

# FileCloud Online Version 23.232 Third Party Integration Settings

# **Copyright Notice**

©2024 CodeLathe Technologies, Inc. dba FileCloud

All rights reserved.

No reproduction without written permission.

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

FileCloud Phone: U.S: +1 (888) 571-6480 Fax: +1 (866) 824-9584 Email: support@filecloud.com

# Table of Contents

Copyright Notice	2
Third Party Integrations	4
Integrating FileCloud with Salesforce	5
Adding FileCloud to Salesforce	6
Configuring FileCloud with Salesforce1	.7
SIEM Integration2	1
FileCloud SIEM Configuration2	2
Managing SIEM Mappings2	4
SIEM Integration with Splunk Enterprise4	0
reCaptcha Settings4	7
To configure reCaptcha:4	7
CASB integration4	8
McAfee CASB integration4	.9
ICAP DLP5	1
What is ICAP?5	1
Integrating ICAP DLP with FileCloud5	1
Microsoft Teams	4
For MS Teams Admins: Configuring FileCloud in Teams5	4
For FileCloud Admins: Enabling Integration with MS Teams6	9
Setting Up AutoCAD File Preview with Autodesk Viewer7	1
Setting up integration of FileCloud and Autodesk Viewer7	'1
Al Integration7	7

# 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.

Server Storage A	uthentication Misc Rese	Admin Email et	Endpoint Backup	License	Policies	SSO	Team Folders
Salesforce SIEM	reCAPTCHA	McAfee MVISIO	N CASB ICAP DLP	Microsof	t Teams		
Salesforce Integrat	ion Settings						
Enable Salesforce							
integration	Turn on Salesfor	rce Integration					

### In this section:

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

# Integrating FileCloud with Salesforce

### (i) 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.

F			<b>Q</b> Search			
FileCloud CCP	Accounts 🗸 Case	es 🗸 Contacts 🗸	🖌 Leads 🗸	Opportunities	✓ Chatter	Configure FileCloud
Account Specialty Coati	ng Systems 🚠					
Phone Billing Addres	s Website	Account Owner	£			
Related Details	FileCloud					
$ \begin{tabular}{lllllllllllllllllllllllllllllllllll$	alesforce > Account /stems-001DT000		Team for the	folder create e SalesForce t Specialty Co	<mark></mark> d in FileCloud	
Search File	C					
Name			Туре	Size	Modify D	Download
New Folder			Folder		Nov 29, 2	4
Dbfile.txt			txt	1 B	Nov 29, 2	Ŧ

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

service appendix	inge Q. Search AppExchange		V ()	
Home Recom	mended for You Solutions by Type Product Collections	Industry Collections Consultants 🎆 Ohana	•••	
Scalable, FREE	s for Salesforce APP Substants Input: The Trusted, Ball Up England, Ball Up England, COMPONENT Salesforce COMPONENT Salesforce Sa	Free So Free Address	olutions for Everyone.	
PICK UP WH LEFT OFF, M	Sharing	Skype Click-to-Call for Mac and PC FREE APP	APP Skype for Salesforce APP	
	Wondering how to	find the right solution? See our best tips and resources		
app'	Y'S PICKS FOR YOU SHOW MORE >	FEATURED SOLUTIONS SHOW M	ORE > TOP CATEGORIES	
S Cob	rowse.io 🗳 Mobify	Statem         accounting see           transp. tearsebuy transformation:         Accounting on Salestorce           ******         CORBULTANT	ed	
		D&B Optimizer	★ Enterprise Resource Planning	
COBROWSE.IO -	CO-BROWSING FOI APP APP APP APP	Accelerate Sales with Clean Lead, Contact & Account Data	App 🛨 Sales	
		CODED Composer	★ Customer Service	
		Engaging documents, presentations, and reports Trg it free		
		***** PAID APP ***** PAID	APP \star Marketing	
		Secure Data Collection Tyle Free NWN NewVoiceMedia	Thegration	
3B FORMS - FOR	ma, sorvers and emecalCOLATOR	FORMASSEMBLY	* Salesforce Labs	

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

substree appexchange	Q FlieCloud Enterprise Flie Sharing		8	9 🖸
Home Recommended for You	Solutions by Type Product Collections Industry Collections Consultants	Ohana		
	Apps			
Reset Apply Filters	4 Results			
Solution Type	LISTING	LATEST RELEASE	RATING	PRICE
Apps     Components	A FlieTree - View Any Attachment or Salesforce Flie	9/24/2018	*****(5)	Paid
<ul> <li>Components</li> <li>Flow Solutions</li> </ul>	DocuVault-Document Management for Salesforce	7/8/2018	****(30)	Paid
Prices	FileCloud Enterprise File Sharing	5/16/2019	****(0)	Paid
✓ Free				
Paid	PowerBox for Salesforce	8/18/2016	****(6)	Free
<ul> <li>Discounted for Nonprofits</li> </ul>				
Editions	Components			
	1 Result			
Essentials     Professional	LISTING	LATEST RELEASE	RATING	PRICE
Enterprise	AC Enterprise Ideas with Lightning Experience support	5/16/2019	*****(1)	Paid
<ul> <li>Unlimited</li> </ul>	ined i o o i iii			
<ul> <li>Performance</li> </ul>	Flow Solutions			
<ul> <li>Force.com</li> </ul>	FIOW SOLUTIONS 1 Result			
<ul> <li>Developer</li> </ul>	1 Result			
Ratings	LISTING	LATEST RELEASE	RATING	PRICE
×****	SlideShare Presentation (Flow Action)	8/31/2018	*****(1)	Free
✓ ★★★★★				
✓ ★★★★★				
✓ ★★★★★				
✓ ★★★★★				
Unrated				
Languages				
✓ Dutch				
<ul> <li>English</li> </ul>				
Finnish				
French				
<ul> <li>German</li> </ul>				
Danish				
✓ Italian				
Japanese				
✓ Korean				
<ul> <li>Portuguese</li> </ul>				
Duccian				

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

			<b>V O</b>
			per year 🛛 Get 🗄 Now
2 Pachad 075 anno - 100 - 100 - 100	an i anna	◎日 ■ ? ● ● 8 RATING LISTED 0 大大大大大(0) 7/22/20	X JAJEST RELEASE
	Where do you wa	nt to install this package?	FileCloud directly from
	Before you install in a producti	on org, we suggest testing in a sandbox.	Nes stored in FileCloud from +premise, public or hybrid Cloud Interface within
	Install where you or your	roduction Environment users work, including developer orgs. all in Production	
		Ill in a Sandbox py of a production org	
•	lof	tall in Sandbox	
		Cancel	
		Key benefits: • Upload, download, access and share remote files fro • Files can be stored in on-premise or public cloud (An accessed securely inside salesforce from anywhere. • Share files and clouborate with team members, ever • Integrate Salesforce with vesting file servers along w	

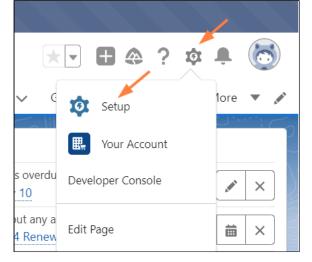
4. Select **Install for All Users** and click **Install**. Wait for the installation to complete.

