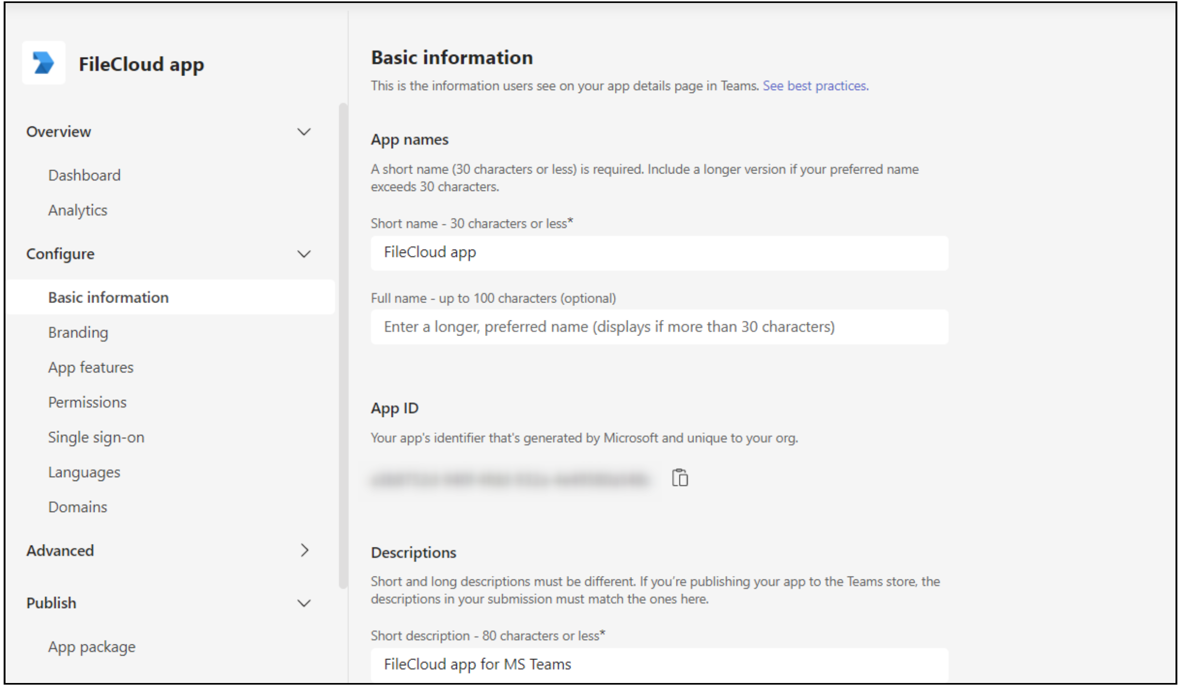


FileCloud app

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**.



FileCloud app

Overview
- Dashboard
- Analytics

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

Advanced

Publish
- App package

**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.

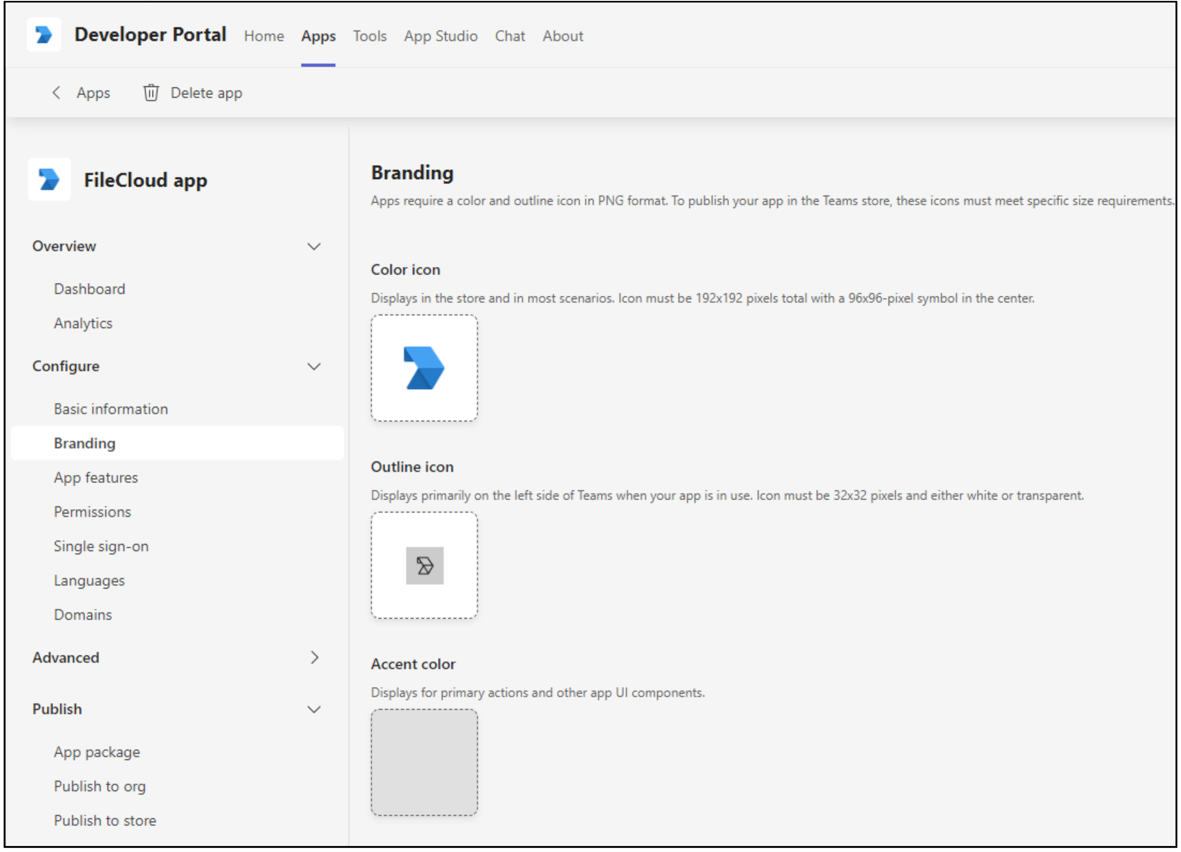
[redacted]

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.



Developer Portal  Home  Apps  Tools  App Studio  Chat  About

< Apps  Delete app

FileCloud app

Overview
- Dashboard
- Analytics

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

Advanced

Publish
- App package
- Publish to org
- Publish to store

**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.

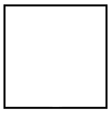
Outline icon

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

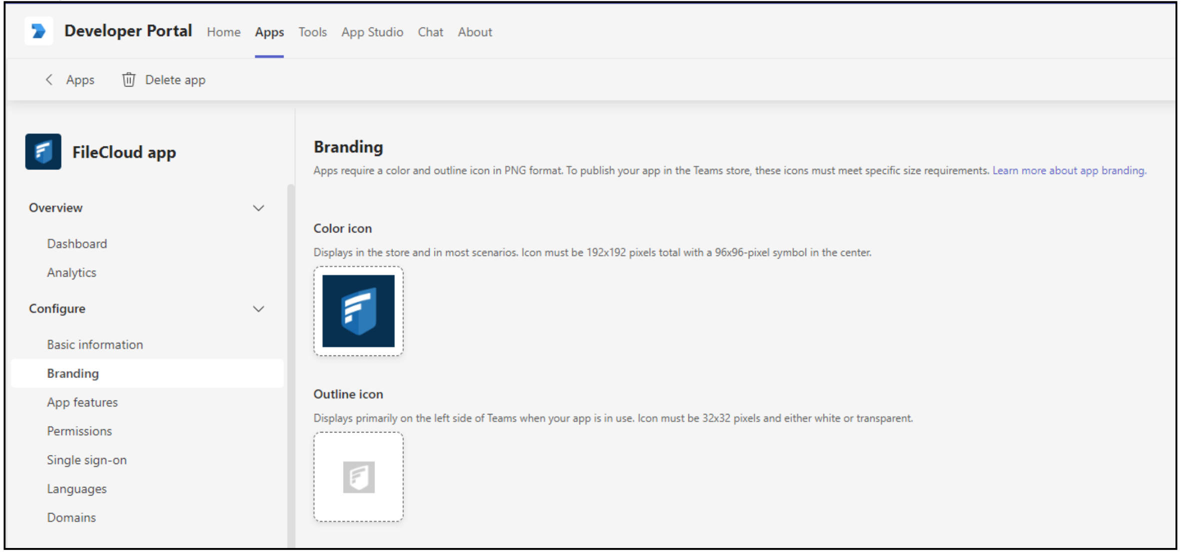
Accent color

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

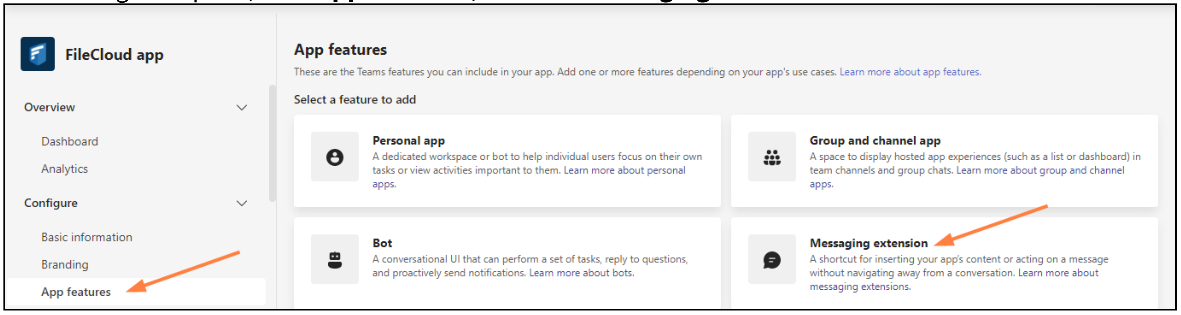
Displays in the store and in most scenarios. Icon must be 192x192 pixels total with a 96x96-pixel symbol in the center.

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.

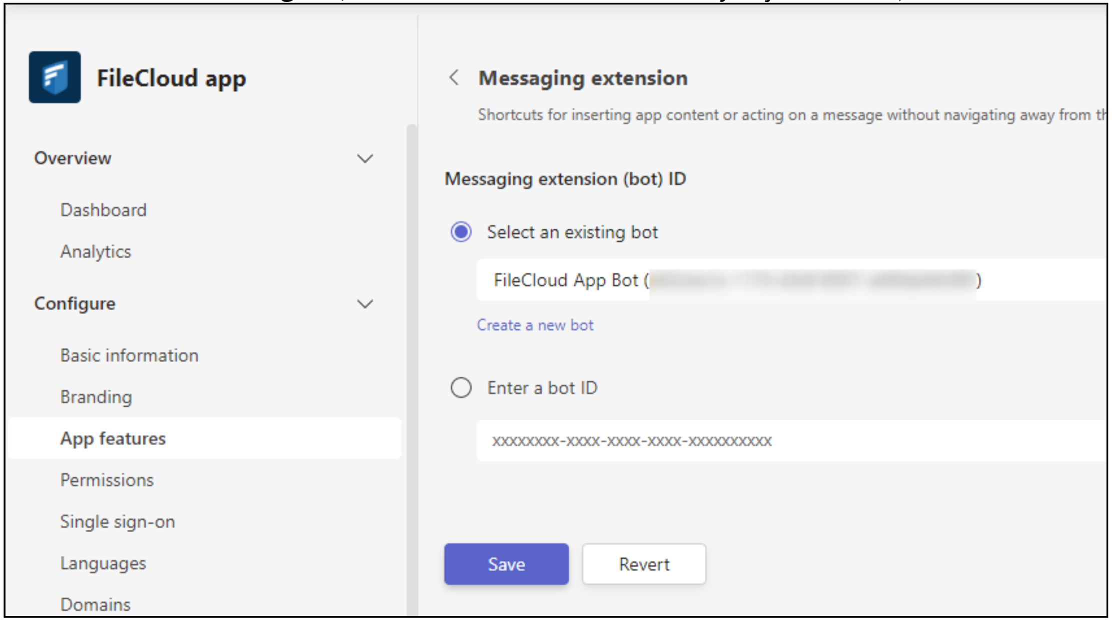
Group and channel app
A space to display hosted app experiences (such as a list or dashboard) in team channels and group chats. Learn more about group and channel apps.

