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

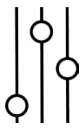
Key features of the FortiGate Inline CASB solution include:

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

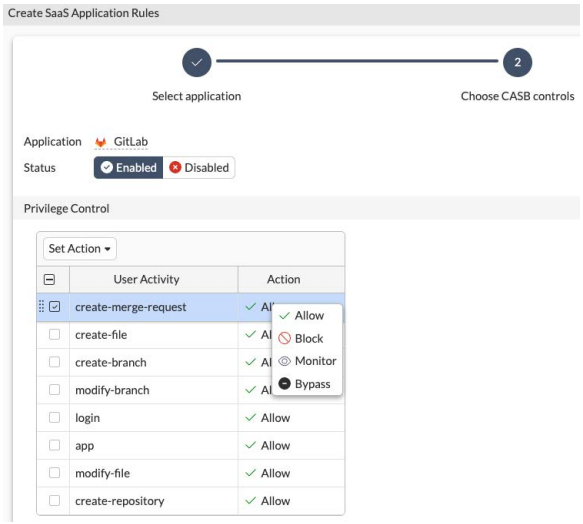
DOMAIN CONTROL

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

Controlling and Monitoring SaaS Apps

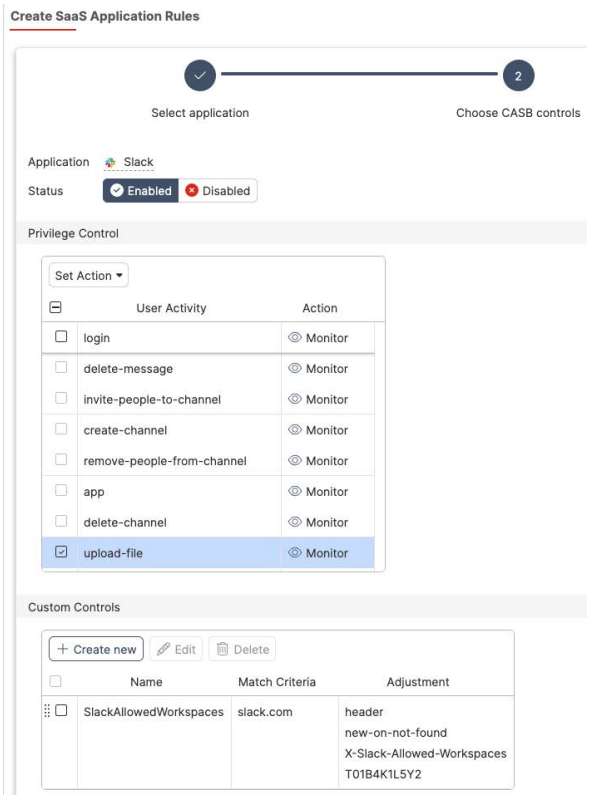
Inline CASB privilege control (access rules) gives granular control over SaaS application user activity.

The following shows an example for configuring privilege control for GitLab. For a more detailed example, see **Privilege control**.



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

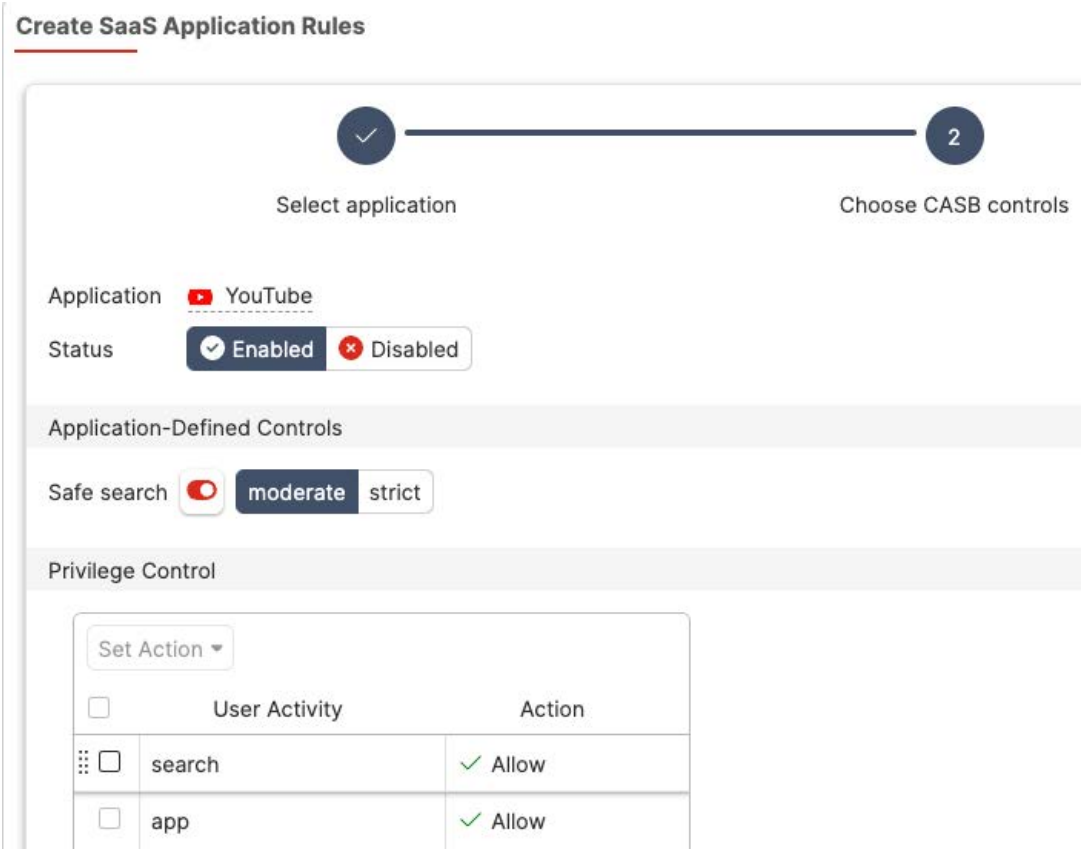
Tenant control provides an additional layer of security and compliance. The following shows an example for configuring privilege control for Slack. For a more detailed example, see **Tenant control**.