In 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 Admins Only       Install for All Users         Install for Admins Only       Install for All Users         Install for Specific Profiles         Install for Admins Only       Install for All Users         Install for Specific Profiles         Install	Installed: 19.2 (19.2)       New Version: 19.2 (19.2)         Install for Admins Only       Install for All Users         Install for Admins Only       Install for All Users         Install for Specific Profiles       Install for Specific Profiles         The Description       CodeLathe       19.2         Description       Sharing         With FlieCloud, users can securely access, share files stored in FlieCloud from Salesforce. FlieCloud makes files stored in any on premise, public or hybrid cloud available within Salesforce. Embed the FlieCloud interface within Salesforce	By CodeLathe	oud Enterprise File	Sharing	
Install for Admins Only       Install for All User       Install for Specific Profiles         Install for Admins Only       Install for All User       Install for Specific Profiles         App Name       Publisher       Version Name       Version Number         FlicCloud Enterprise File       CodeLathe       19.2       19.2         Sharing       Description         With FileCloud, users can securely access, share files stored in FileCloud from Salesforce. FileCloud makes files stored in any coordinate within Salesforce. Embed the FileCloud interface within Salesforce records.	Install for Admins Only       Install for All Users       Install for Specific Profiles         Install for Admins Only       Install for All Users       Install for Specific Profiles         Install for Admins Only       Install for All Users       Install for Specific Profiles         App Name       Publisher       Version Name       Version Number         FileCloud Enterprise File       CodeLathe       19.2       19.2         Sharing       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.	An earlier version is insta Installed: 19.2 (19.2) Ne	talled. It can be upgraded while   ew Version: 19.2 (19.2)	preserving the existing data.	
FileCloud Enterprise File CodeLathe 19.2 19.2 Sharing 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 Enterprise File CodeLathe 19.2 19.2 Sharing 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.	Install for Admins Only	C Install for All Users	Install for Specific Profiles	
Sharing 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.	Sharing  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.	App Name Publisher	Version Name	Version Number	
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.	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.		19.2	19.2	
		With FileCloud, users can securely access, sh any on-premise, public or hybrid cloud avail: records.			

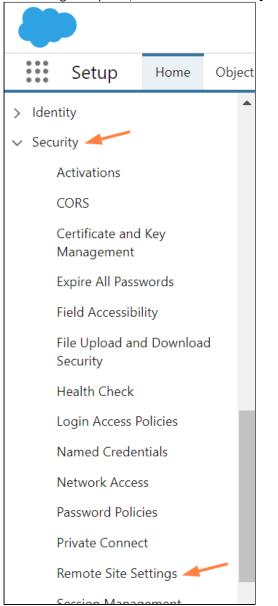
				Q	Search Setup			
Setup	Home	Object Manager 🗸						
		▲ \\	RIC	The ALL ANNUA THE	/!\\\\$_']1(////		A THUR	1111:17
Q Quick Find			SETUP					
Setup Home			Installed Packages					
Lightning Experience T	ransition							
Assistant		Instal	led Packages					
Lightning Usage		On AppExc	hange you can browse, test drive, dowr	nload, and install pre-built apps and components r	right into your salesforce.com enviro	nment. <u>Learn More abou</u>	t Installing P	<u>ackages</u> .
Manage Subscription			omponents are installed in packages. A icking Deploy.	ny custom apps, tabs, and custom objects are init	tially marked as "In Development" a	nd are not deployed to yo	our users. Th	is allows
ADMINISTRATION		Depending	on the links next to an installed packag	e, you can take different actions from this page.				
> Users		To remove	a package, click Uninstall. To manage	your package licenses, click Manage Licenses.				
> Data		Installed	l Packages					
-		Action	Package Name	Publisher	Version Number	Namespace Prefix	Status	Allow
> Email		Uninstall	the resonance of the set of					
PLATFORM TOOLS		Uninstall	±					-
✓ Apps			and the second second					
App Manager		Uninstall	*					
AppExchange M	larketpla	ce in the second s	the first on our to the					
> Connected App	s	Uninstall	<b>*</b>					
> Lightning Bolt		Uninstall	4					
		Uninstan						
> Mobile Apps			FileCloud EFSS	CodeLathe	19.2	FileCloud	Free	N/A
✓ Packaging		Uninstall	Description	CodeLathe	19.2	FlieCloud	Free	N/A
Installed Pack	kages		With FileCloud Enterprise Sharin	o, users can securely access, share files stored in		ud Enterprise Sharing ma		
Package Man	ager	Uninstall						
> Feature Settings			Salesione.com Ortivi Dashbuard	15				
> Einstein		Uninsta	lled Packages					
> Objects and Fields		No unins	talled package data archives					

#### FileCloud EFSS appears under Installed Packages.

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.

	Sandbox: newSandbox   <u>Log_out</u>
	* 🖬 🚓 ? 🌣 单 🐻
	Q Search Setup
Setup Home Object M	anager 🗸
> Identity	SETUP
✓ Security	Remote Site Settings
Activations	
CORS	All Remote Sites Help for this Page 😶
Certificate and Key Management	Below is the list of Web addresses that your organization can invoke from salesforce.com. To add another Web address, click New Remote Site.
Expire All Passwords	View: All Remote Sites V Create New View
Field Accessibility	
File Upload and Download	New Remote Site
Security	Action Remote Site Name + Namespace Prefix Remote Site URL Active Created By Created Date
Health Check	
Login Access Policies	and seen a Representation of the last
Named Credentials	
Network Access	A   B   C   D   E   F   G   H   I   J   K   L   M   N   O   P   Q   R   S   T   U   V   W   X   Y   Z   Other All
Password Policies	
	📕 Q 💵 😪 🕲 🐂 🥥 🤨 🏥 🗐

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

	Sandbox: newSandbox   <u>Log out</u>	
	Q Search Setup	
Setup Home Object N	Aanager 🗸	
File Upload and Download Security Health Check	SETUP Remote Site Settings	
Login Access Policies	Remote Site Edit Help for this Page 🥹	
Named Credentials	Enter the URL for the remote site. All s-controls, JavaScript OnClick commands in custom buttons, Apex, and AJAX	
Network Access	proxy calls can access this Web address from salesforce.com.	
Password Policies	Remote Site Edit Save Save & New Cancel	-
Private Connect		
Remote Site Settings	Remote Site Name	
Session Management	Remote Site URL https://my-filecloud-url.com	
Session Settings	Disable i Protocol Security	
Sharing Settings	Description	
Trusted URLs		
Trusted URLs for Redirects	Active 🗸	
View Setup Audit Trail		
Setup Assistant	Save & New Cancel	-

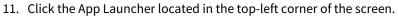
The remote FileCloud site is listed in the **All Remote Sites** view.

$\odot$	emote Site Se	ettings		
All Rer	note Sites	ノービュンリノナグ		
elow is the	list of Web addresses	that your organiza	ation can invoke from salesforce.co	om. To add another Wel
View: AI	I Remote Sites V Creat	e New View		
				A B C
				New Remote Site
Action	Remote Site Name ↑	Namespace Prefix	Remote Site URL	New Remote Site
Action Edit   Del	Remote Site Name ↑	Namespace Prefix	Remote Site URL	New Remote Site
	Remote Site Name ↑	Namespace Prefix	Remote Site URL https://my-filecloud-url.com	New Remote Site

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.

	Sandbox: newSandbox   <u>Log out</u>
	★       ▼       ★       ?       ☆       ₽
Setup Home Object M	1anager 🗸
File Upload and Download Security Health Check	Serup Session Settings
Login Access Policies	Cross-Site Request Forgery (CSRF) Protection
Network Access	<ul> <li>Enable CSRF protection on GET requests on non-setup pages i</li> <li>Enable CSRF protection on POST requests on non-setup pages i</li> </ul>
Password Policies	Content Security Policy protection
Private Connect	Override Restriction on Accessing Email Templates in Salesforce Classic Using Internet Explorer
Remote Site Settings	Enable Stricter Content Security Policy i
Session Management	Lightning Locker API Version
Session Settings	Use security 57.0 V i
Sharing Settings	API version
Trusted URLs	Lightning Web Security
Trusted URLs for Redirects	Use Lightning Web Security for Lightning web components and Aura components i
View Setup Audit Trail	XSS protection



