



# Inline CASB Deployment Brief

**FORTINET®**

# Inline CASB

## Challenge

Employees using personal unmanaged devices to access corporate networks from new, disparate locations creates even more cloud security risks. Inline CASB provides cybersecurity protection against malware and phishing attacks, secures access to cloud services, and ensures cloud application security.

FortiGate Inline CASB consists of many components. The following table summarizes the different components and their benefits:

## FortiOS Documentation

- [Inline CASB examples](#)
- [Privilege control for Microsoft Outlook](#)
- [Tenant control for Microsoft Office 365](#)
- [Safe search enforcement for Google traffic](#)

- **Monitoring:** intercept traffic between users and SaaS applications and provides real-time visibility.
- **Configured profiles:** single control point where you can apply consistent security policies for all cloud services, ensuring unified security management and simplified policy administration.
- **Tenant control:** enforce policies that restrict access to specific tenants. With tenant control, you can segment Internal and external tenants to help protect data from being inadvertently shared outside approved environments. Provides real-time insights into tenant usage.
- **Domain control:** enforce conditional access based on location.
- **HTTP header manipulation:** inject headers needed for custom integrations, enabling seamless communication with cloud services that have specialized requirements.

## Key Features of the FortiGate Inline CASB Solution

Key features of the FortiGate Inline CASB solution include:



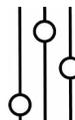
### TENANT CONTROL

- Granular access control
- Regulatory compliance
- Reduced security risk



### SAFE SEARCH

- Reduced risk of inappropriate browsing
- Reduced security risk
- Secure browsing



### ACCESS RULE

- Mitigation of insider risk
- Network traffic optimization
- Simplified policy management



### DOMAIN CONTROL

- Domain-based access control
- Prevention of personal usage
- Corporate policy enforcement

# Controlling and Monitoring SaaS Apps

**Inline CASB privilege control (access rules) gives granular control over SaaS application user activity.**

The following shows an example for configuring privilege control for GitLab. For a more detailed example, see [Privilege control](#).

Application: GitLab  
Status: Enabled

Privilege Control

User Activity	Action
create-merge-request	Allow
create-file	Block
create-branch	Monitor
modify-branch	Bypass
login	Allow
app	Allow
modify-file	Allow
create-repository	Allow

**Inline CASB tenant control enforces access restrictions by ensuring only authorized users from specific tenants or directories can access protected SaaS applications.**

Tenant control provides an additional layer of security and compliance. The following shows an example for configuring privilege control for Slack. For a more detailed example, see [Tenant control](#).

Application: Slack  
Status: Enabled

Privilege Control

User Activity	Action
login	Monitor
delete-message	Monitor
invite-people-to-channel	Monitor
create-channel	Monitor
remove-people-from-channel	Monitor
app	Monitor
delete-channel	Monitor
upload-file	Monitor

Custom Controls

Name	Match Criteria	Adjustment
SlackAllowedWorkspaces	slack.com	header new-on-not-found X-Slack-Allowed-Workspaces T01B4K1L5Y2

# Controlling and Monitoring SaaS Apps

Inline CASB Safe Search enforces content filtering by ensuring that only appropriate and Safe Search results display to users, helping to maintain a secure and compliant browsing environment.

The following shows an example for configuring Safe Search for YouTube. For a more detailed example, see [Safe search](#).

**Create SaaS Application Rules**

1 Select application ————— 2 Choose CASB controls

Application YouTube

Status  Enabled  Disabled

Application-Defined Controls

Safe search  moderate strict

Privilege Control

Set Action ▾

<input type="checkbox"/>	User Activity	Action
<input checked="" type="checkbox"/>	search	✓ Allow
<input type="checkbox"/>	app	✓ Allow

# SaaS Application Visibility

A policy with an Application Control profile can give SaaS application visibility with the help of cloud signatures.

