FortiSASE for Education

Deployment Brief

FortiSASE for Education

Challenge

In the education sector, organizations must protect staff and students regardless of where they are working: in school, at home, or elsewhere.

Having visibility into all traffic, including encrypted traffic, without compromising the user experience, is crucial.

FortiSASE provides features that are especially useful for education customers.

FortiSASE documentation

- 4-D documentation
- Architecture Guide
- SIA Agent-based Deployment
- SIA Agentless SWG Deployment

Key FortiSASE features for Education

SAFE SEARCH

Block inappropriate or explicit images from search results to restrict students from accessing mature content.

CYBERBULLYING AND SELF-HARM REPORTS

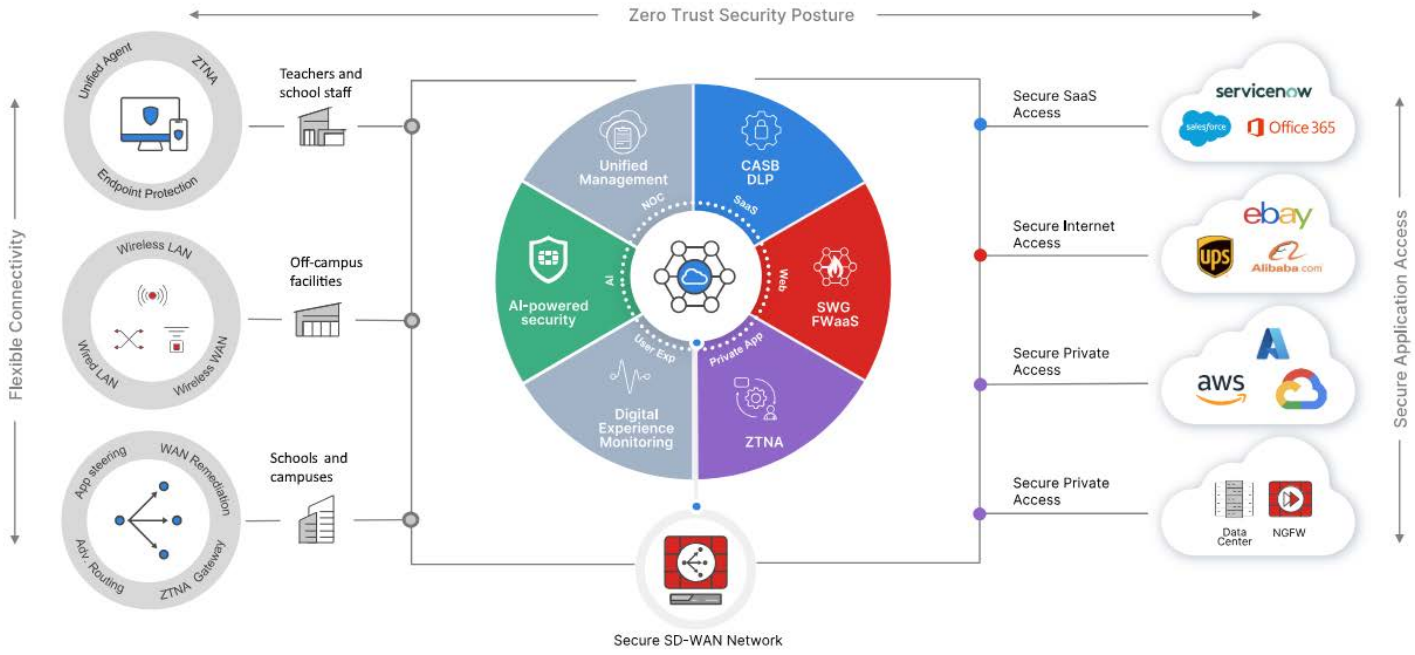
Generate reports to monitor behaviors that align with cyberbullying and self-harm indicators.

APPLICATION ACCESS CONTROL USING GOOGLE WORKSPACE

Secure students and staff from accessing non-approved cloud resources.

SWG BEHAVIOR CONTROL ON UNMANAGED DEVICES

Enforce secure web gateway (SWG) connectivity for selected endpoints with Chrome installed.



Safe Search

Enforcing safe search to restrict students from accessing mature content

Search engines provides a safe search feature that **blocks inappropriate or explicit images from search results**.

The safe search feature helps avoid most adult content that you want to prevent students and staff from accessing.

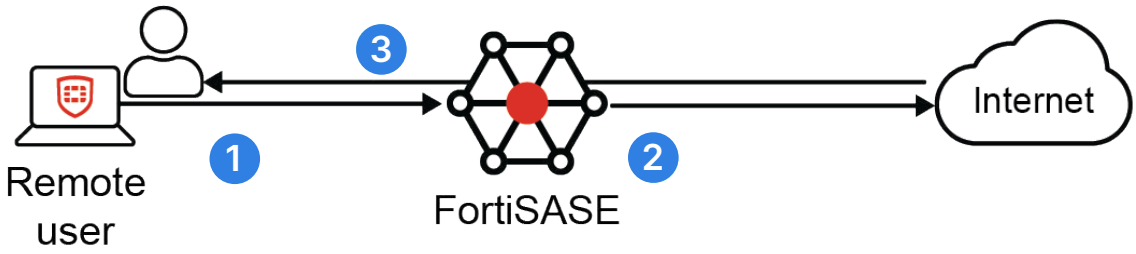
You can enforce safe search using the following FortiSASE security features:

Web Filter

See Enforcing safe search in web filter.