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])

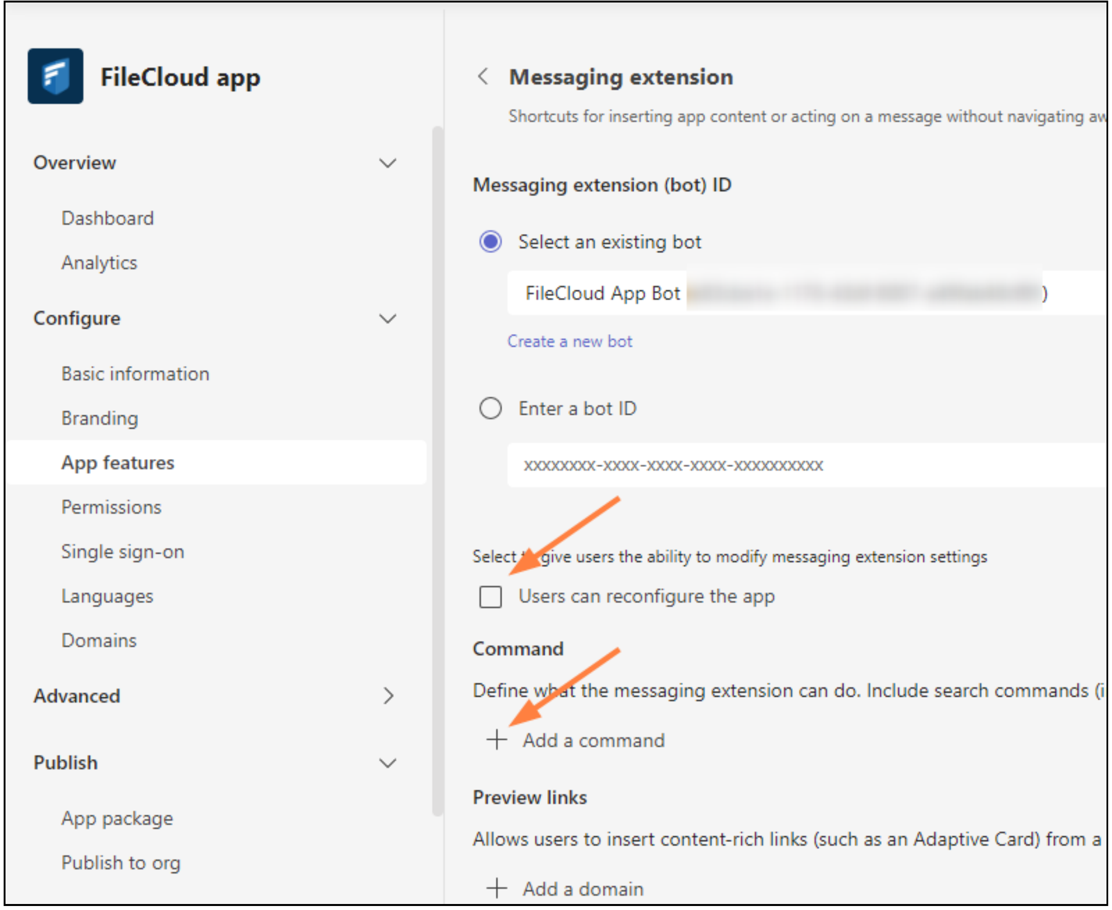
Create a new bot

○ Enter a bot ID

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx

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-xxxxxxxxxxx

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

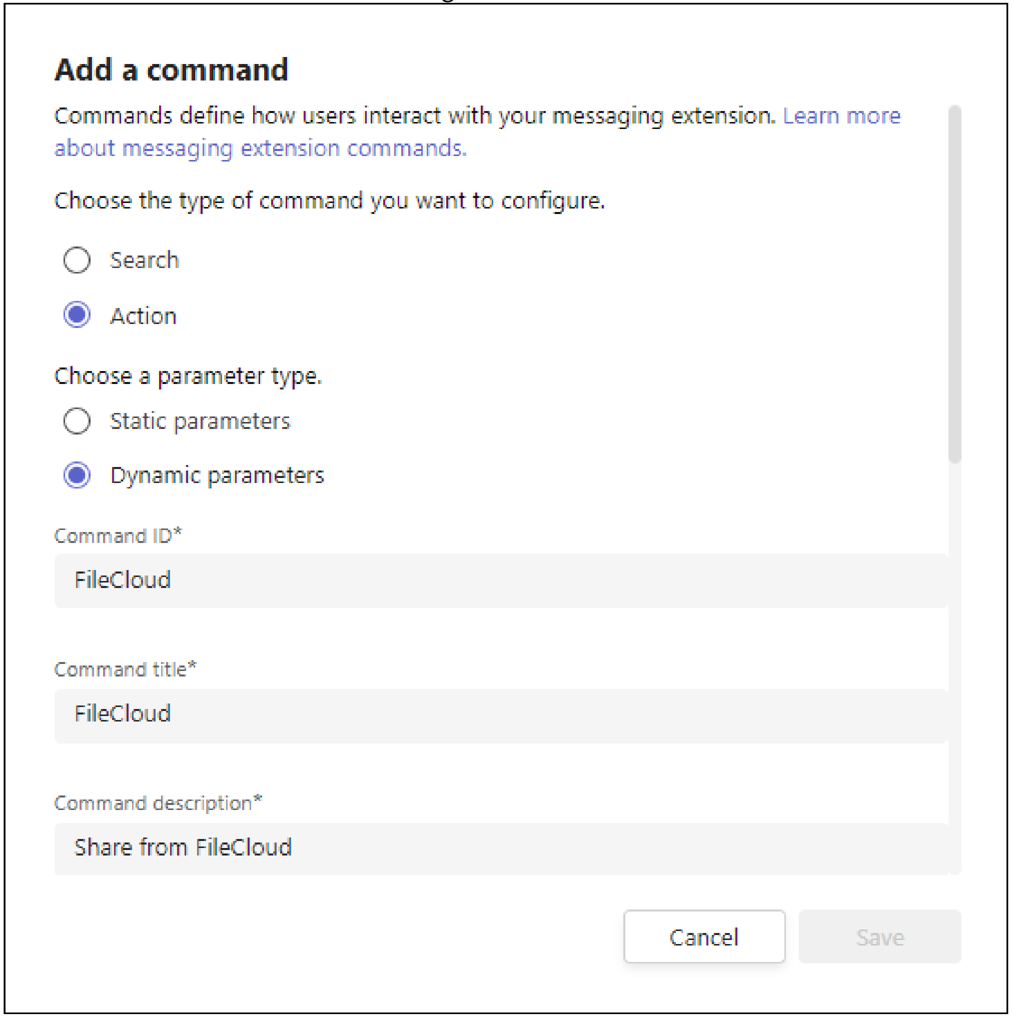
Preview links

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*

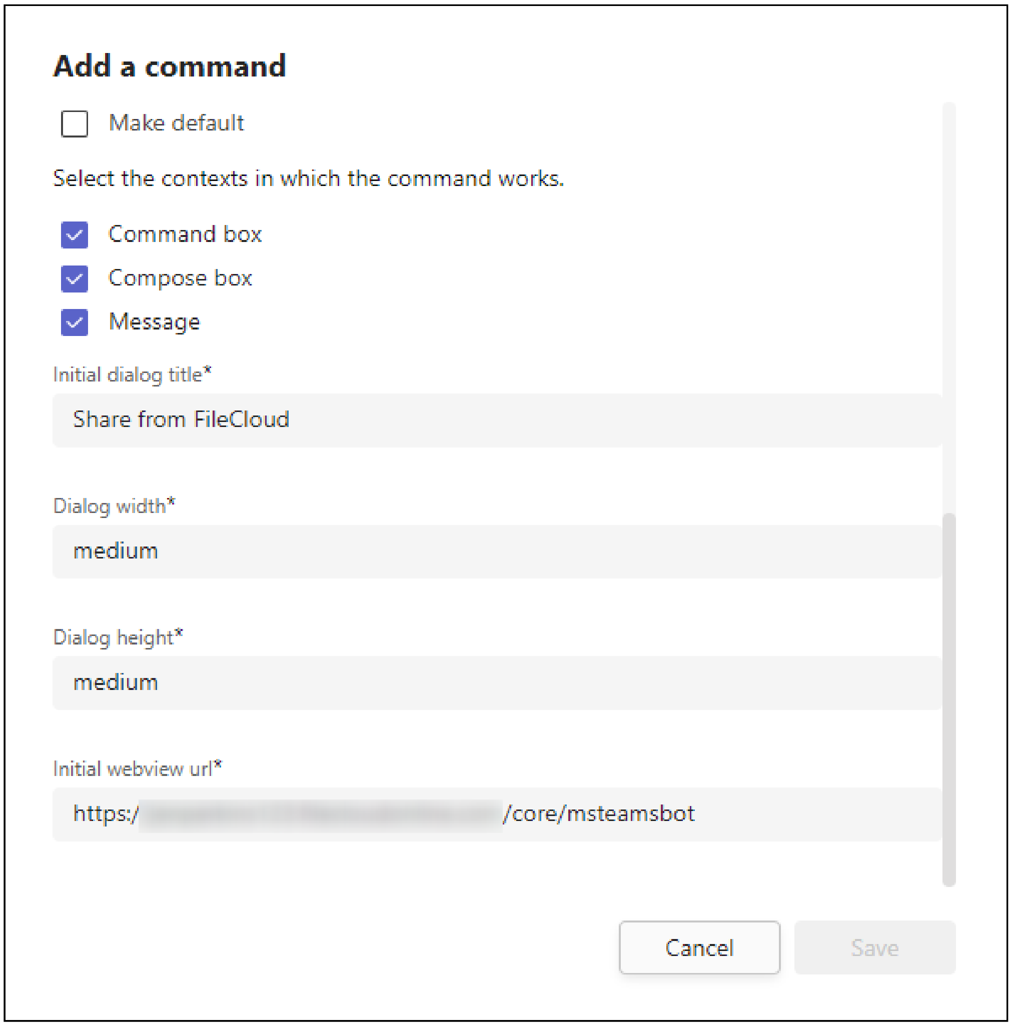
FileCloud

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

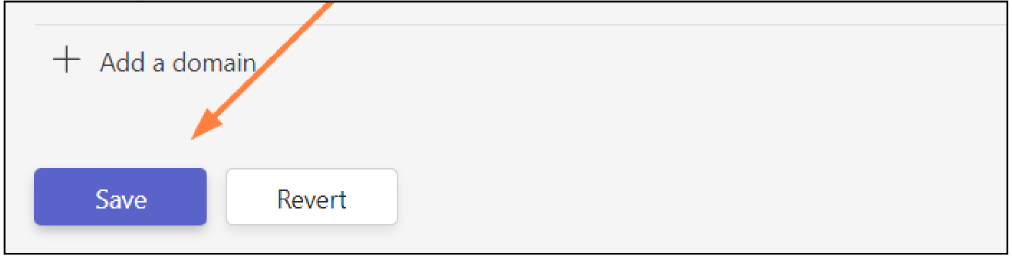
Dialog width*
medium

Dialog height*
medium

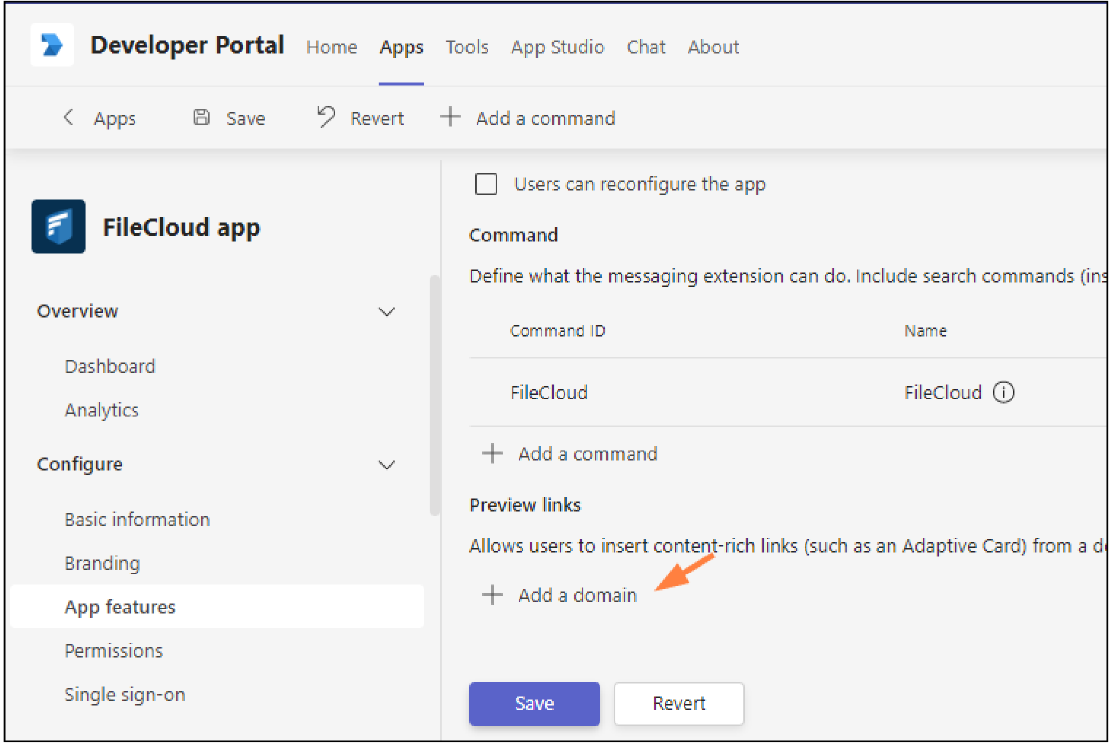
Initial webview url*
https:/[redacted]/core/msteamsbot

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**.



□ Users can reconfigure the app

Command

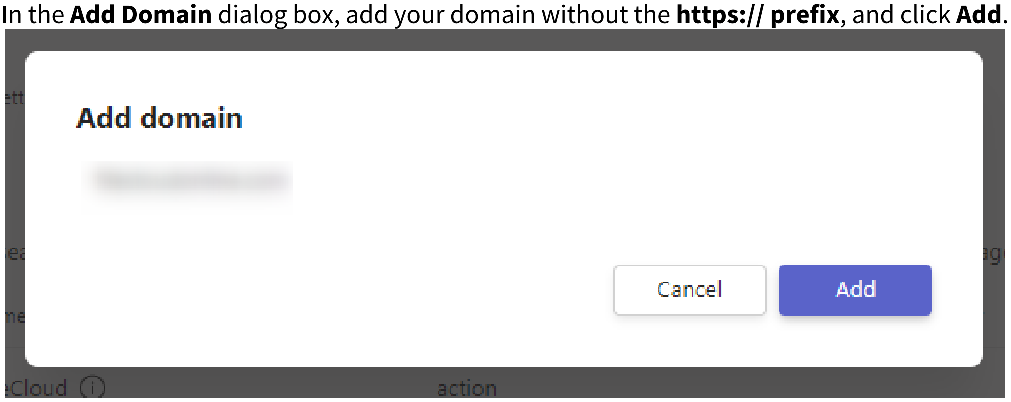