-			Q, Searc	h Setup									$\star$	- 🖬 ? 🌣 🐥
5etup Home Object	Manager 🗸													
Q. Quick Find		ETUP Installed Packages	CANNAN INNA ANGA IN	NNS-111-7777	4-5 UU 17 - N	S. 111115	ING ANN	~111 _///	2-5 HET ( )	ANANA <i>JUNIT</i>	/1!\\\s='11		11,>>	A STANNA THUS
ightning Experience Transition	Installs	ed Packages			>	. ) \ `~.				1112-12	$\Box \bigtriangledown$			Help for this Pag
ightning Usage		•												
Ianage Subscription		ange you can browse, test drive, download, and insta mponents are installed in packages. Any custom app						i customize before de	ninsing Yau and deploy	u the components individually i	ution the other:	fashuras is	neturo or te	a appexch
anage subscription	group by click	king Deploy.		ed as in Dereighnen a	na are not deproyee to y	u usus. n	is anona you to wat and	continue before de	proying. Too can depro-	y the components incitiating t	using the other		and or as	. Opposed
DMINISTRATION		n the links next to an installed package, you can take package, click Uninstall. To manage your package li												Visit AppExchang
Users	Installed I		consos, ont manage Licenses.											
Data	Action	Package Name	Publisher	Version Number	Namespace Prefix	Status	Allowed Licenses	Used Licenses	Expiration Date	Install Date	Limits	Appa	Tabs O	bjects AppExchange Ready
Email	Uninstall	· strage italite	Publisher	version Number	realizespace Prette	Status	Allowed Licenses	Used Licenses	Expiration Date	inter card	<ul> <li>Image: A state of the state of</li></ul>	Apps 0	0	0 Not Applicable
LATFORM TOOLS	Uninstall	*		-		-	-	-	-			0	0	0 Passed
Apps														
App Manager	Uninstall	A										0	1	1 Passed
AppExchange Marketplace		the West on one to be transition in a												
Connected Apps	Uninstall	*	Contract of the			-						1	3	15 Passed
	Uninstall								-		1	0	0	1 Not Applicable
> Lightning Bolt	Uninstall	<b>A</b>					-	-		100000000000000000000000000000000000000		0	0	0 Passed
> Mobile Apps		the state of the s	CodeLathe		FileCloud	-	N/A	N/A	11/4	7/24/2019 11:41 AM		1		
<ul> <li>Packaging</li> </ul>	Uninstall	EleCloud EFSS Description		19.2		Free	N/A	N/A	N/A	7/24/2019 11:41 AM	Ý	1	2	2 Passed
Installed Packages		With FileCloud Enterorise Sharing, users can se			ud Enterorise Sharino m		_					0		0 Not Applicable
Package Manager	Uninstall	and a second sec					-	-	-		*	0	U	<ul> <li>Not applicable</li> </ul>
Feature Settings		Salestorice.com Ceon Dashibitarius												
Einstein	Uninstalle	ed Packages												
Objects and Fields	No uninsta	iled package data archives												
Events														
Process Automation														
User Interface														
Custom Code														
Development														

			Q Search Setup				📧 🖬 ? 😤 🛛
Setu	App Launcher		Search apps or items			[	Visit AppExchange
Quick Fin	✓ All Apps						ŕ
thing Elper stant thing Use t	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	
/INISTRA isers ata	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 Ughtning Experience		Bulk Object Field Creator	cha
mail TFORM To pps	FileCloud EFSS						tes
App Ma	✓ All Items						
> Connec							
> Lightnin > Mobile							
> Lightnin > Mobile ~ Packagi							
> Lightnin > Mobile - < Packagi: Insta							
> Lightnin > Mobile > Packagi Insta Packa							
> Lightnin > Mobile - V Packagi: Insta Packa ieature Sett							
> Lightnin > Mobile ; < Packagi Insta Pack: Feature Sett Einstein				1			
<ul> <li>&gt; Lightnin</li> <li>&gt; Mobile -</li> <li>&gt; Packagin</li> <li>Instain</li> <li>Packa</li> <li>Feature Sett</li> <li>Einstein</li> <li>Objects and</li> </ul>							
Pack: Feature Set: Einstein Objects and Events Process Auti				1			
<ul> <li>Lightnin</li> <li>Mobile -</li> <li>Packagii</li> <li>Insta Packa</li> <li>Packa</li> <li>Pack</li></ul>							

12. From the App Launcher, click FileCloud EFSS.

### Installation is complete.

	All 💌 🔍 Search Accounts and more		★ 🖬 ? 卒 🐥
FileCloud EFSS Accounts v Cases v Contacts v L	eads V Opportunities V Chatter FileCloud Configure FileCloud		
C CHERNIC ANNIA MILLE JUNE C CH		- JUNS 2110 COMPANY AND AND COMPANY	
Accounts Recently Viewed 🔻 👎			New Imp
ems · Updated a few seconds ago		Q. Search this list	\$• II• C / C
	✓ PHONE	✓ ACCOUNT OWNER ALIAS	×
	* Phone	* ACCOUNTOWNER ALIAS	

# Configuring FileCloud with Salesforce

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

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

<b>↓</b>		
	Server Storage Authentication Admin Email Endpoint Backup Licen	ise
_	Third Party Integrations Misc Reset	
	Salesforce SIEM reCAPTCHA McAfee MVISION CASB ICAP DLP Micros	soft Tea
	AutoCAD Viewer	
	Salesforce Integration Settings	
	Enable Salesforce integration	
	Turn on Salesforce Integration	
	Client Secret	
	Salesforce Client Secret, which has to be provided in the Salesforce client app to allow authentication	
	Generate Secret	
	Supported Salesforce object types	
	account,lead,contact,opportunity,case	
	Specifies which Salesforce Object types will be automatically handled in FileCloud [Comma separated list of object types]	
	Salesforce Team Folder Name	
	Salesforce	
	Name of the main directory under which all files/folders related to Salesforce objects wi be stored	ill

- 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.

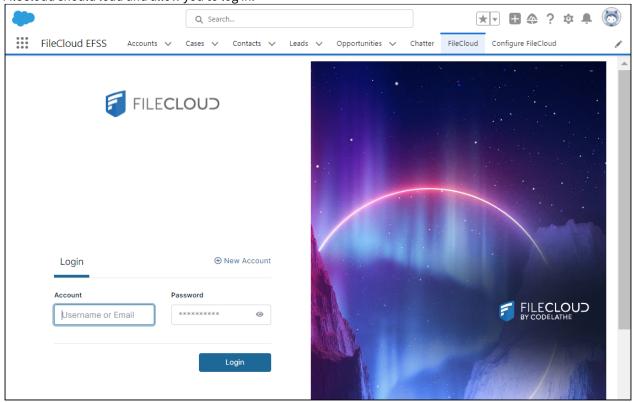
c. Under OAuth policies, in the Permitted Users drop-down list choose Admin approved users are preauthorized.

Connected App FileCloud EFSS		
Connected App Edit		
F		Version 22 Description
Basic Information		
Start URL	i	
OAuth Policies		
Permitted Users Enable Single Logout	All users may self-authorize  All users may self-authorize Admin approved users are pre-authorized	
Session Policies		
Timeout Value	None Y	
Custom Connected App Handler		
Apex Plugin Class Run As	S i	
User Provisioning Settings		
Enable User Provisioning 1		
	Save	

- 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.