DNS Filter

See Enforcing safe search in DNS filter.



When you enable safe search, the following happens:

1. Remote user (FortiClient endpoint user or agentless SWG user) searches for an inappropriate term in a supported search engine.
2. FortiSASE receives the search request, modifies it to enable the safe search feature, and forwards the modified search request to the search engine.
3. Since the search term is inappropriate and flagged by the search engine's safe search feature, the search engine returns a limited search results page to the user.

FortiSASE supports safe search for the following search engines:

Cyberbullying and Self-Harm Reports

Using reports on cyberbullying and self-harm behaviors to identify potential risk

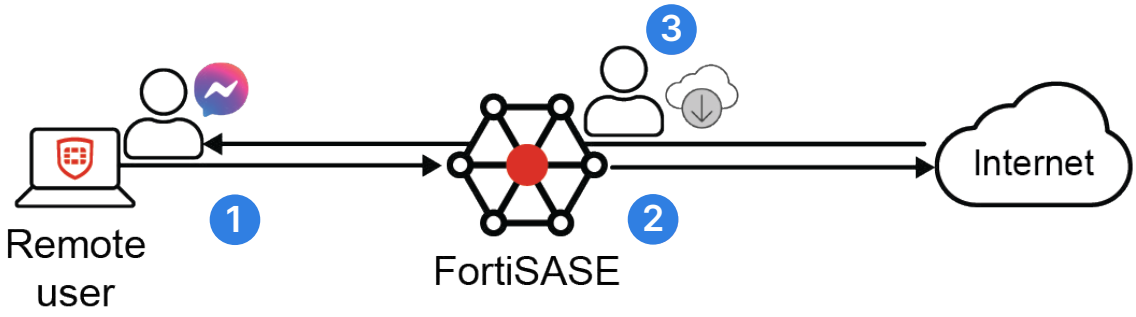
You can generate the following report types in FortiSASE that are of special interest in the education sector.
See **Report types** for supported FortiSASE report types.

Cyber-Bullying Indicators Report

Logs users exhibiting behavior that aligns with common cyberbullying indicators, such as use of offensive phrases on social media.

Self-Harm and Risk Indicators Report

Logs users exhibiting behavior that aligns with common self-harm and risk indicators, such as use of risky terms on social media.

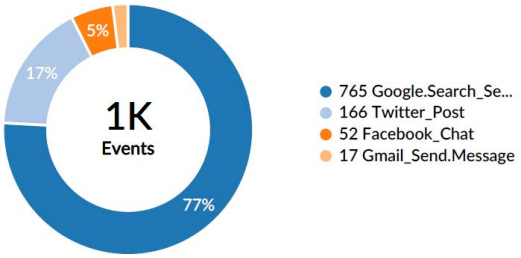


The following shows how you can generate a Cyber-Bullying Indicators Report:

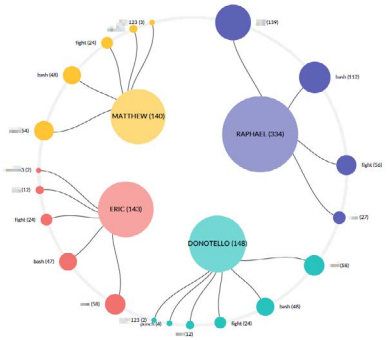
1. Remote user (FortiClient endpoint user or agentless SWG user) sends a Facebook message that contains cyberbullying indicators.
2. FortiSASE inspects the Facebook message as it is sent and logs it as containing cyberbullying indicators.
3. The FortiSASE administrator can download the Cyberbullying Indicators Report from FortiSASE to see the user's activity.

The following shows an examples of the charts in the Cyberbullying Indicators Report:

Offensive or Threatening Phrases Distribution by Platforms



Search terms which way indicate cyber-bullying:
Top 10 Users with Bad Terms or Phrases in Searches