Define what the messaging extension can do. Include search commands (ins

| Command ID | Name |
|---|---|
| FileCloud | FileCloud ⓘ |

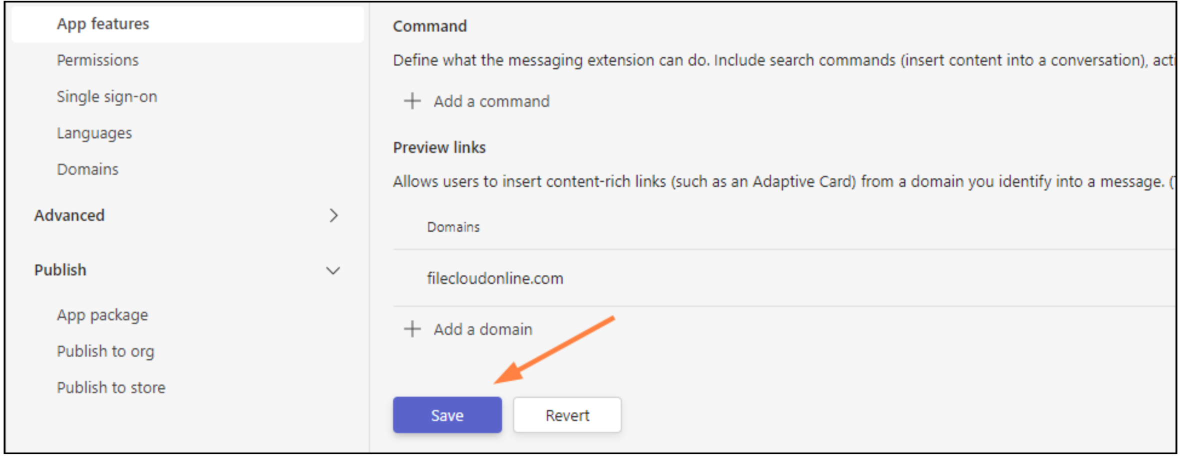
Preview links

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

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**.



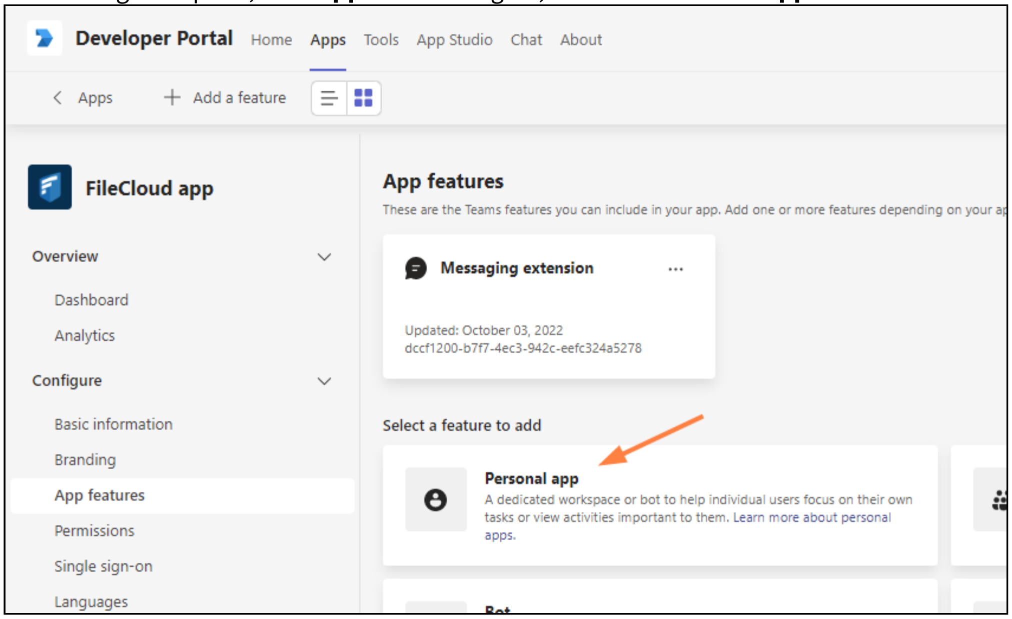
Define what the messaging extension can do. Include search commands (insert content into a conversation), act

Allows users to insert content-rich links (such as an Adaptive Card) from a domain you identify into a message. (

Domains

filecloudonline.com

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

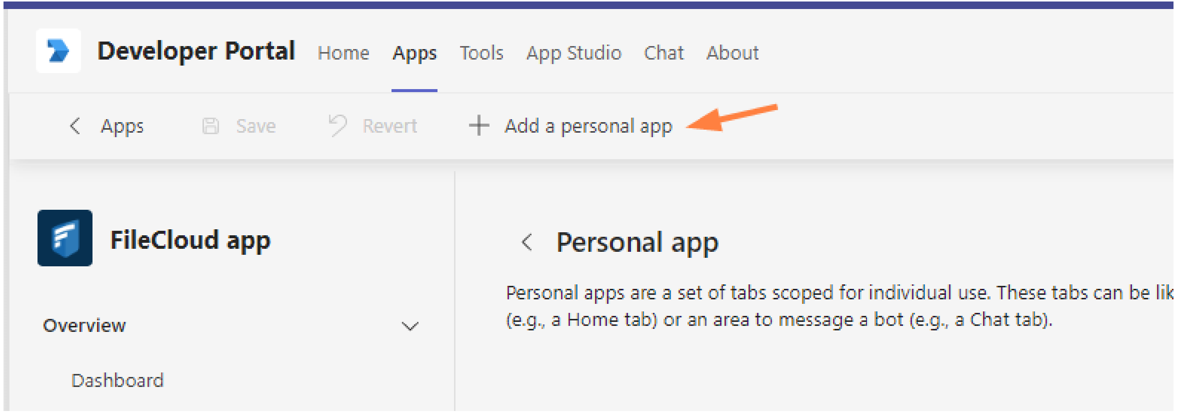
Messaging extension

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

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.