Name	Category	Popularity	Risk	Behavior
Acrobat.Cloud_Download	Storage/Backup	★★★★★	■■■■■	Excessive-Bandwidth Cloud
Acrobat.Cloud_Upload	Storage/Backup	★★★★★	■■■■■	Excessive-Bandwidth Cloud
Act!	Business	★★★★★	■■■■■	Cloud
ActiveCampaign	Business	★★★★★	■■■■■	Cloud
Adobe.Connect	Collaboration	★★★★★	■■■■■	Cloud
Adobe.Connect_Meeting.Chat	Collaboration	★★★★★	■■■■■	Cloud
Adobe.Connect_Meeting.Remote.Control	Remote Access	★★★★★	■■■■■	Cloud
Adobe.Connect_Meeting.Share.Document.Upload	Collaboration	★★★★★	■■■■■	Excessive-Bandwidth Cloud
Adobe.Connect_Meeting.Share.My.Screen	Collaboration	★★★★★	■■■■■	Cloud
Adobe.Connect_Meeting.Share.Whiteboard	Collaboration	★★★★★	■■■■■	Cloud
Adobe.Creative.Cloud	Storage/Backup	★★★★★	■■■■■	Cloud

FortiOS supports the following cloud signature types:

- **Deep application control signatures:** require deep inspection. Logs contain additional information, such as SaaS username, video files played, and files uploaded and downloaded. FortiOS displays these signatures with a cloud icon beside the name.

Name	Category	Popularity	Risk	Behavior
Application signature 17/5715				
YouTube	Video/Audio	★★★★★	■■■■■	Cloud
YouTube.Downloader.YTD	Video/Audio	★★★★★	■■■■■	Excessive-Bandwidth
YouTube_Category.Control	Video/Audio	★★★★★	■■■■■	Cloud
YouTube_Channel.Access	Video/Audio	★★★★★	■■■■■	Cloud
YouTube_Channel.Control	Video/Audio	★★★★★	■■■■■	Cloud
YouTube_Channel.ID	Video/Audio	★★★★★	■■■■■	Cloud
YouTube_Comment.Posting	Video/Audio	★★★★★	■■■■■	Cloud
YouTube_HD.Streaming	Video/Audio	★★★★★	■■■■■	Excessive-Bandwidth
YouTube_Music	Video/Audio	★★★★★	■■■■■	
YouTube_Search.Safety.Mode.Off	Video/Audio	★★★★★	■■■■■	

The following shows a deep application signature for YouTube traffic:

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2024/12/17 15:55:41	10.211.255.213	74.125.168.73 (par10s45-in-f9.1e100.net)	YouTube_Video.Play	✓ Pass		Video Play
2024/12/17 15:55:10	10.211.255.213	173.194.0.137 (par21s26-in-f9.1e100.net)	YouTube_Video.Play	✓ Pass		Video Play
2024/12/17 15:55:10	10.211.255.213	173.194.0.199 (par21s28-in-f7.1e100.net)	YouTube_Video.Play	✓ Pass		Video Play
2024/12/17 15:54:27	10.211.255.213	74.125.105.167 (par21s25-in-f7.1e100.net)	YouTube_Video.Play	✓ Pass		Video Play
2024/12/17 15:54:19	10.211.255.213	173.194.3.7 (par10s47-in-f7.1e100.net)	YouTube_Video.Play	✓ Pass		Video Play

# SaaS Application Visibility

- **Cloud application that requires deep inspection:** provide additional granular control for some cloud applications. Details pane displays SSL Deep Inspection as a requirement.

The screenshot shows a table with columns 'Name' and 'Category'. A row for 'Dropbox\_File.Edit' is highlighted. A details pane is open over this row, displaying the following information:

- Dropbox\_File.Edit** (with logo)
- ID:** 44019
- Summary:** This indicates an attempt to edit a file on Dropbox.
 

Dropbox allows users to edit Microsoft Office files, such as Word, Excel, and PowerPoint. The signature detects that a user is editing a office file on Dropbox.
- Category:** Storage.Backup
- Risk:** [4 yellow squares]
- Popularity:** [5 yellow stars]
- Protocol:** TCP, HTTP
- Ports:** TCP/443
- Technology:** Browser-Based
- Behavior:** Excessive-Bandwidth, Cloud
- Vendor:** Other
- Requirements:** [lock icon] SSL Deep Inspection

The following shows a log for Dropbox\_File.Edit:

Summary		Logs						
Date/Time	Source	Destination	Application Name	Action	Application User	Application Details	Application ID	
2024/12/17 16:07:29	10.211.255.213	3.162.38.46	Dropbox_File.Edit	Block		File Edit	44019	

# SaaS Application Visibility

- **Cloud application that does not require deep inspection:** detects application with certificate inspection SSL/SSH profile.