F		All 💌 🔍 Search Salesforce
FileCloud EFSS Accounts 🗸	Cases $\checkmark$ Contacts $\checkmark$ Leads $\checkmark$ Opportunities $\checkmark$ Chatter	FileCloud Configure FileCloud
FileCloud Settings		
Edit FileCloud Settings	Save	
Connection Settings		
	Client Secret	
	Save	

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



# **SIEM Integration**

### (i) 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

Enable SIEM integration	Irrn on SIEM Integration
SIEM Integration Method	TCP Receiver
SIEM Server Host	https://arsight.domain
SIEM Server Port	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
	Test connection Send Test Message Validate Mappings

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

LEEF	~
Select Message Format	
.EEF Version	
1.0	~
Select LEEF format version	
.EEF 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	<ul> <li>Specifies the SIEM Integration method. Following options are available:</li> <li>TCP Receiver - messages are sent to the specified SIEM server endpoint (host and port) via TCP socket connection</li> <li>UDP Receiver - messages are sent to the specified SIEM server endpoint (host and port) via UDP socket connection</li> <li>Syslog - messages are written directly to the Syslog, which can be imported by the SIEM server</li> </ul> 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	<ul> <li>Specifies the SIEM Message format. The following formats are available:</li> <li>CEF - Common Event Format</li> <li>LEEF - Log Event Extended Format</li> <li>NOTE: SIEM software provider should specify supported formats in the SIEM documentation.</li> </ul>
LEEF Version (LEEF Format only)	<ul> <li>Specifies the version of the LEEF format message. Available versions:</li> <li>1.0</li> <li>2.0</li> </ul>
LEEF Message Delimiter (LEEF Format only)	The delimiter to be used for LEEF messages. The options are <b>whitespace</b> and <b>tab</b> . Choose the option that is compatible with the SIEM tool you are using.
Enable Audit Trail	Specifies whether Audit records should be processed and send to the SIEM Server. Please check the Managing SIEM mappings section for more details.
Enable System Alert Trail	Specifies whether System Alerts generated within FileCloud should be processed and send to the SIEM Server. Please check the Managing SIEM mappings section for more details.
Test Connection (TCP and UDP integration only)	Tests connection to the server specified by the Host and Port. NOTE: All settings have to be saved first. Connection tests are based on the <i>currently</i> 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.
	NOTE: All settings have to be saved first. Connection tests are based on the <i>currently</i> saved settings.
Validate Mappings	Validates all defined mappings. Please check the Managing SIEM mappings section for more details.

### Managing SIEM Mappings

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

### SIEM Mappings - general rules

### Create and access SIEM mappings files

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

Windows	Linux (later than Ubuntu 14.04)	Linux (earlier than Ubuntu 14.04)
c:\xampp\htdocs	/var/www/html	/var/www
Navigate to the following directory		

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.

```
'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.

Sample System Alert Mappings

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

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

As a literal value (string or number)

#### Sample System Alert Mappings

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

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

#### Sample System Alert Mappings

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

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

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

#### Sample System Alert Mappings

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

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

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

### Shared properties

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

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

Property	Description	Values
ts	Operation timestamp	Timestamp

## Audit mappings

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

### **Shared Audit Properties**

Property	Description	Values	
request	Request payload	The full request payload provided as a collection of key-value pairs that can be extracted in the mapping. Each operation carries a unique request.	
		The request can be mapped as a full object, and its info will be sent to the SIEM server as a string. For example: `'request' => '\$request'`, will be sent as `{"op":"loginguest","userid":"john.doe","password":"xxx"}`	
		Each field can also be sent individually if provided in the mapping: `'loggedUser' => '\$request.userid'`, where `userid` is one of the parameters of the request.	
response	Response payload	Similar to the request, the response provides a collection of key-value pairs that can be extracted in the mapping or sent as a string.	
		Each operation has a different response, so it is better to use this for dedicated rules.	
		NOTE: Responses are not stored in audit by default, and they have to be enabled in <b>Admin &gt; Settings &gt; Admin (Audit Settings section) &gt; Audit Logging Level (FULL)</b> ,	
		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.	
userAgen t	The User-Agent that triggered the operation	NOTE: Web browser is used as a generic user-agent for all web browsers.	

Property	Description	Values
userNam e	Name of the user that triggered the operation	
operation	Name of the operation that was triggered	
resultCod e	Result of the operation	1 - the operation was performed successfully (for example, login attempt was successful, a file was deleted)
		0 - operation failed (for example, login was not possible, a file was not deleted due to invalid permissions)
recordId	A MongoDB id of the audit entry	This is a MongoDB ObjectId
hostnam e	A name of the host	The name of the current host. This allows SIEM to differentiate tenants.

### **Operation-specific Audit Properties**

Property	Description	Values	Supported operations
auditArea	Provides information about the system area of the operation	Name of the system area	Currently only supported for operations from the following groups: • workflows • retention
serviceId	Additional information about the operation target	Carries additional information about the operations such as the name of the workflow or the id of the retention policy that was updated	Available only when the auditArea field is present
bandwidt h	Information about the size of the file	File size in bytes	Available for the following operations: • upload (file upload operation) • downloadfile

Property	Description	Values	Supported operations
realpath	File or folder realpath	FileCloud's original location of the file/folder, for example. / johndoe/document/internal/ doc.txt	Available only for retention-related and dlp operations
metadata	A list of non-empty, custom attributes assigned to the file or folder	Any non-empty attributes assigned by the Custom metadata sets as a result of the Smart Classification rule	<ul> <li>The following operations are supported:</li> <li>downloadfilemulti - Download multiple files</li> <li>downloadfile - Download single file</li> <li>getaudio - Play audio file</li> <li>getfsslideimage - View image file</li> <li>docconvert - Open/view file</li> <li>quickshare - Quick share</li> <li>addusertoshare - Add specific users to share</li> <li>addgrouptoshare - Add specific groups to share</li> <li>setallowpublicaccess - Make share public (after sharing only with certain users/groups)</li> </ul>
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:

```
'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'
       ]
   ]
];
// 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'
       ]
   ]
];
// 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'
        ]
    1
```

```
// 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'
       1
   ]
];
// 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'
       ]
   ]
1;
//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
       1
```

```
]
];
//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 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'
       ]
   ]
];
$mappings[] = [
   'id' => 'adduser',
   'prefilter' => [],
    'map' => [
       'eventClass' => 'Users',
       'eventName' => '$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
       ]
   ]
];
// 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.

Property	Description	Values
siemArea	System area where the alert was raised	One of the following values: SiemArea::INFECTED_FILE SiemArea::INVALID_FILE_TYPE SiemArea::AV_CHECK_FAILED SiemArea::UNHANDLED_EXCEPTION SiemArea::DISK_SPACE_EXCEEDED SiemArea::INDEX_DB_FAILURE SiemArea::RMC_INVALID_POLICY SiemArea::BACKGROUNDING_FAILED SiemArea::METADATA_HEALTH_CHECK SiemArea::ZIP_BACKUP_FAILURE SiemArea::SIEM_SERVER_CONNECTION SiemArea::DLP_SHARE_KILL
level	System alert critical level	One of the following values: SysAlert::SYSALERT_LEVEL_MELTDOWN SysAlert::SYSALERT_LEVEL_CRITICAL SysAlert::SYSALERT_LEVEL_WARNING SysAlert::SYSALERT_LEVEL_INFORMATION

## Supported properties

Property	Description	Values				
type	Type of system alert	One of the following values:				
		SysAlert::SYSALERT_TYPE_DLP_SHARE_KILL_FAILED SysAlert::SYSALERT_TYPE_DLP_SHARE_KILLED SysAlert::SYSALERT_TYPE_CODE_CONFIGURATION_ERR ROR SysAlert::SYSALERT_TYPE_CODE_AV_FAILURE SysAlert::SYSALERT_TYPE_CODE_SIGNATURE_FAILURE SysAlert::SYSALERT_TYPE_CODE_EXCEPTION SysAlert::SYSALERT_TYPE_CODE_ERROR SysAlert::SYSALERT_TYPE_QUOTA_EXCEEDED				
description	Alert description					
notes	Alert notes					
username	The user whose actions raised the alert					
alertContext	Additional information, related to the alert	Various contexts, depending on the Alert. For example:				
		<b>file</b> - filename for the File version deletion operation <b>filePath</b> - file location for the Infected file				
		fileName - file name for the Infected file				

## Sample mappings

## Sample System Alert Mappings

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

```
'severity' => 10,
        'extension' => [
            'user' => '$username',
            'ip' => '$ip'
        ]
    ]
];
//AV system alert - infected file found
$mappings[] = [
    'id' => SiemArea::INFECTED_FILE,
    'map' => [
        'eventClass' => 'System Error',
        'eventName' => '$description',
        'severity' => [[SiemConversionHelper::class, 'getSysAlertSeverity'], ['$level']]
,
        'extension' => [
            'user' => '$username',
            'ip' => '$ip',
            'path' => '$alertContext.filePath',
            'file' => '$alertContext.fileName'
        ]
    ]
];
//Type mismatch report
$mappings[] = [
    'id' => SiemArea::INVALID_FILE_TYPE,
    'map' => [
        'eventClass' => 'System Error',
        'eventName' => '$description',
        'severity' => [[SiemConversionHelper::class, 'getSysAlertSeverity'], ['$level']]
,
        'extension' => [
            'user' => '$username',
            'ip' => '$ip',
            'path' => '$alertContext.file'
        ]
    ]
];
```

# SIEM Integration with Splunk Enterprise

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

## Splunk Server Configuration

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

- 1. Log in to Splunk.
- 2. Click Add Data.
- 3. In the **TCP** row, click **Add new**. An **Add Data** wizard opens.
- 4. In the **Select Source** screen, in **Port**, enter the port that will receive messages from FileCloud. In **Source name override**, enter a name for the FileCloud server.