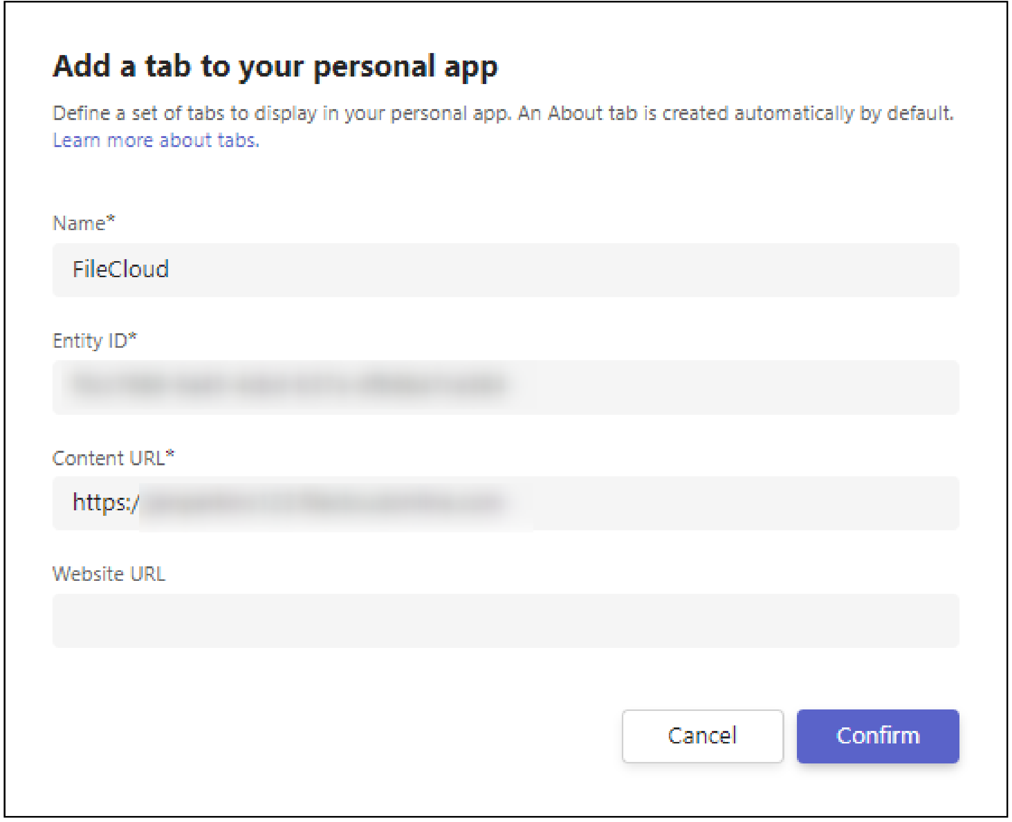
k. Click **Add a personal app**.



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*

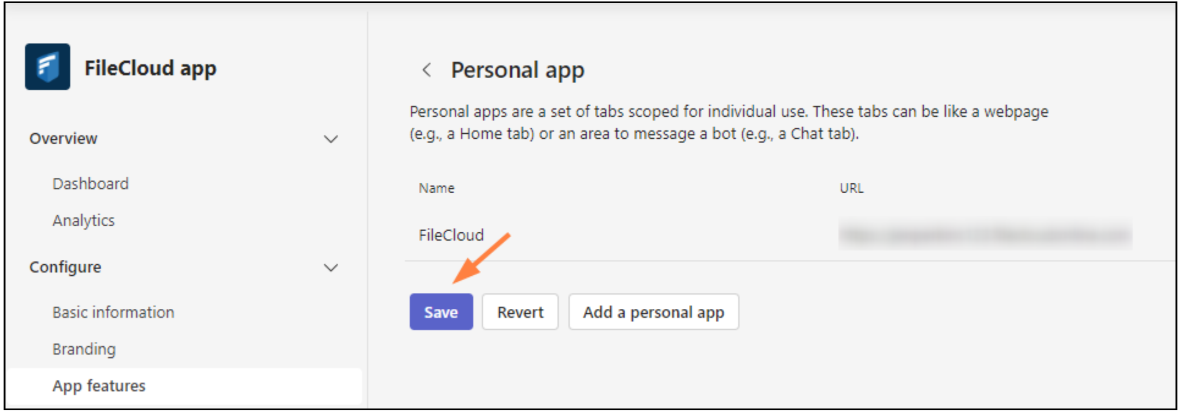
[redacted]

Content URL*

https:/[redacted]

Website URL

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



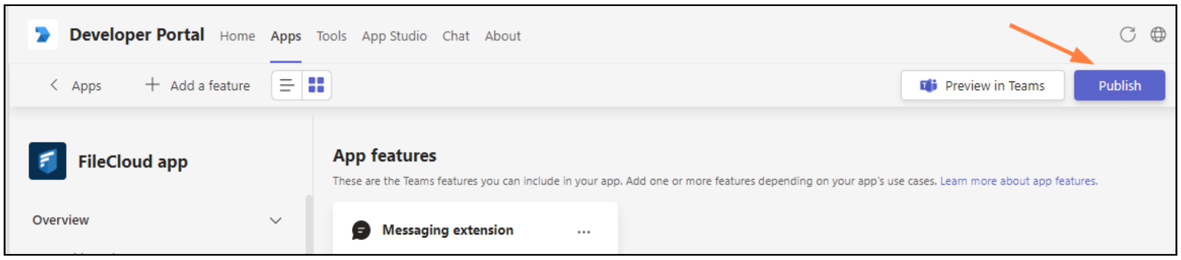
Personal app

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] |

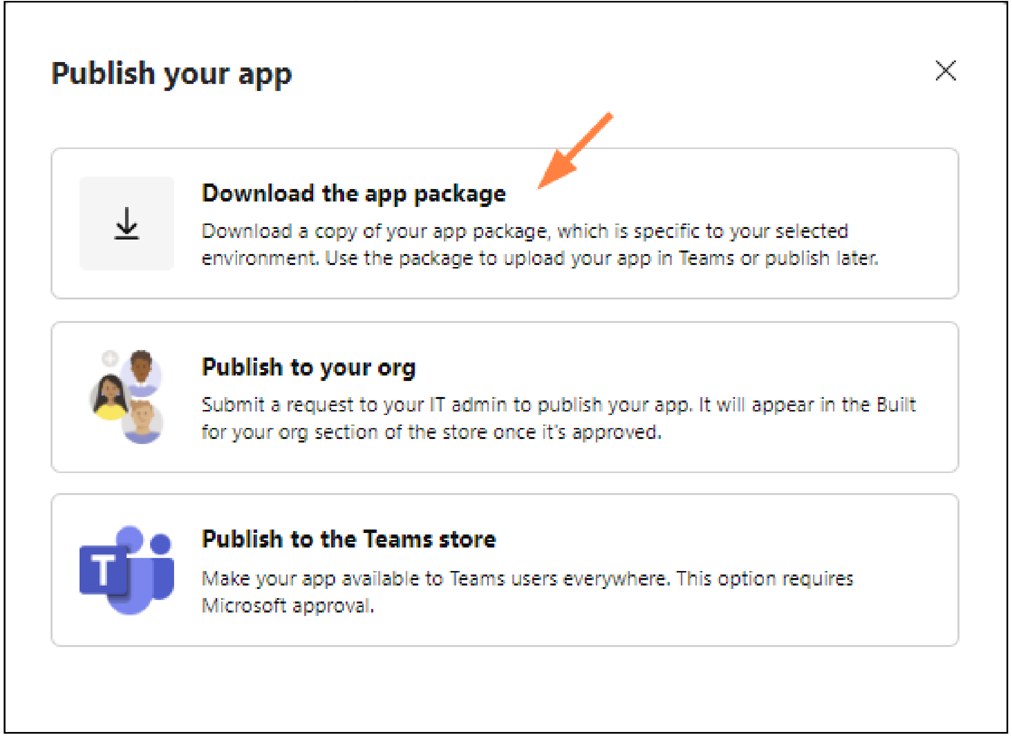
5. Export the application manifest zip file from Teams' **Developer Portal**.

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.

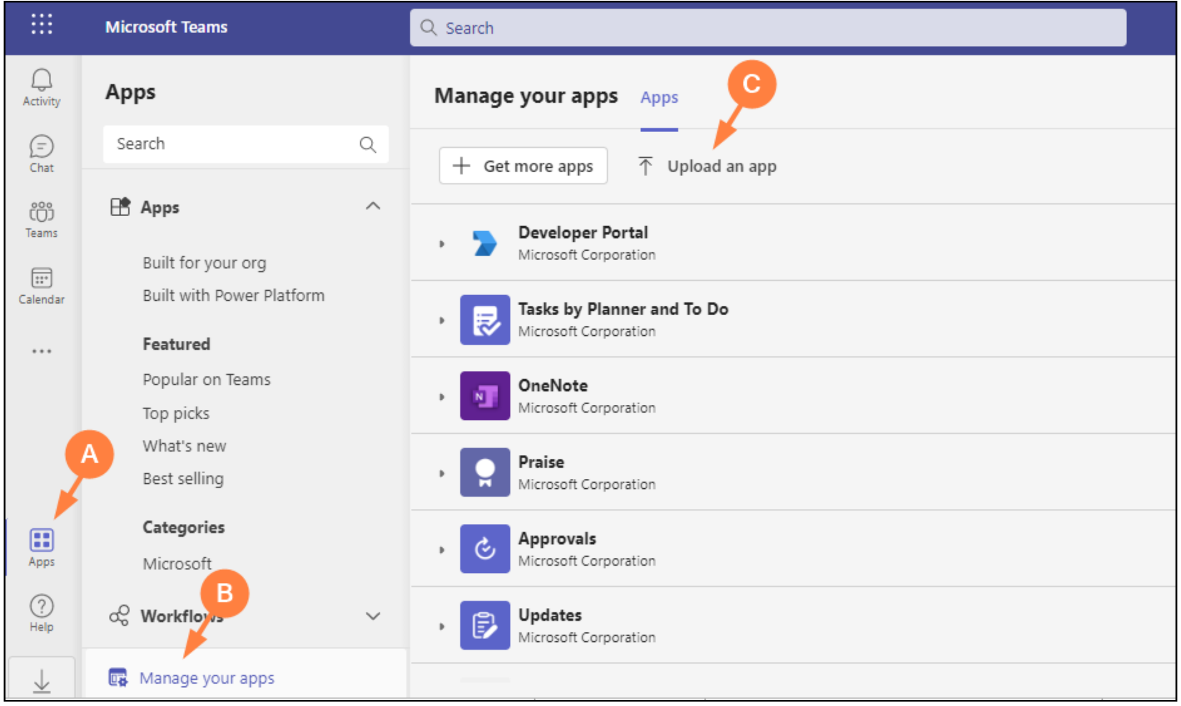
Publish to your org
Submit a request to your IT admin to publish your app. It will appear in the Built for your org section of the store once it's approved.

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.