Controlling and Monitoring SaaS Apps

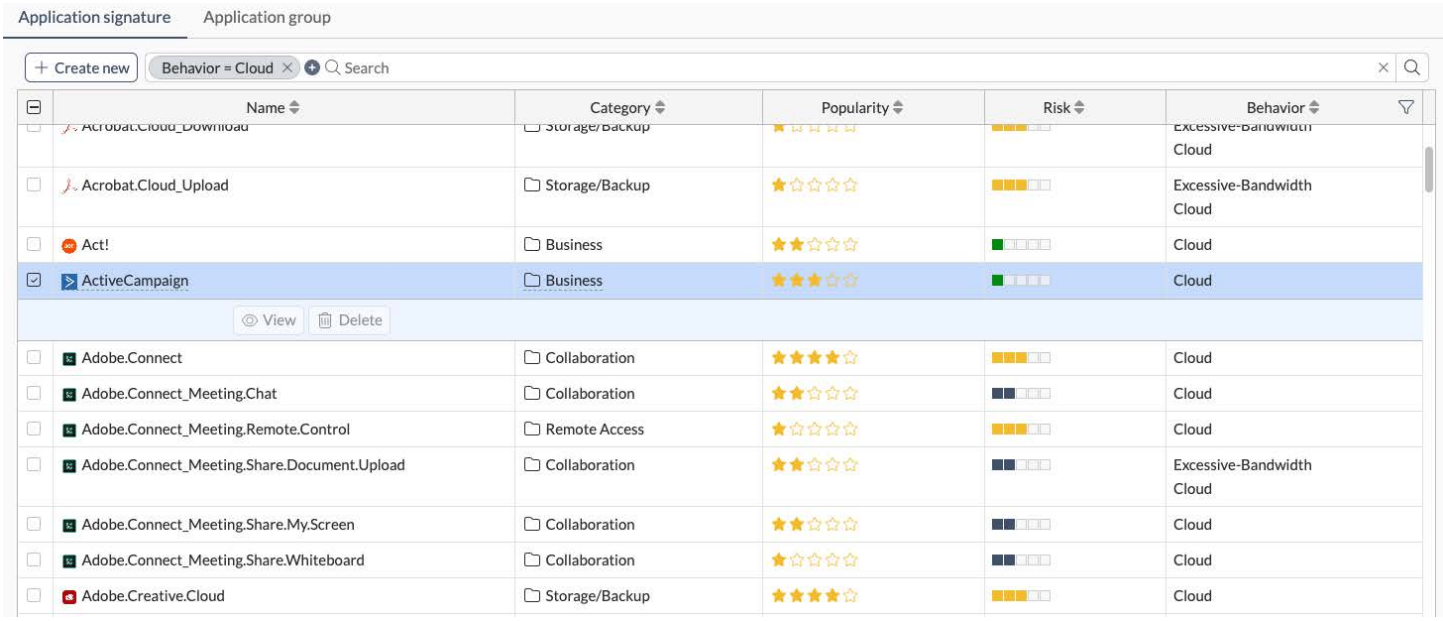
Inline CASB Safe Search enforces content filtering by ensuring that only appropriate and Safe Search results display to users, helping to maintain a secure and compliant browsing environment.