Local Event Logs Collect event logs from this machine.	Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More [2]				
Remote Event Logs Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.		TCP	UDP		
Files & Directories Upload a file, index a local file, or monitor an entire directory.	Port ? 8889 Example: 514				
HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.	Source name override ?	FileCloud Test Server			
TCP / UDP >	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:		
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		Select New
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 [2]	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 [2]	Method ?	IP DNS Custom

7. Go to the next screen in the wizard, **Review**, and check your settings.

8. Click next to complete your TCP Data Input entry configuration.

## Setting up FileCloud to connect to the Splunk Server

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

- 1. 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.
- 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.

SIEM Integration S	jettings
Enable SIEM integration	✓ Turn on SIEM Integration
SIEM Integration Method	TCP Receiver <ul> <li>Select SIEM Integration Method</li> <li>Integration Method</li></ul>
SIEM Server Host	192.168.0.17 Specify the SIEM Server Host
SIEM Server Port	8888 SIEM Server Port
SIEM Message Format	CEF ~
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
	Test connection Send Test Message Validate Mappings

#### For the other settings, see SIEM Integration.

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

i	Time	Event				
+	9/20/22 12:16:27.000 AM	CEF:0 Cod			.3.5.18513  <mark>FC<sup>-</sup>Test</mark>   <mark>Test</mark> MSG 1	
		Туре	$\checkmark$	Field	Value	Actions
		Selected	$\checkmark$	source 🔻	FileCloudLabs	~
			$\checkmark$	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 🕶	:III-I_II	~
				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**:

New Search					Save As • Cr	eate Ta	ole View Close
Invalid login attem	ot				Report Alert		All time 👻 🔍
✓ 10 events (before 9/2)	8/22 10:27:39.000	PM)	No Event Sampling	•	C Existing Dashboard	Ŧ	Smart Mode ▼
Events (10) Pattern	s Statistics	Visua	lization		New Dashboard		
Format Timeline 🔻	- Zoom Out	+ Zoo	m to Selection	KDeselect	Event Type		1 day per colum
		List	▼ ✓ Format	20 Per Page 🕶			
< Hide Fields	i≣ All Fields	i	Time	Event			
SELECTED FIELDS a recordid 10		>	9/28/22 3:28:40.000 AM	CEF:0[CodeLathe]FileCloud]21.3.5.18513]login]Invalid login attempt[2]user=johnsmith [p=192.168.137.1 samplehost=fileCloud]abs.com recordId=63334ee82f5900008 recordId = 63334ee82f5900008900344b   source = FileCloudLabs   sourcetype = FileCloud	8900344b		
a source 4         3:28-4           a sourcetype 1         > 9/15/2           INTERESTING FIELDS         1:58-3		9/28/22 3:28:40.000 AM	CEF:0[CodeLathe[FileCloud]21.3.5.18513]login]Invalid login attempt[2]user=johnsmith [pr192.168.137.1 samplehost=filecloud]abs.com recordid=63334ee82f5900008 recordid=63334ee82f59000089003449   source = FileCloudLabs   sourcetype = FileCloud	89003449			
		9/15/22 1:58:33.000 AM	CEF:0[CodeLathe]FileCloud[21.3.5.18513]login]Invalid login attempt[2]user=admin ip=152,168.137.1 samp]ehost=fileCloudlabs.com recordId=63221645a86660000000 recordId = 63221649a866600000007366   source = FileCloud Server   sourcetype = FileCloud	73e6			
a host 1 a index 1 a ip 1		>	9/15/22 1:58:33.000 AM	CEF:0[CodeLathe]FileCloud[21.3.5.18513]login]Invalid login attempt[2]user=admin ip=152.168.137.1 samplehost=fileCloudlabs.com recordId=63221649a866000000073e4   source = FileCloud Server   sourcetype = FileCloud	73e4		
# linecount 1 a punct 1 a samplehost 1		>	9/14/22 11:38:33.000 PM	CEF:0[CodeLathe[FileCloud]21.3.5.18513]login Invalid  ogin attempt[2 user-admin ip=192.168.137.1 samplehost=fileCloudlabs.com recordId=6321f579c031000033006da   source=19216813740   sourcetype=FileCloud	66da		
a splunk_server 1         >         9/14/22           a timestamp 1         >         9/14/22           a user 2         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=fileCloud]abs.com recordId=6321f578c031000033006668 [ source=19216813740 [ sourcetype= FileCloud	66d8		
+ Extract New Fields		>	9/9/22 10:12:14.000 PM	CEF:0[CodeLathe]FileCloud[21.3.5.18513]login]Invalid login attempt[2]user=johnsmith 1p=192.168.137.1 shost=filecloudlabs.com recordId=631b49be3a578008b28038 recordId = 631b49be3a570000b2003877   shost = filecloudlabs.com   source = 192.168.13740   sourcetype = FileCloud	8f7		
		>	9/9/22 10:12:14.000 PM	CEF:0[CodeLathe]FileCloud]21.3.5.18513]login]Invalid login attempt[2]user=johnsmith ip=192.168.137.1 shost=filecloudlabs.com recordId=631b49bea41a0002b0035cc is shost=filecloudlabs.com is ource = 192.168.13740 is ourceype = FileCloud	5dc		
		>	9/9/22 10:00:01.000 PM	CEF:0[codeLathe]FileCloud]21.3.5.18513]login]Invalid login attempt[2]user=johnsmith ip=192.188.137.1 shost=filecloudlabs.com recordId=631b46e1a41a00002b003566 [ shost = filecloudlabs.com   source = tcp3888   sourcetype = FileCloud	5d6		
		>	9/9/22 10:00:01.000 PM	CEF:0[codeLathe[FileCloud]21.3.5.18513[login]Invalid login attempt[2]user=johnsmith ip=192.168.137.1 shost=fileCloud]abs.com recordId=631b46e1a41a00002b0035 computed a 531b46e1a41a00002b003564 _ chost = Benefaultible com _ compute = Kenefaultible com _ compute = FileCloud	5d4		

#### 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 e	every hour 🔻
	At 0 - minutes past the hour	
Expires	24	day(s) 🔻
Trigger Conditions		
Trigger alert when	Numbe	er of Results 🔻
	is greater than ▼	5
Trigger	Once	For each result
Throttle ?		
Trigger Actions		
	+ Add Actions 🔻	

When triggered	<ul> <li>Send emai</li> </ul>	I	Remove
	То		
		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	
		Trigger Time Attach PDF Allow Empty Attachment	
	Туре	HTML & Plain Text Plain Text	
			Cancel Save

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



# 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.

Device Management	Contraction Admin Database Email Endpoint Backup
	Third Party Integrations Misc Reset
Retention	Salesforce Anti-Virus SIEM reCAPTCHA McAfee MVISION CASB ICAP DLP
○ Smart DLP	
Smart Classification	reCAPTCHA Integration Settings
✓ Compliance Center	Select to enable Captcha
MISC.	reCAPTCHA Host Name
Audit	www.google.com
. Alert	If planning to use a non-default reCAPTCHA site, enter the site hostname in the format
🔒 User Locks	<www.hostname.com>.</www.hostname.com>
凸 Workflows	reCAPTCHA Site Key
≣ Reports	•••••••••••••••••••••••••••••••••••••••
Q Federated Search	Enter reCAPTCHA Site Key
🗂 Metadata	reCAPTCHA Secret
SETTINGS	······
Settings	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.