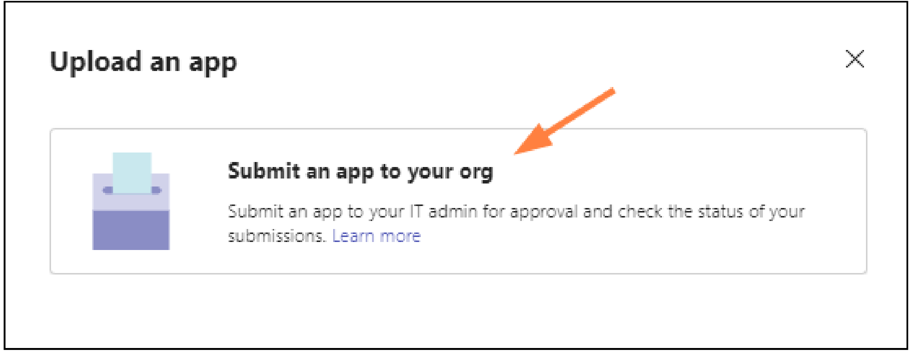
6. Upload the application and submit it for approval in MS Teams.
   a. In the MS Teams navigation pane, click **Apps.**
   b. In the left panel click **Manage your apps**.

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



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

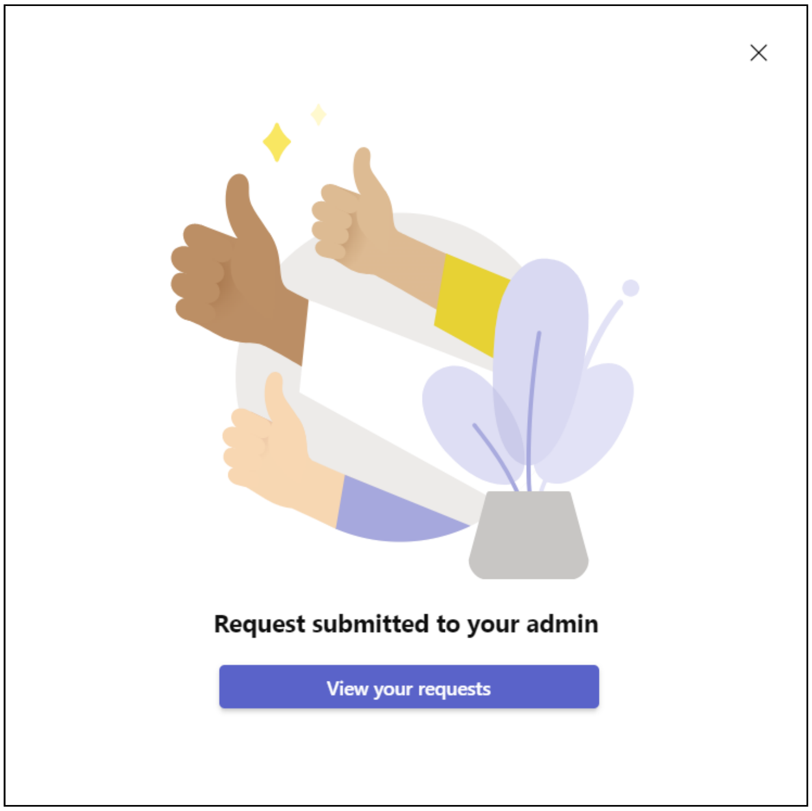
d. Click **Submit an app to your org.**



Upload an app
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.

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.

ⓘ If you update FileCloud from a version prior to 21.2, you must manually add some configurations to the .htaccess file so that login to FileCloud from MS Teams works correctly. See Configuration after FileCloud upgrade, below.

ⓘ 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.

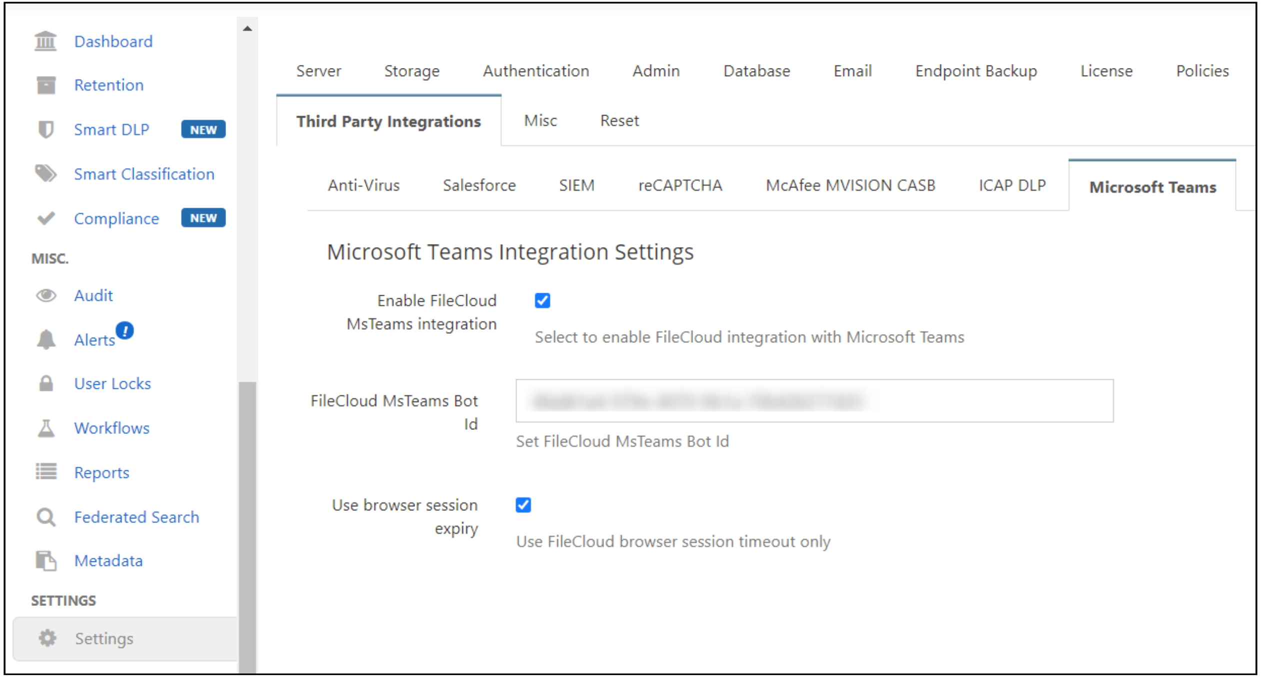
**Note regarding Chrome and Edge users**

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

For instructions on setting the **SameSite** value, see Improving Cookie Security.

## 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).



Microsoft Teams Integration Settings

Enable FileCloud MsTeams integration ☑
Select to enable FileCloud integration with Microsoft Teams

FileCloud MsTeams Bot Id [redacted]
Set FileCloud MsTeams Bot Id

Use browser session expiry ☑
Use FileCloud browser session timeout only

**1 Server, Third Party Integrations, MS Teams**

5. Click **Save**.

## Configuration after FileCloud upgrade

If you upgrade FileCloud from a version prior to 21.2, edit your .htaccess file so that login to FileCloud from MS Teams works correctly:

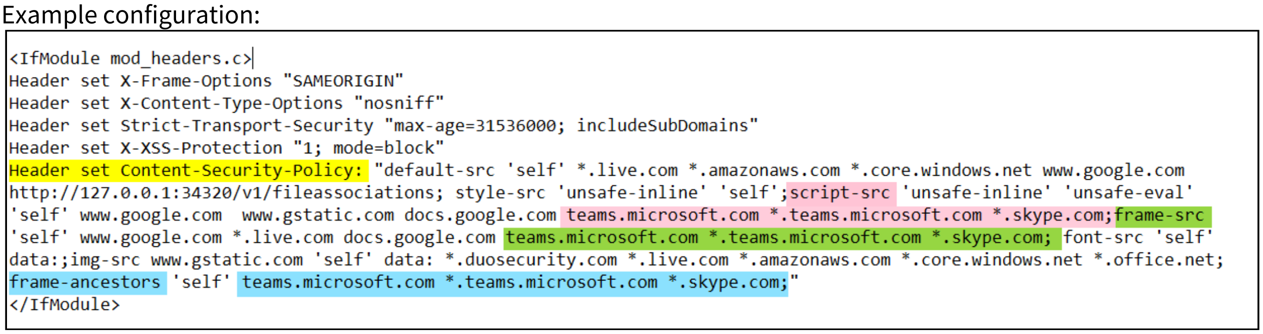
1. Open the **.htaccess** file:

- in Windows, C:\xampp\htdocs\.htaccess
- in Linux, /var/www/.htaccess

2. Find the **Content-Security-Policy** header.
3. Add:
   **teams.microsoft.com *.teams.microsoft.com *.skype.com**
   to each of the following three directives in the Content-Security-Policy:

   - **script-src**
   - **frame-src**
   - **frame-ancestors**

2. Make sure that each directive is followed by 'self' and ends with a semicolon.
   Example configuration:



```
<IfModule mod_headers.c>
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Header set X-XSS-Protection "1; mode=block"
Header set Content-Security-Policy: "default-src 'self' *.live.com *.amazonaws.com *.core.windows.net www.google.com
http://127.0.0.1:34320/v1/fileassociations; style-src 'unsafe-inline' 'self';script-src 'unsafe-inline' 'unsafe-eval'
'self' www.google.com  www.gstatic.com docs.google.com teams.microsoft.com *.teams.microsoft.com *.skype.com;frame-src
'self' www.google.com *.live.com docs.google.com teams.microsoft.com *.teams.microsoft.com *.skype.com; font-src 'self'
data:;img-src www.gstatic.com 'self' data: *.duosecurity.com *.live.com *.amazonaws.com *.core.windows.net *.office.net;
frame-ancestors 'self' teams.microsoft.com *.teams.microsoft.com *.skype.com;"
</IfModule>
```

## Redirection to Login Screen

If you have integrated your system with MS Teams, and login frequently redirects users back to the login page:

1. Open cloudconfig.php:
   Windows Location: XAMPP DIRECTORY/htdocs/config/cloudconfig.php
   Linux Location: /var/www/config/cloudconfig.php
2. Add the following settings:

```
define("TONIDOCLOUD_COOKIE_SAME_SITE_TYPE", "None");
define("TONIDOCLOUD_SECURE_COOKIE", 1);
define("TONIDOCLOUD_HTTPONLY_COOKIE", 1);
```

# 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.

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

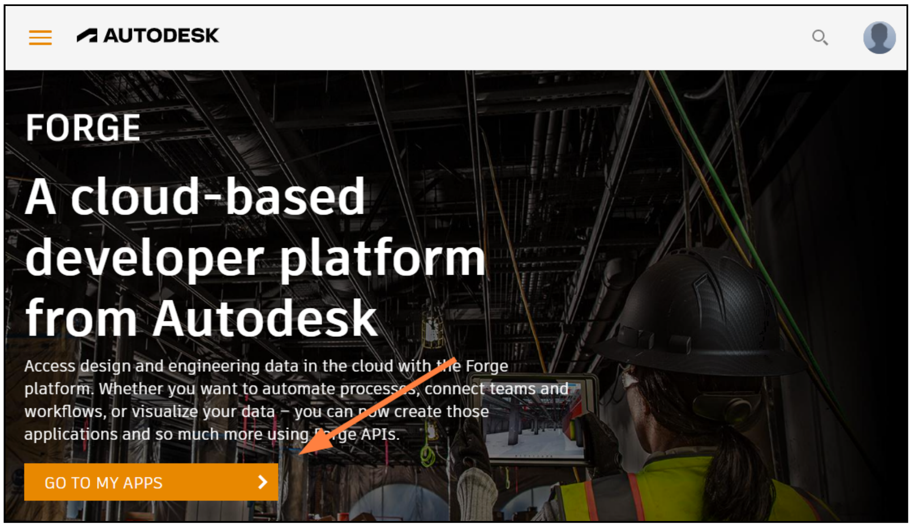
After you configure FileCloud integration with Autodesk Viewer, when users preview 3D and 2D model data file types, they are shown in Autodesk Viewer.