The screenshot shows a security console interface. At the top, there is a search bar with "Application signature 1/5715". Below it, a card for "Blogger" is displayed. The card includes the Blogger logo, the name "Blogger", and the ID "30073". A summary states: "This indicates an attempt to access Blogger. Blogger is a free weblog publishing tool from Google, for sharing text, photos and video. It comes with built-in templates, themes and gadgets." Other details include: Category: General.Interest; Risk: (4 bars, 3 filled); Popularity: (5 stars); Protocol: TCP, HTTP, SSL; Ports: TCP/80, TCP/443, UDP/443; Technology: Browser-Based; Behavior: Cloud; Vendor: Google.

The following shows a sample log for the Blogger application signature:

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details	Application ID	Application Risk
2024/12/17 16:19:49	10.211.255.213	142.250.201.9 (mrs08s19-in-f9.1e100.net)	Blogger	✓ Pass			30073	■ ■ ■ ■
2024/12/17 16:15:49	10.211.255.213	142.250.201.9 (mrs08s19-in-f9.1e100.net)	Blogger	✓ Pass			30073	■ ■ ■ ■
2024/12/17 16:15:48	10.211.255.213	142.250.201.9 (mrs08s19-in-f9.1e100.net)	Blogger	✓ Pass			30073	■ ■ ■ ■

You can view cloud application usage per user in **FortiView Applications**.

The screenshot shows the "FortiView Applications by Bytes" interface. On the left, a summary card for "LinkedIn" is shown with a category of "Social Media", a risk level of 3 bars, and a total of 98.48 MB in bytes and 24,645 sessions. On the right, a line graph displays "Bytes Sent" (light green) and "Bytes Received" (dark green) over a 7-day period from Sat 14 to Fri 20. The graph shows a significant peak in usage on Tue 17. Below the graph is a table listing users and their usage statistics.

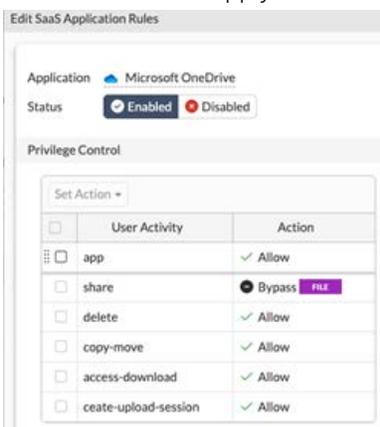
Source	Device	Threat Score	Bytes	Sessions
ian_wung - 10.1.2.135		0	607.39 kB	152
wayne_ethans - 10.1.2.178		0	599.4 kB	150
mirial_cullinae - 10.1.2.146		0	587.41 kB	147
alie_grace - 10.1.2.30		0	587.41 kB	147
luba_madden - 10.1.2.18		0	587.41 kB	147
carin_cota - 10.1.2.32		0	583.42 kB	146
brian_cappon - 10.1.2.43		0	583.42 kB	146
binfoh_nystrom - 10.1.2.63		0	575.42 kB	144
booking_shaw - 10.1.2.41		0	575.42 kB	144
kimberle_flikstein - 10.1.2.81		0	563.44 kB	141

# Deploying Inline CASB

## Best Practices

Consider the following best practices when deploying Inline CASB:

1. Inline CASB profile requires deep inspection. You must select a deep inspection profile on the firewall policy with the inline-casb profile attached to it.
2. For SaaS application visibility, enable cloud application control signatures on the firewall policy.
3. Inline CASB can allow bypassing unified threat management (UTM) functions based on privilege control. Based on the requirement, you can bypass some UTM functions. Here is a sample for bypassing File Filter for Microsoft OneDrive that can apply certain user groups.



4. Define clear policies based on user role, location, and device type.
5. For data protection, enable data loss prevention (DLP) based on data protection requirements. See [Data loss prevention](#).
6. Web Filter helps to cover giving control and visibility based on FortiGuard categories. See [Web filter](#).
7. Conduct regular policy reviews for any changes in compliance requirements or organizational changes.

## Deployment Examples

Review comprehensive [Inline CASB examples](#) for help facilitating your Inline CASB deployment:

- [Privilege control for Microsoft Outlook](#)
- [Tenant control for Microsoft Office 365](#)
- [Safe search enforcement for Google traffic](#)