Server Storage Aut	hentication	Admin	Database	Email	Endpoint Backup	License
Third Party Integrations	ServerLink	Misc	Reset			
Salesforce SIEM	reCAPTCHA	McAfe	e MVISION CAS	SB IC	AP DLP	
McAfee MVISION (	CASB Integra	ation Se	ttings			
Enable FileCloud CASB integration	☑ Select to ena	ble McAfe	ee MVISION CAS	В		
FileCloud CASB API Key	FileCloudCa	sbDefault	АріКеу			
	Set FileCloud C	ASB API K	еу			

- 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
<b>DLP</b> Features	Content- aware Public Shared Link, or Pure Public Shared link Policy evaluation for Item Shared event
	Content-ware Policy evaluation for File Upload/Update event
	Response Actions: Incident
	Remove Shared link
	Email notification
	Send user notification
	Delete

## FileCloud events and McAfee responses

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

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

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

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

- register
- deregister

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

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

# ICAP DLP

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

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

## What is ICAP?

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

## Integrating ICAP DLP with FileCloud

- 1. Open a browser and log in to the Admin Portal.
- 2. On the left navigation panel, click Settings.
- 3. Select the Third Party Integrations tab.
- 4. Select the ICAP DLP tab.
- 5. Fill in the fields according to the table below.
- 6. Click Save.

rver Storag	e Authentication	Admin	Email	Endpoint Backup	License	Policie
nird Party Integ	rations Misc	Reset				
Salesforce S AutoCAD Viewer		McAfee	MVISION CAS	ICAP DLP	Microsoft	Teams
Server Local IF	)					
0.0.0.0						
Specify this se	rver's local IP (must n	ot be 127.0.0.1	)			
ICAP Remote I	Hostname					
Specify the IC/	AP server remote hos	name				
ICAP Port						
11344						
	AP server port. for regular ICAP or 1	1344 for secur	e ICAP server			
	for regular term of r					
Secure ICAP						
Enable if the second	ne ICAP server is runn	ing with SSL o	r TLS protoco	ls		
File Size Limit						
Units 🕶	25				MB	
Files larger tha	an this size will not be	scanned				
ICAP Service n	ame					
reqmod						
Enter the nam						

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

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

# **Microsoft Teams**

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

	Microsoft Teams		Q Search
Activity	Teams	=	MT General Posts Files Wiki +
Chat Teams	Your teams MT Marketing Team General	•••	vasine
Calls			Here is the file of user names that we talked about.
Apps ?			FileCloud Users (1).csv Shared from FileCloud Password: 1hkdpg
	Coo Join or create a team	ŝ	Open

To set up integration:

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

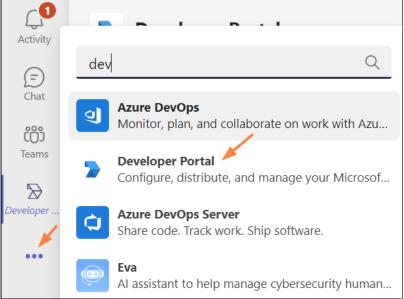
# For MS Teams Admins: Configuring FileCloud in Teams

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

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

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

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



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

Develoj	per Portal Home Apps Tools App Studio Chat About	
< Tools	+ New Bot	
Bot manager Bots are conversation designing Teams bo	nal apps that perform a specific set of tasks. They communicate with users, respond to the	r q

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

Add bot		
FileCloud App Bot		/
	Cancel	Add

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

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

<b>Developer Portal</b> Home Apps	Tools App Studio Chat About
< Bots	
FileCloud App Bot   Configure Client secrets	Configure Update icon and other bot properties at the Bot Framework Portal. Endpoint address Bot endpoint address https://mysite.filecloud.com/core/msteamsbot Save Revert

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

g. Click Bots.

Developer Portal Home Apps	Tools App Studio Chat About
< Bots	
SileCloud App Bot	<b>Configure</b> Update icon and other bot properties at the Bot Framework Portal.
Configure Client secrets	Endpoint address
	Bot endpoint address https://core/msteambo
	Save Revert

- 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.

pps <b>Tools</b> Chat 2 more ~
ic set of tasks. They communicate with users, respond to their question n more about designing Teams bots.
Bot ID
ARTING THE REPORT ARRANGED

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

a. In the **Developer Portal**, click the **Apps** tab, and then click **New App**.

Microsoft Teams			Q Search		
> Developer Portal	Home Apps	Tools	App Studio	Chat	About
+ New app ↑ Import a	app				
<b>Apps</b> Select an app to see more information	on or update its co	nfiguratio	ns.		

#### An **Add App** window opens.

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

Add app		×
FileCloud app		
	Cancel	Add

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

c. Fill in the form, and click **Save**.

Depending on your MS Teams environment policies, you may not be required to enter a value for

## Application (client) ID.

	-	
FileCloud app		Basic information This is the information users see on your app details page in Teams. See best practices.
Overview	$\sim$	App names
Dashboard		A short name (30 characters or less) is required. Include a longer version if your preferred name exceeds 30 characters.
Analytics		Short name - 30 characters or less*
Configure	$\sim$	FileCloud app
Basic information		Full name - up to 100 characters (optional)
Branding		Enter a longer, preferred name (displays if more than 30 characters)
App features		
Permissions		App ID
Single sign-on		Your app's identifier that's generated by Microsoft and unique to your org.
Languages		[D
Domains		
Advanced	>	Descriptions
Publish	~	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.
App package		Short description - 80 characters or less*
http://www.upp.com/		FileCloud app for MS Teams

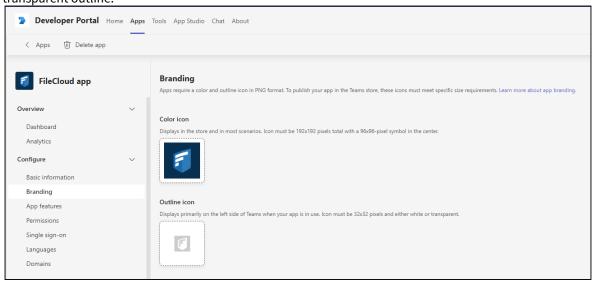
## d. In the navigation pane, click **Branding**. The **Branding** screen opens.

> Developer Portal Home	Apps	Tools App Studio Chat About
く Apps 🖞 Delete app		
FileCloud app		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.
Overview	$\sim$	Color icon
Dashboard Analytics		Color rcon Displays in the store and in most scenarios. Icon must be 192x192 pixels total with a 96x96-pixel symbol in the center.
Configure Basic information	$\sim$	
Branding		
App features		Outline icon
Permissions		Displays primarily on the left side of Teams when your app is in use. Icon must be 32x32 pixels and either white or transparent.
Single sign-on		2
Languages		
Domains		
Advanced	>	Accent color
Publish	$\sim$	Displays for primary actions and other app UI components.
App package		
Publish to org		
Publish to store		·

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

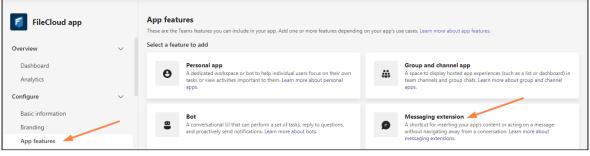


f. Upload the first image for Color icon, and the second image for Outline icon.
 You may use custom images, but they must be 192px X 192px for the color image and 32px X 32px for the transparent outline.



#### 4. Set up your MS Teams bot.

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



The Messaging Extension screen opens.