## 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**.

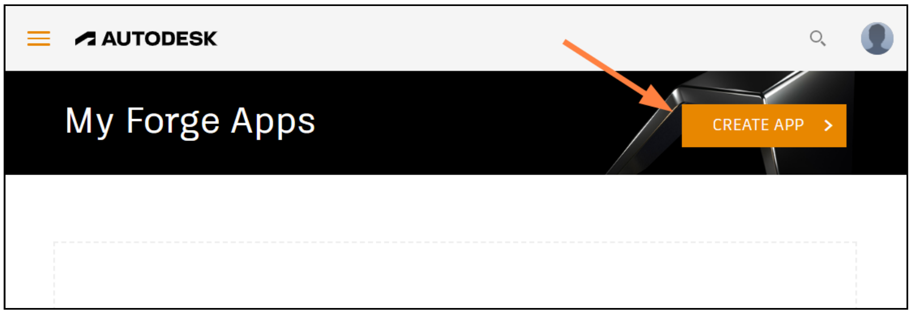


FORGE

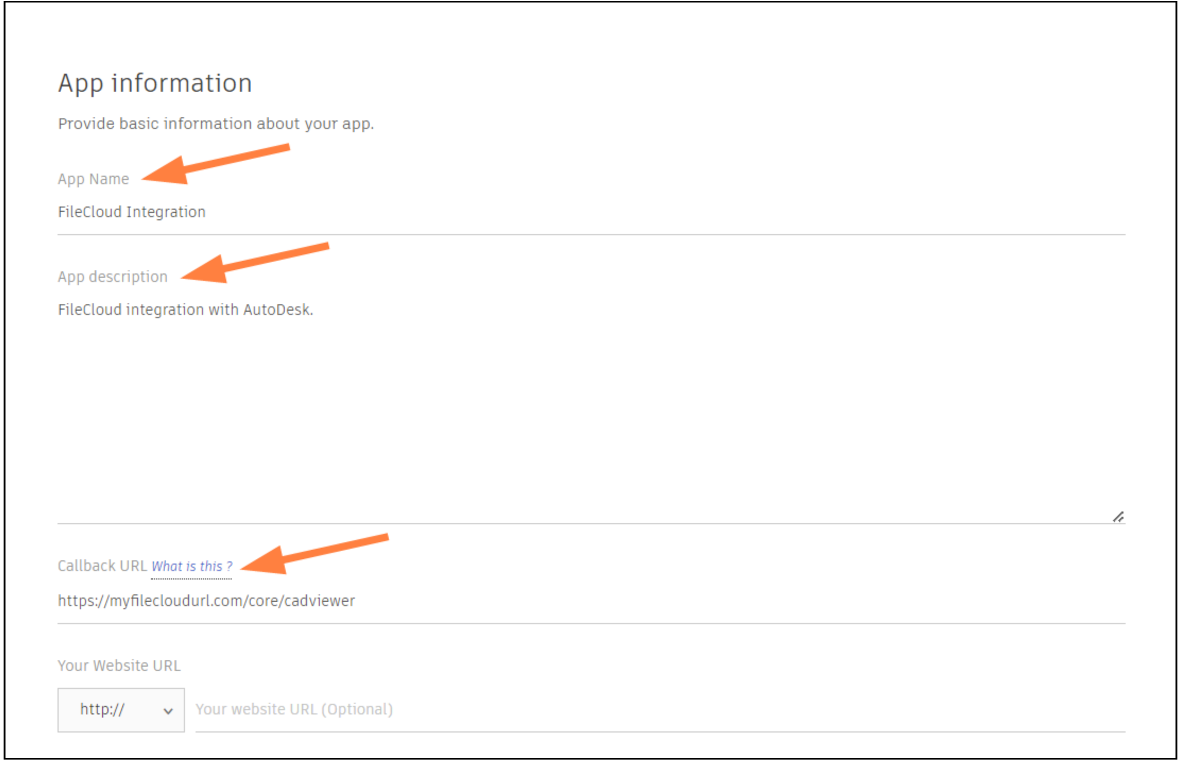
A cloud-based developer platform from Autodesk

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.

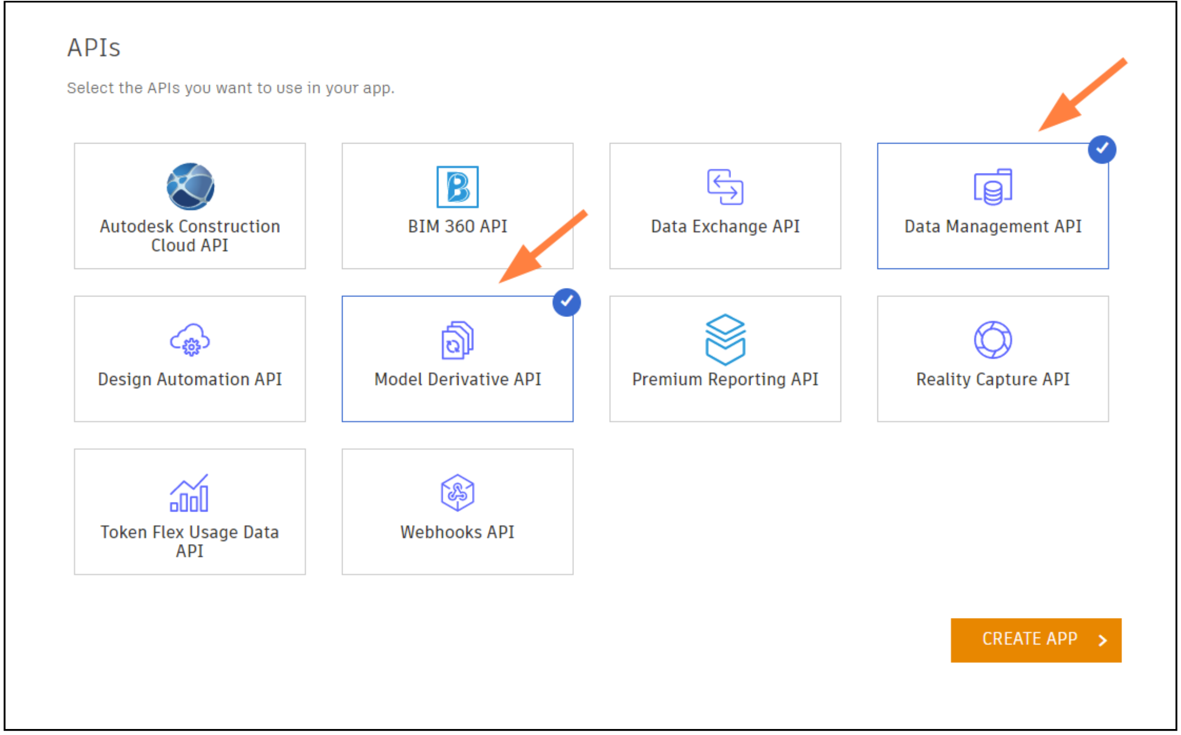
Callback URL *What is this ?*

https://myfilecloudurl.com/core/cadviewer

Your Website URL

http:// Your website URL (Optional)

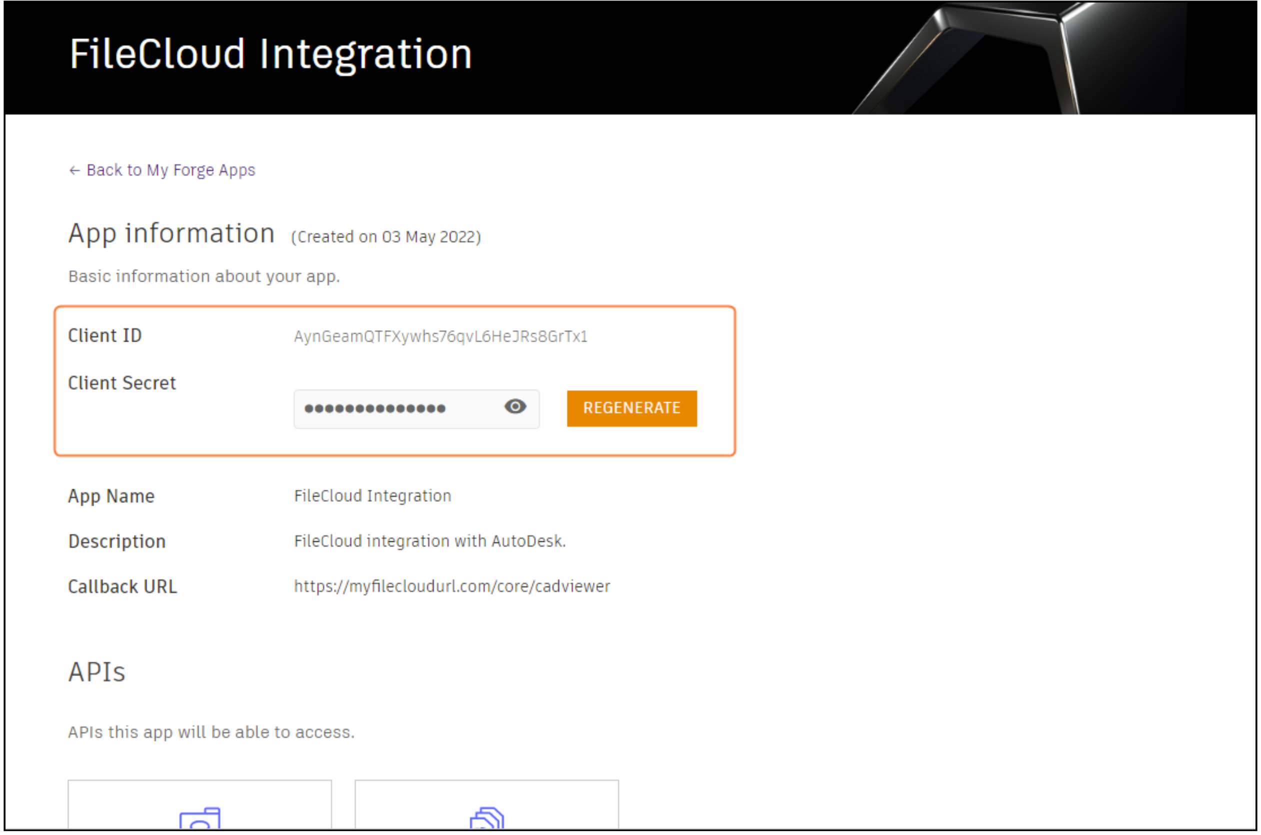
- In the APIs section, select only **Data Management API** and **Model Derivative API**.