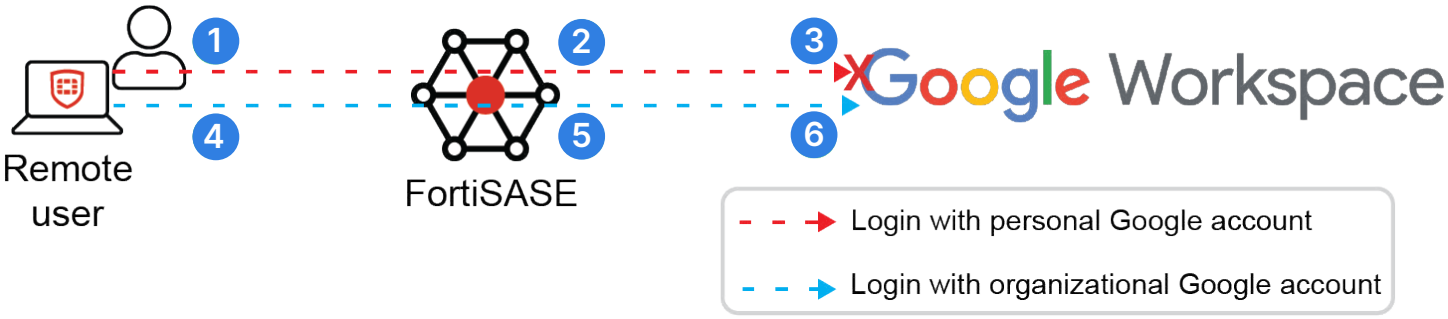


Application Access Control Using Google Workspace

Controlling application access with Google Workspace

You may want to **restrict SaaS access to resources like Google Workspace and Microsoft Office 365 by tenant to block login attempts from external users and secure students and staff from accessing nonapproved cloud resources such as applications within personal accounts**. Many cloud vendors enable this by applying tenant restrictions for access control. For example, FortiSASE remote users accessing Google Workspace applications with tenant restrictions will only be allowed to log in as the organization's tenant and access the organization's applications.

For remote users, FortiSASE uses inline-CASB to support HTTP header insertion, which is also known as customizing HTTP headers. See **Customizing inline-CASB headers**.



When you enable application access control with Google Workspace, the following happens:

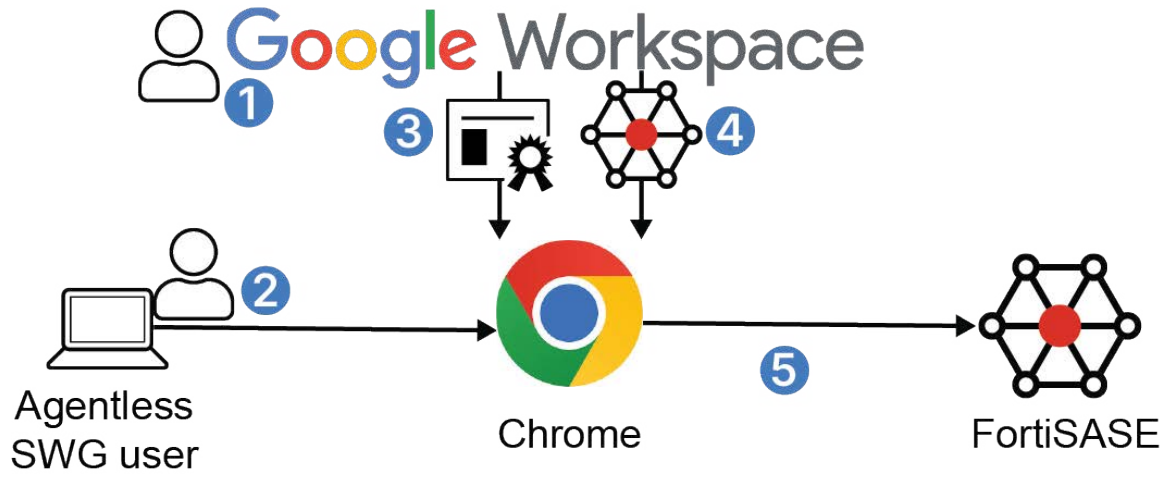
1. Remote user (FortiClient endpoint user or agentless SWG user) attempts to log in to Google Workspace using their personal Google account.
2. FortiSASE receives the login request, adds information to it that denies access to personal accounts, and forwards it to Google Workspace.
3. Google Workspace denies access since the account is not part of the organization.
4. Remote user logs in to Google Workspace using their organizational Google account.
5. FortiSASE receives the login request, adds information to it that denies access to personal accounts, and forwards it to Google Workspace.
6. Google Workspace grants access since the account is part of the organization.

SWG Behavior Control on Unmanaged Endpoints

Using Chrome extension to control SWG behavior on unmanaged devices

FortiSASE supports a Chrome extension that allows **enforcing FortiSASE secure web gateway (SWG) connectivity for selected endpoints with the Chrome browser installed**, including Chromebooks, based on the endpoint operating system (OS) and the corresponding extension policy that the Google Workspace administrator configured. This allows you to control SWG behavior on unmanaged devices. See **SWG Chrome extension and Chromebook support**.

Here, **unmanaged** means devices without an agent (without the FortiClient application installed).



The following shows how to deploy a Chrome extension to control SWG behavior on a managed Chrome browser:

1. Administrator configures Google Workspace.
2. User signs into Google using Chrome.
3. Google Workspace installs certificates on the managed Chrome browser.
4. Google Workspace installs the FortiSASE SWG Chrome extension on the managed Chrome browser.
5. Chrome is now configured for SWG. HTTP and HTTPS traffic are forwarded to FortiSASE for inspection.