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

FileCloud app		Messaging extension Shortcuts for inserting app content or acting on a message without navigating away from the state of the state o
Overview	~	Messaging extension (bot) ID
Dashboard Analytics		<ul> <li>Select an existing bot</li> </ul>
Configure	~	FileCloud App Bot ( )
Basic information Branding		O Enter a bot ID
App features		X0000000(-)000(-)000(-)000(-)000000000
Permissions		
Single sign-on		
Languages		Save Revert
Domains		

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

FileCloud app	Messaging extension Shortcuts for inserting app content or acting on a message without navigating aw
Overview $\checkmark$	Messaging extension (bot) ID
Dashboard	
Analytics	Select an existing bot
Configure $\checkmark$	FileCloud App Bot )
Basic information	Create a new bot
Branding	O Enter a bot ID
App features	X0000000-X000-X000-X000-X00000000
Permissions	
Single sign-on	Select give users the ability to modify messaging extension settings
Languages	Users can reconfigure the app
Domains	Command
Advanced	Define what the messaging extension can do. Include search commands (i
Publish 🗸	+ Add a command
App package	Preview links
Publish to org	Allows users to insert content-rich links (such as an Adaptive Card) from a
i donan to org	+ 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 m about messaging extension commands.	essaging extension. Le	arn more
Choose the type of command you want to configu	ire.	
O Search		
Action		
Choose a parameter type.		
Static parameters		
Oynamic parameters		
Command ID*		
FileCloud		
Command title* FileCloud		
Command description*		
Share from FileCloud		
	Cancel	Save

Make default		
Select the contexts in which the c	ommand works.	
Command box		
Compose box		
Message		
Initial dialog title*		
Share from FileCloud		
Dialog width*		
medium		
Dialog height*		
medium		
Initial webview url*		
https:/	/core/msteamsbot	
	Cancel	Save

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

+ Add a domair	
Save	Revert

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

Developer Portal	Home Apps	Tools App Studio Chat Abc	ut
< Apps 🛛 Save	9 Revert	+ Add a command	
FileCloud app		Users can reconfigure th Command Define what the messaging ex	e app tension can do. Include search commands (ins
<b>Overview</b> Dashboard	~	Command ID	Name
Analytics		FileCloud	FileCloud ()
Configure	~	+ Add a command	
Basic information Branding			rich links (such as an Adaptive Card) from a d
App features		+ Add a domain	
Permissions			
Single sign-on		Save	

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

Add domain				
er		Cancel	Add	з <u>с</u>
ne cloud (i)	action	Current		

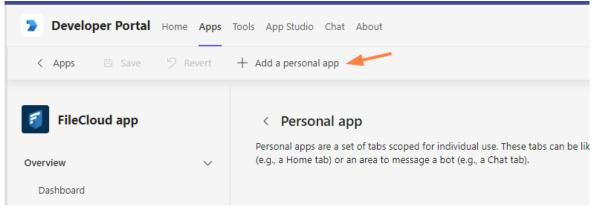
#### i. In the Messaging Extension screen, click Save.

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

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

> Developer Portal Ho	ome Apps	Tools App Studio Chat About
< Apps + Add a featu	ure =	
FileCloud app		App features These are the Teams features you can include in your app. Add one or more features depending on your ap
Overview	$\sim$	Messaging extension
Dashboard		-
Analytics		Updated: October 03, 2022 dccf1200-b7f7-4ec3-942c-eefc324a5278
Configure	$\sim$	
Basic information		Select a feature to add
Branding		
App features		A dedicated workspace or bot to help individual users focus on their own
Permissions		tasks or view activities important to them. Learn more about personal apps.
Single sign-on		
Languages		

k. Click Add a personal app.



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

URL

٦

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

Add a tab to yo Define a set of tabs to di Learn more about tabs.	-	onal app Ir personal app. An About tab is created automatically by default.
Name*		
FileCloud		
Entity ID*		
Content URL*		
https:/		
Website URL		
		Cancel Confirm
ck <b>Confirm</b> . he <b>Personal app</b> scre	en, click <b>S</b>	Save.
FileCloud app	~	< Personal app Personal apps are a set of tabs scoped for individual use. These tabs can be like a web (e.q., a Home tab) or an area to message a bot (e.q., a Chat tab).

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

 $\sim$ 

Name

FileCloud

Save

Revert

Add a personal app

m.

Dashboard

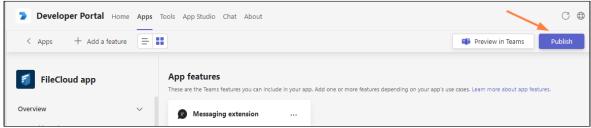
Analytics

Branding App features

Basic information

Configure

a. Click Publish.



The **Publish your app** dialog box opens. b. Click **Download the app package**.

	Download the app package
Ŧ	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
IJ	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. **Microsoft Teams** Q Search Q Activity С Apps Manage your apps Apps (=) Chat Search Q + Get more apps  $\overline{\uparrow}$  Upload an app 🗄 Apps  $\overline{}$ ເຕິງ Developer Portal Teams . Microsoft Corporation Built for your org ::\* Built with Power Platform Calendar Tasks by Planner and To Do . Microsoft Corporation Featured ••• Popular on Teams OneNote Microsoft Corporation Top picks What's new Praise Best selling Microsoft Corporation Categories Approvals E Apps Microsoft Microsoft Corporation В ? Workflows Updates  $\sim$ Þ Help Microsoft Corporation Manage your apps  $\downarrow$ 

## The Upload an app dialog box opens.

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

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

## Your file explorer opens.

- Kequest submitted to your admin

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

 f. As the Teams administrator, approve and publish the app.
 For more information, see https://docs.microsoft.com/en-us/MicrosoftTeams/manage-apps#approve-acustom-app.

The app's **Status** changes to **Approved**, and the app becomes available in your company's app store.

7. Next enable MS Teams integration in FileCloud

# For FileCloud Admins: Enabling Integration with MS Teams

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

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

## Note regarding Chrome and Edge users

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

Contact FileCloud Support to set your SameSite value to None,

## To enable FileCloud integration with MS Teams:

- 1. 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).

Server	Storage	Authentication	Admin	Email	Endpoint Backup	License	Policies	
Third Part	ty Integration	ns Misc R	eset					
Salesford	e SIEM	reCAPTCHA	McAfee N	IVISION CAS	B ICAP DLP	Microsoft	Teams	
AutoCAE	0 Viewer							
Micros	soft Teams	s Integration S	Settings					
		S Teams integration	-					
		FileCloud integrat		rosoft Teams				
FileClo	oud MS Teams	s Bot Id						
Set Fil	eCloud MS Te	ams Bot Id						
Use bi	rowser sessior	n expiry						
		rowser session time	eout only					

5. Click Save.

# Setting Up AutoCAD File Preview with Autodesk Viewer

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

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

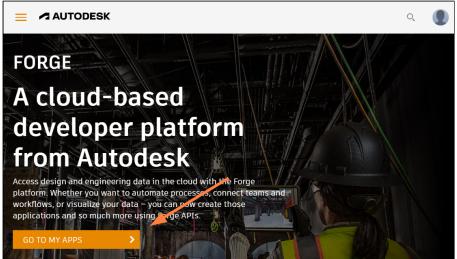
After you configure FileCloud integration with Autodesk Viewer, when users preview 3D and 2D model data file types, they are shown in Autodesk Viewer.

# Setting up integration of FileCloud and Autodesk Viewer

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

To integrate FileCloud with Autodesk Viewer:

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



#### 4. Click **CREATE APP**.

	۹ 🌒
My Forge Apps	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.

Provide basic information about your app. App Name FileCloud Integration	
FileCloud Integration	
App description	
FileCloud integration with AutoDesk.	
Callback URL What is this ?	
Callback URL <u>What is this ?</u> https://myfilecloudurl.com/core/cadviewer	

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

	B	Ę	l
Autodesk Construction Cloud API	BIM 360 API	Data Exchange API	Data Management API
$\sim$			
Cසූට Design Automation API	لالم Model Derivative API	Premium Reporting API	Reality Capture API
~1	(R)		
Token Flex Usage Data API	Webhooks API		

### 6. Click **CREATE APP**.

The screen lists your **Client ID** and **Client Secret**.