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

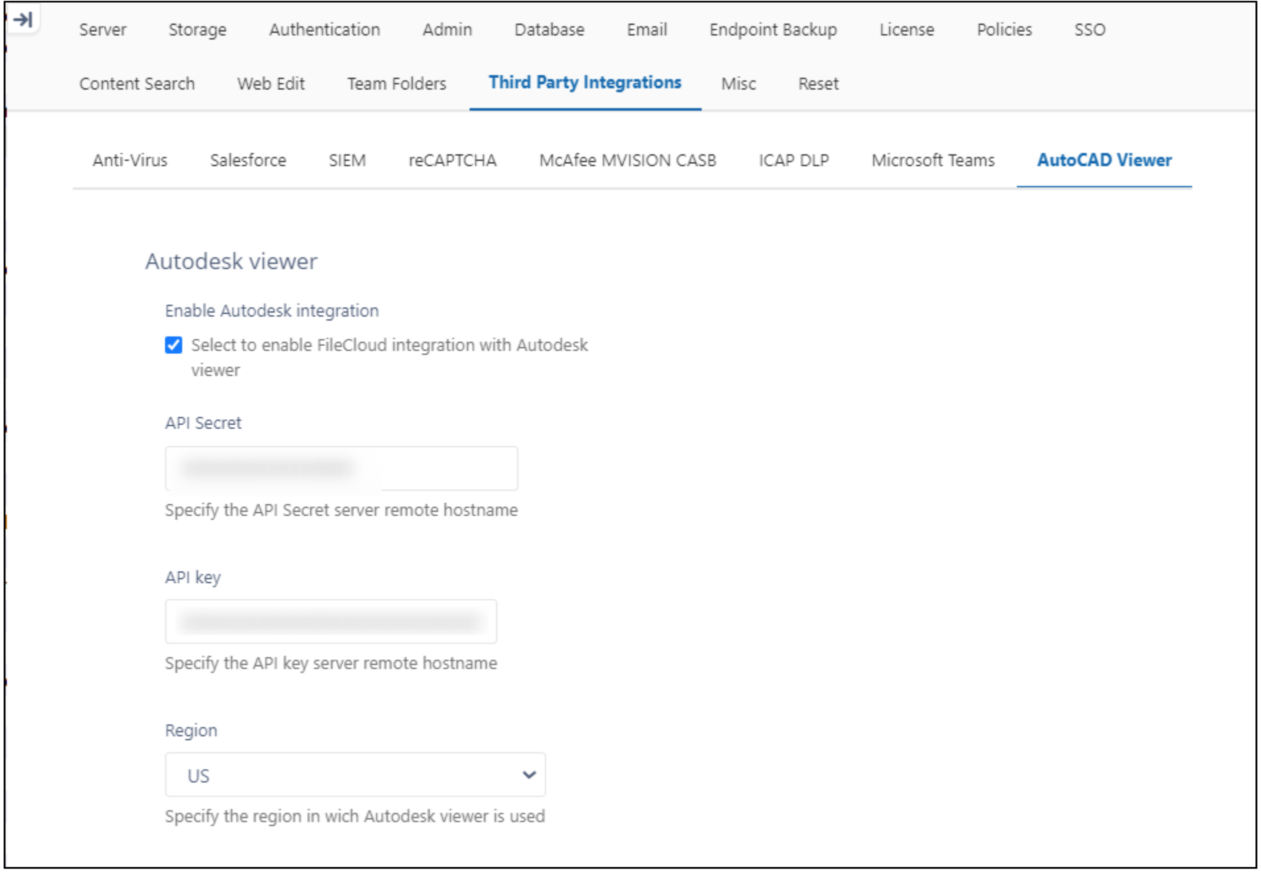
Description FileCloud integration with AutoDesk.

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

APIs

APIs this app will be able to access.

7. In the FileCloud admin portal, 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**.



Autodesk viewer

Enable Autodesk integration

☑ Select to enable FileCloud integration with Autodesk viewer

API Secret

[redacted]

Specify the API Secret server remote hostname

API key

[redacted]

Specify the API key server remote hostname

Region

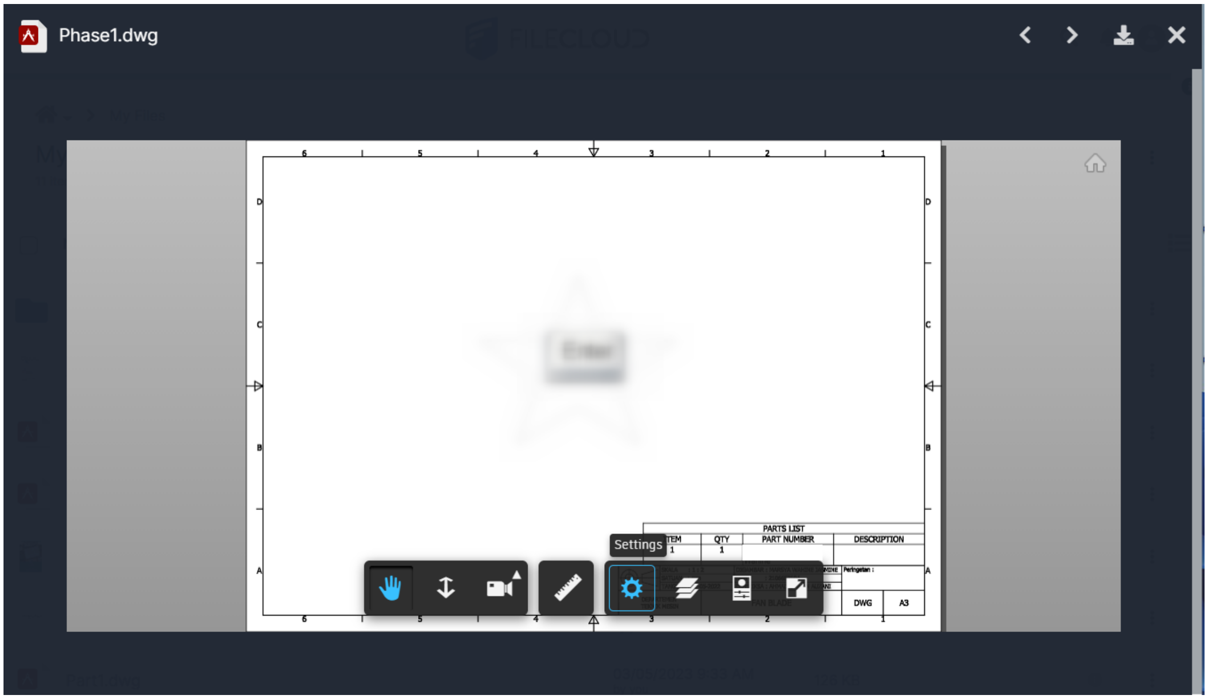
US

Specify the region in wich Autodesk viewer is used

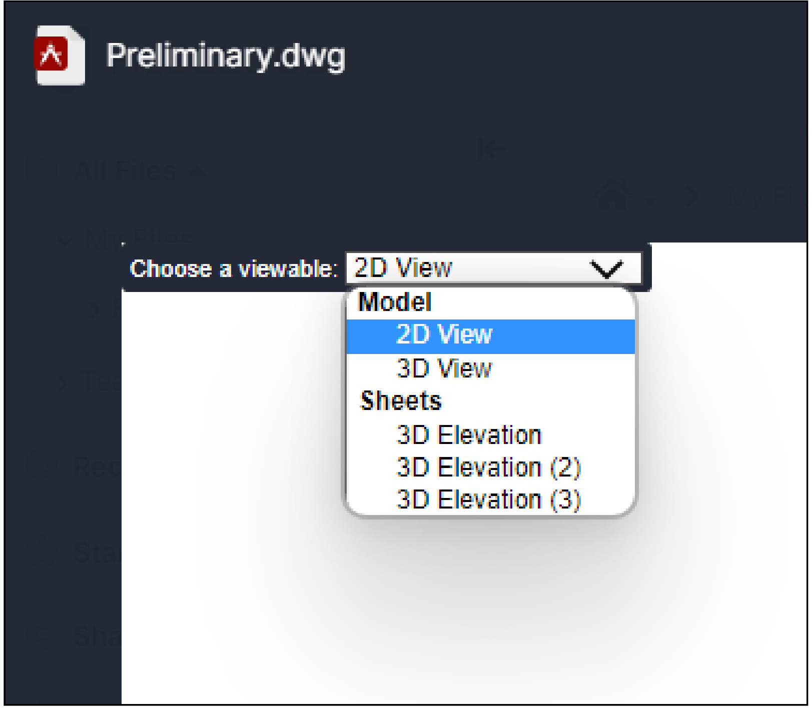
11. Click **Save**.
12. Make the following change to the Apache SSL config file in the **<VirtualHost>** definition:
    a. Open httpd-ssl.conf:
       Windows Location: **XAMPP DIRECTORY\apache\conf\extra\httpd-ssl.conf**
       Linux Location: **/etc/apache2/sites-enabled/000-default.conf**
    b. Near the end of the file, but before **</VirtualHost>** , add the following:

```
AllowEncodedSlashes NoDecode
```

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

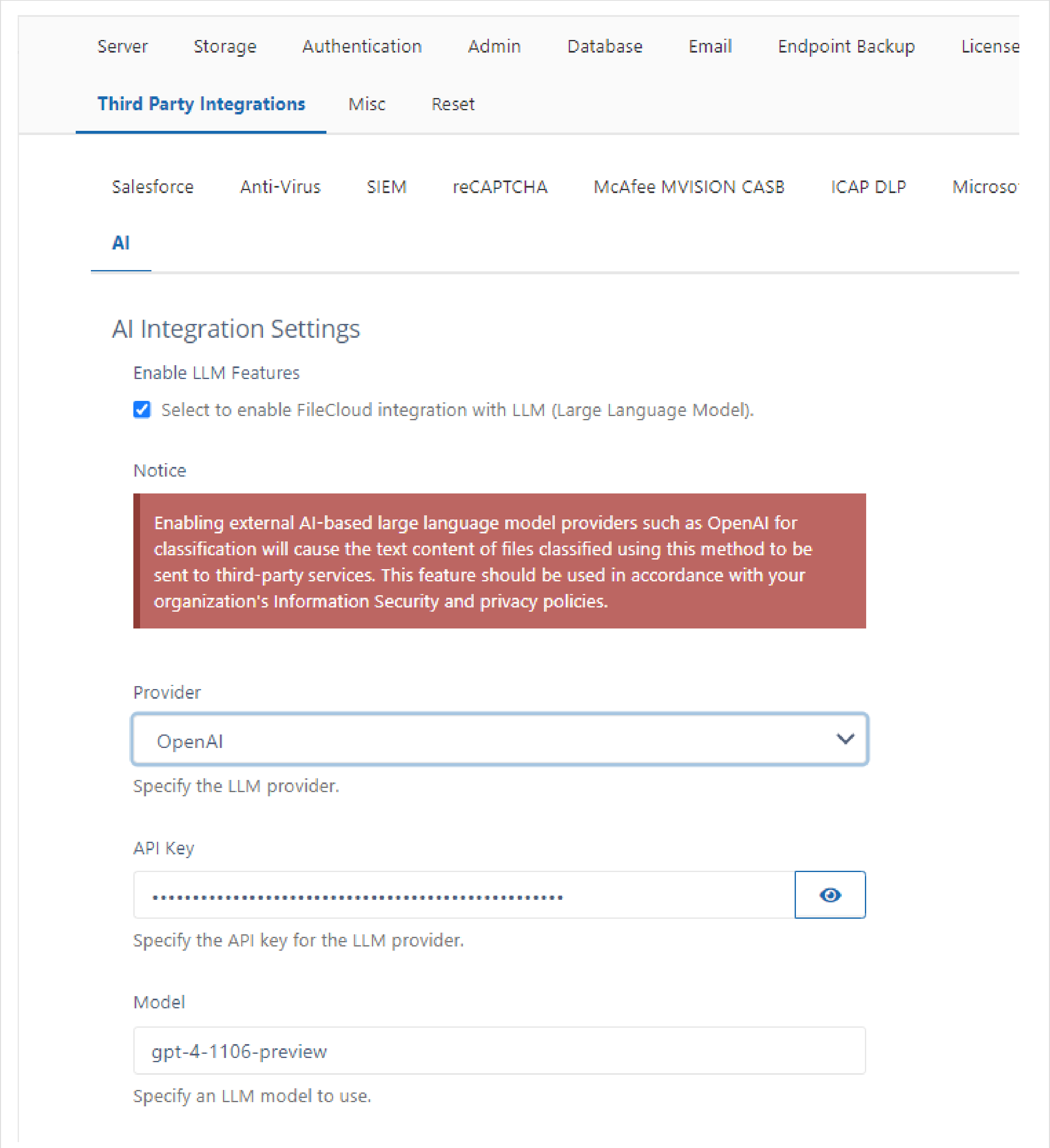
The ability to configure a Large Language Model for FileCloud Smart Classification is available in versions 22.232 and higher.