The following shows an example for configuring Safe Search for YouTube. For a more detailed example, see **Safe search**.



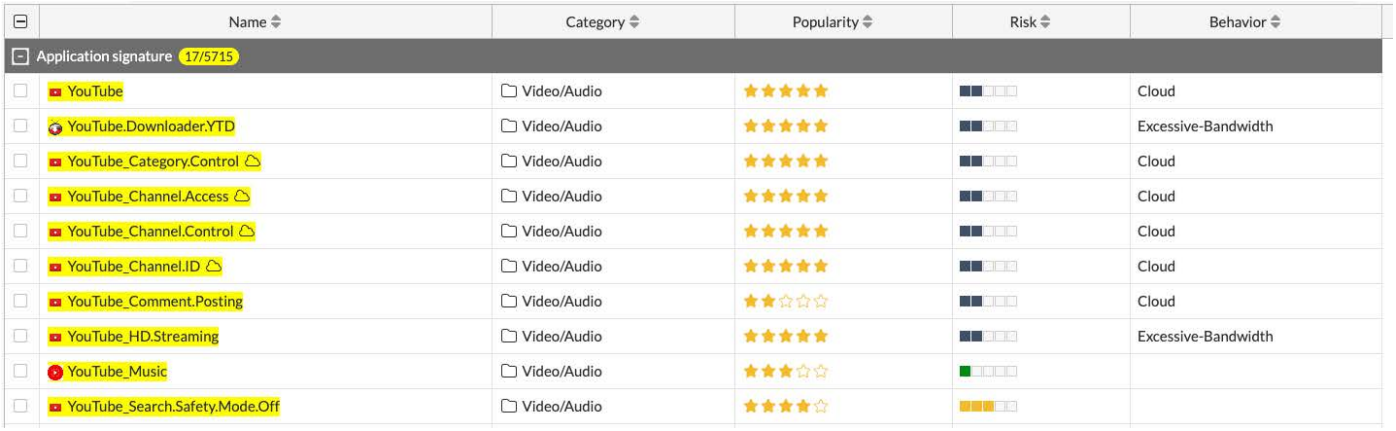
SaaS Application Visibility

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

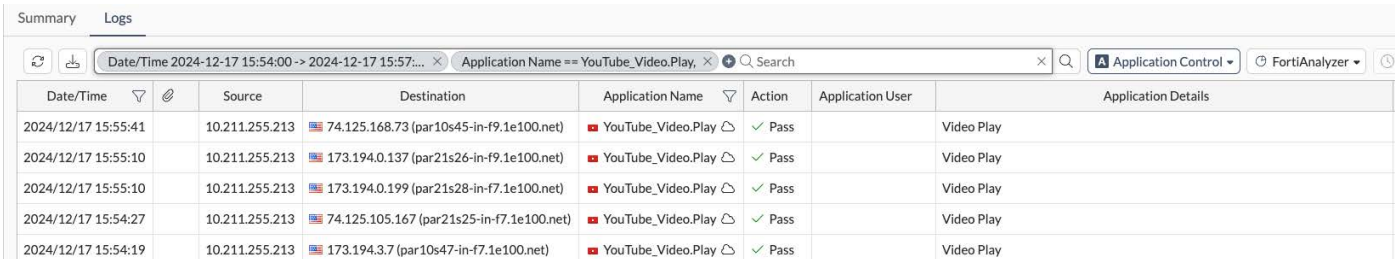


FortiOS supports the following cloud signature types:

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

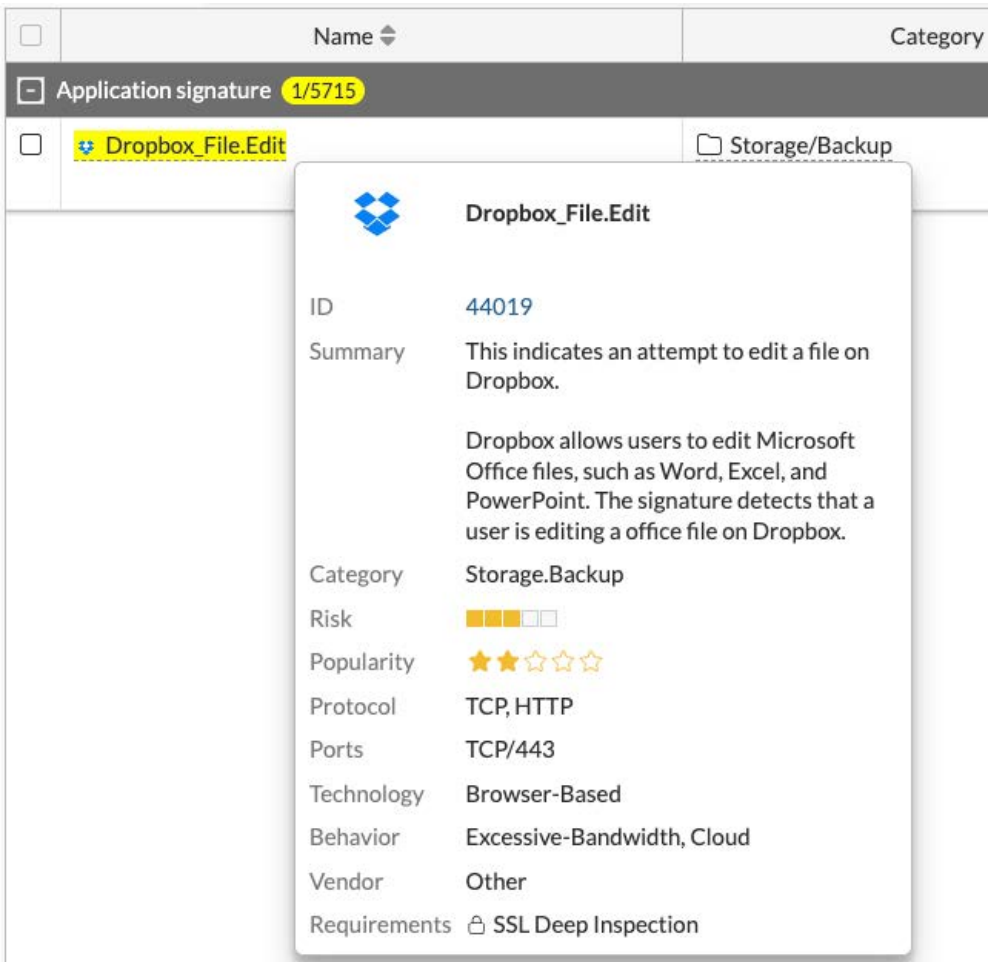


The following shows a deep application signature for YouTube traffic:

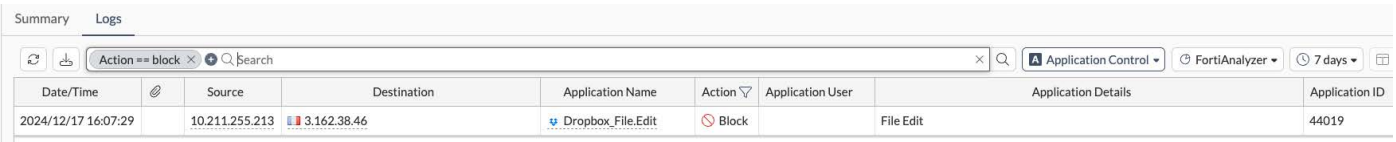


SaaS Application Visibility

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

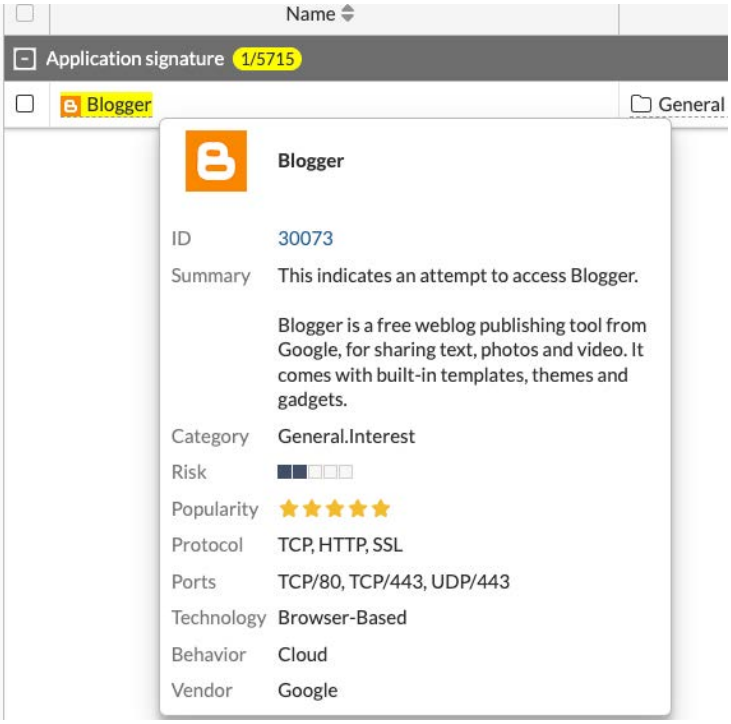


The following shows a log for Dropbox_File.Edit:

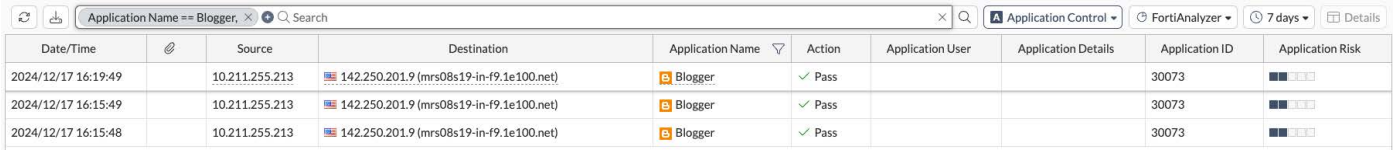


SaaS Application Visibility

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

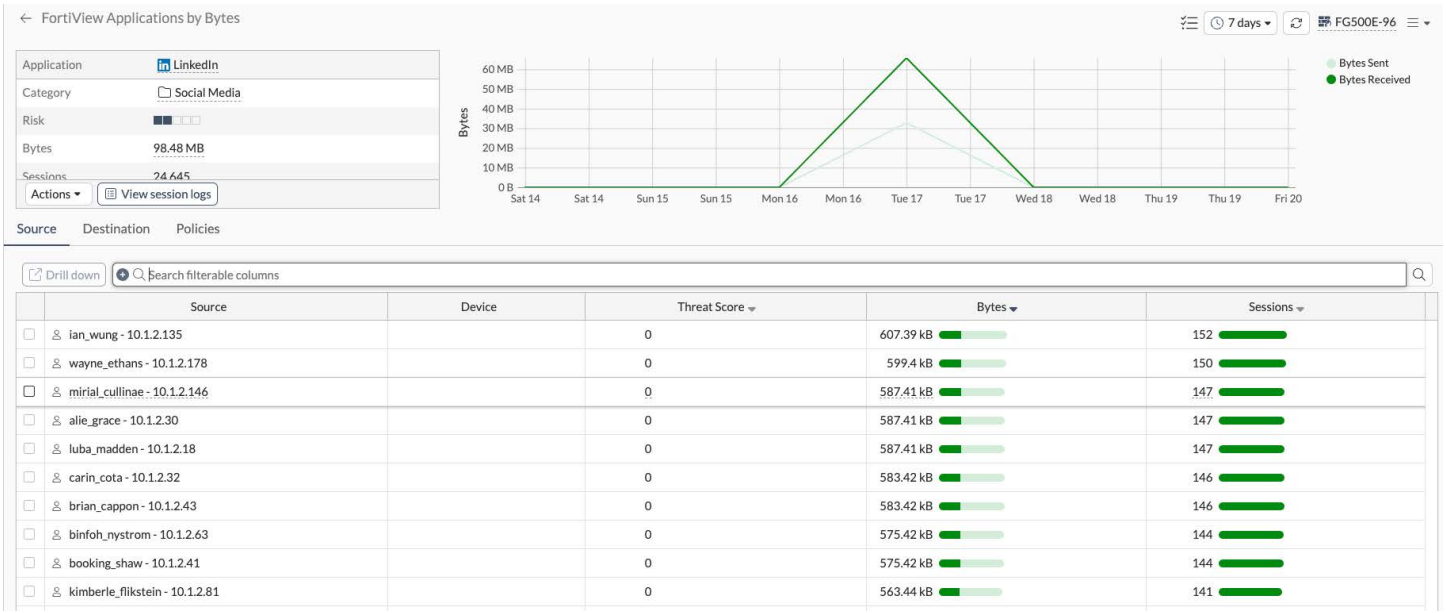


The following shows a sample log for the Blogger application signature:



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**.

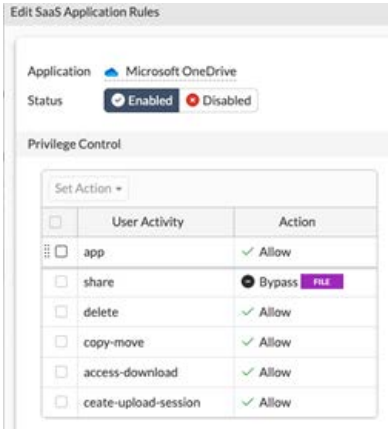


Deploying Inline CASB

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**