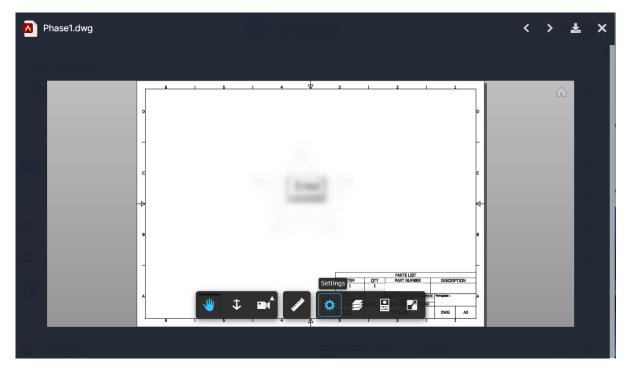
← Back to My Forge Ap	pps	
App informat	ion (Created on 03 May 2022)	
Basic information ab	out your app.	
Client ID	AynGeamQTFXywhs76qvL6HeJRs8GrTx1	
Client Secret	••••••••••••••••••••••••••••••••••••••	
App Name	FileCloud Integration	
Description	FileCloud integration with AutoDesk.	
Callback URL	https://myfilecloudurl.com/core/cadviewer	
APIs		
	able to access.	

- 7. In the FileCloud admin portal, go to **Settings > Third Party Integration > AutoCAD Viewer**.
- 8. Check Select to enable FileCloud integration with Autodesk viewer. Additional fields appear.
- 9. In API Secret, enter your Autodesk Viewer Client Secret.
- 10. In API key, enter your Autodesk Viewer Client ID.

→	Server Storage Authentication Admin Database Email Endpoint Backup License Policies SSO
	Content Search Web Edit Team Folders Third Party Integrations Misc Reset
	Salesforce SIEM reCAPTCHA McAfee MVISION CASB ICAP DLP Microsoft Teams AutoCAD Viewer
	Autodesk viewer
	Enable Autodesk integration
	Select to enable FileCloud integration with Autodesk viewer
	API Secret
	Specify the API Secret server remote hostname
	API key
	Specify the API key server remote hostname
	Region
	US 🗸
	Specify the region in wich Autodesk viewer is used

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

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



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

Preliminary.dwg	g
Choose a viewable	
	Model 2D View
> Te	3D View Sheets
(C) Rec	3D Elevation 3D Elevation (2)
	3D Elevation (3)
ing Site	
📲 She	

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

FileCloud Online Version 23.232 Third Party Integration Settings

# Al Integration

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

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

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

## To integrate FileCloud with OpenAI:

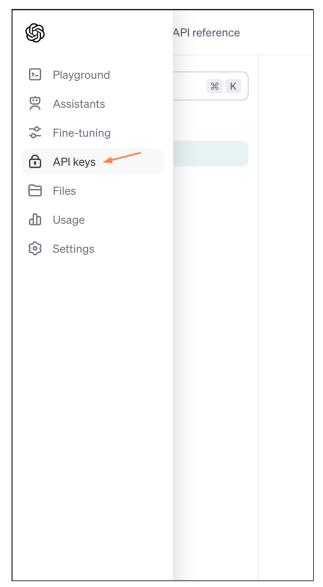
1. In the admin portal, go to Settings > Third Party Integrations > AI.

Server Stora	age /	Authentication	Admin	Email	Endpoint Ba	ckup L	icense
Third Party Inte	grations	Misc	Reset				
Salesforce	SIEM	reCAPTCHA	McAfee I	MVISION CA:	SB ICAP D	DLP Mi	icrosoft Te
AutoCAD View	er A	I					
Al Integrati	ion Set	tings					
Enable LLM I		ungo					
		ileCloud integra	tion with LLN	/I (Large Lang	guage Model).		
Notice							
Notice							
		\I-based large la					
classificati	ion will ca	ause the text co	ntent of files	classified usi	ng this metho	d to be	
classificati sent to th	ion will ca ird-party		ntent of files ature should	classified usi be used in a	ng this metho	d to be	
classificati sent to th	ion will ca ird-party	ause the text co services. This fe	ntent of files ature should	classified usi be used in a	ng this metho	d to be	
classificati sent to thi organizati	ion will ca ird-party	ause the text co services. This fe	ntent of files ature should	classified usi be used in a	ng this metho	d to be	
classificati sent to thi organizati Provider	ion will ca ird-party	ause the text co services. This fe	ntent of files ature should	classified usi be used in a	ng this metho	d to be	~
classificati sent to thi organizati	ion will ca ird-party ion's Info	ause the text co services. This fe rmation Security	ntent of files ature should	classified usi be used in a	ng this metho	d to be	-
classificati sent to thi organizati Provider OpenAl	ion will ca ird-party ion's Info	ause the text co services. This fe rmation Security	ntent of files ature should	classified usi be used in a	ng this metho	d to be	~
classificati sent to thi organizati Provider OpenAl Specify the L API Key	ion will ca ird-party ion's Info LLM provi	ause the text co services. This fe rmation Security	ntent of files ature should / and privacy	classified usi be used in a policies.	ng this metho	d to be	
classificati sent to the organizati Provider OpenAl Specify the L API Key	ion will ca ird-party ion's Info	ause the text co services. This fe rmation Security	ntent of files ature should / and privacy	classified usi be used in a policies.	ng this metho	d to be n your	
classificati sent to thi organizati Provider OpenAl Specify the L API Key	ion will ca ird-party ion's Info	ause the text co services. This fe rmation Security	ntent of files ature should / and privacy	classified usi be used in a policies.	ng this metho	d to be n your	<ul> <li></li></ul>
classificati sent to thi organizati Provider OpenAl Specify the L API Key Specify the A	ion will ca ird-party ion's Info LLM provi	ause the text co services. This fe rmation Security ider.	ntent of files ature should / and privacy	classified usi be used in a policies.	ng this metho	d to be n your	

Organization		
org-********************		
Optional - Specify the Org	anization ID.	
Custom URL		
Optional - Specify a custo	m endpoint URL to use.	
Check AI Credentials		
Test Credentials		

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

To get these values, log in to the OpenAI platform at https://platform.openai.com/login (you must have a valid OpenAI subscription) and click **API keys** in the left navigation panel.



The **API keys** page opens:

	after you generate the Do not share your API protect the security of	m.	that we do not display y	our secret API key	ys agair	ı	
protect the security of your account, OpenAl may also automatically disable any API key that we've found has leaked publicly.          NAME       KEY       CREATED       LAST USED ©         filecloud_test_key       Jun 14, 2023       Jul 20, 2023       Image: Create new secret key         postman test key       Nov 13, 2023       Never       Image: Create new secret key         H       Create new secret key       Image: Create new secret key       Image: Create new secret key         If you belong to multiple organizations, this setting controls which organization is used by default when making requests with the API keys above.       Image: Create new secret key	protect the security of		t in the browser or othe	client-side code	In orde	r to	
filecloud_test_key Jun 14, 2023 Jul 20, 2023  postman test key Nov 13, 2023 Never  r							
postman test key       Nov 13, 2023       Never       Image: Comparison of the c	NAME	KEY	CREATED	LAST USED 🛈			
+ Create new secret key  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_test_key		Jun 14, 2023	Jul 20, 2023	C	创	
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.	postman test key		Nov 13, 2023	Never	C	创	
when making requests with the API keys above.	Default organizat	ion					
FileCloud R&D	, ,		g controls which organi	zation is used by d	lefault		
	FileCloud R&D	\$					
Note: You can also specify which organization to use for each API request. See Authentication to learn more.	Note: You can also specify v	which organization to use for each	API request. See Authentica	tion 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, <b>you won't be able to view it again</b> through your OpenAl account. If you lose this secret key, you'll need to generate a new one.	
P	
Done	

- 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 OpenAl instance.
- 7. Click **Test Credentials** to confirm that **FileCloud** and **AI** are properly integrated.