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**.



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

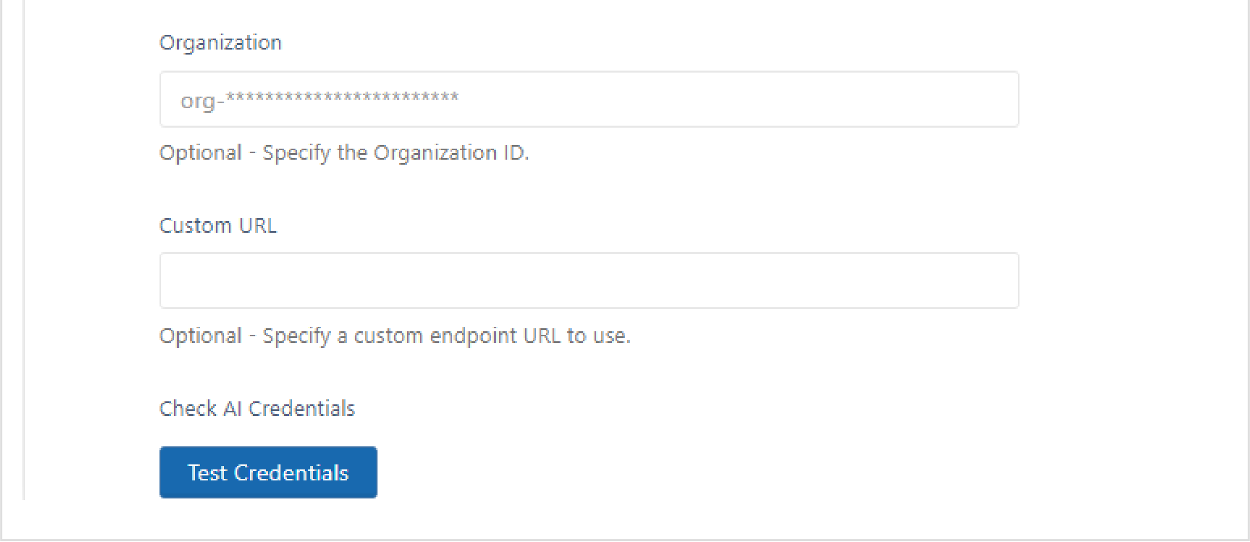
••••••••••••••••••••••••••••••••••••••••••••••••••••

Specify the API key for the LLM provider.

Model

gpt-4-1106-preview

Specify an LLM model to use.



Organization

org-************************

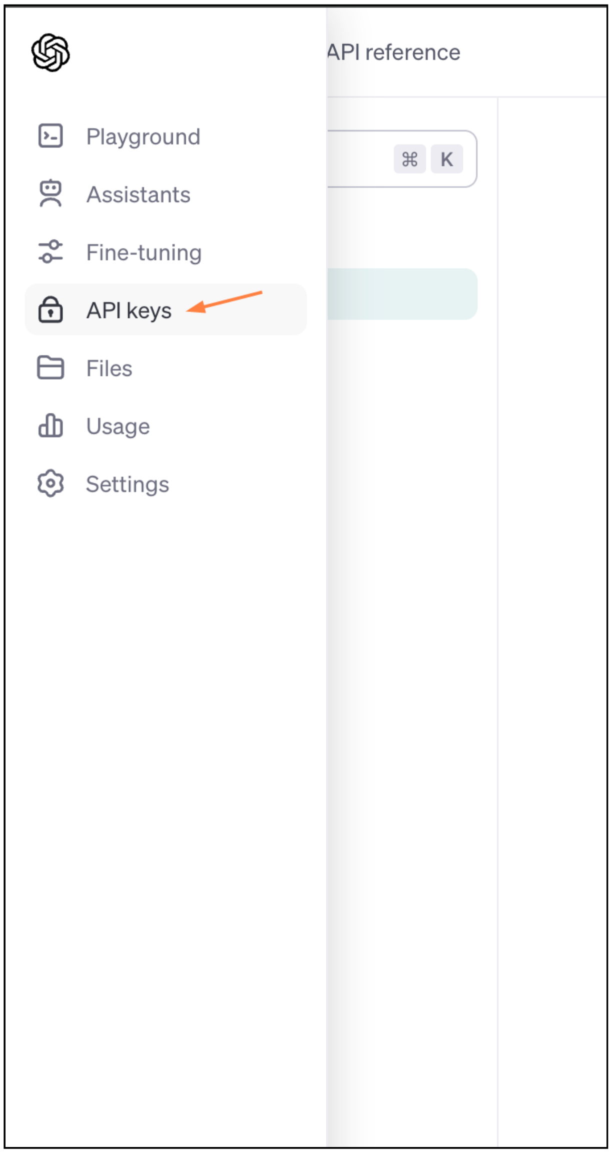
Optional - Specify the Organization ID.

Custom URL

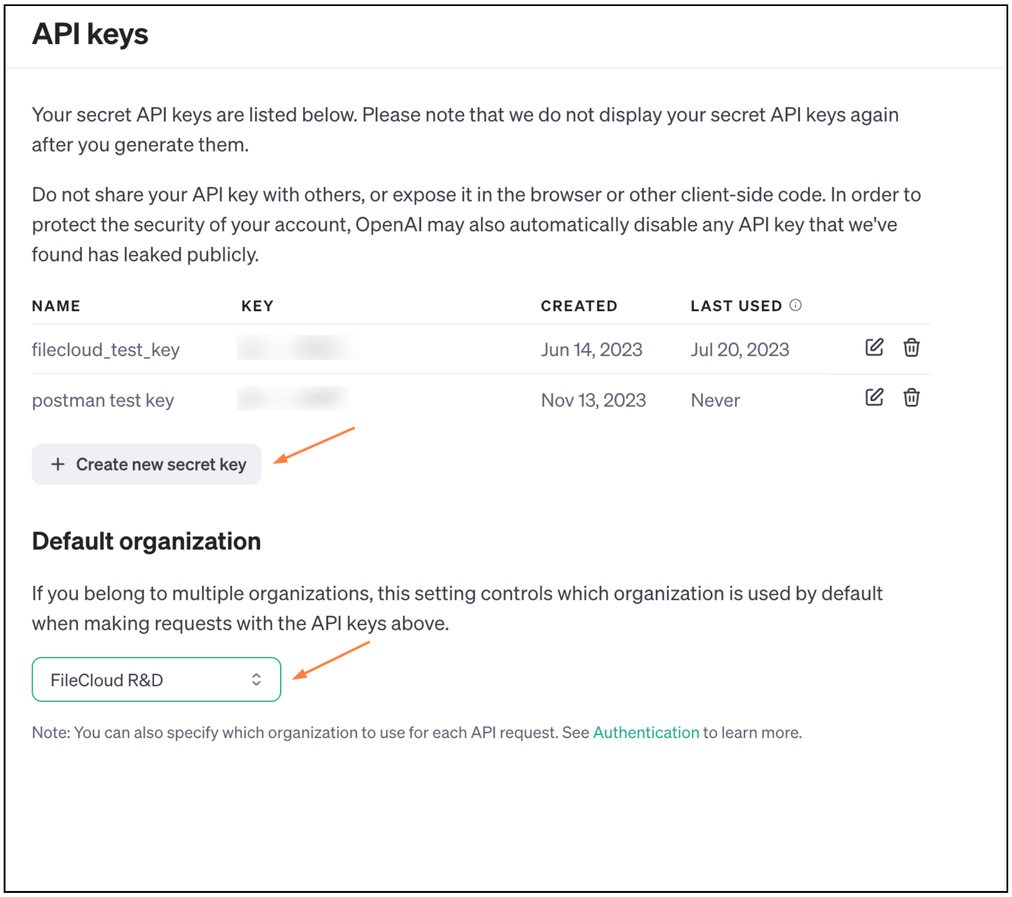
Optional - Specify a custom endpoint URL to use.

Check AI 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:



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

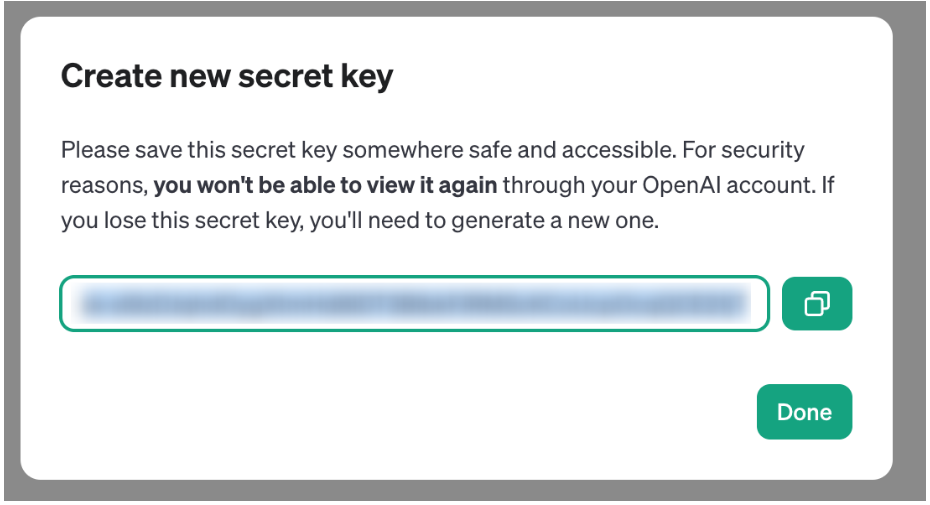
If you belong to multiple organizations, this setting controls which organization is used by default when making requests with the API keys above.

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.

[redacted]

- 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.

5. In **Model**, enter the value for your model. For help determining your model, see https://platform.openai.com/docs/models.

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.