

Forcepoint ONE

Secure Web Gateway

Key Benefits:

- › 999.99% verified uptime since 2015
- › Auto-scaling, over 300 points of presence, and distributed SWG architecture minimizes latency and maximizes throughput
- › Unified administrator console reduces repetitive and redundant configuration management
- › Unified managed device agent for CASB, SWG, and ZTNA simplifies deployment
- › SCIM provisioning accelerates user on-boarding
- › Data-in-motion scanning blocks malware and data exfiltration between users and any web application, no matter where they are located.
- › Field Programmable SASE Logic can block specific HTTP/S request methods resulting in granular control of any element in a web page
- › RBI with CDR enables safe use of unknown websites and safe use of files downloaded from those websites
- › Controls website access down to the URL directory level
- › SWG function cannot be bypassed or disabled by the user

The Forcepoint ONE Secure Web Gateway (SWG) is one of the three foundational gateways of the Forcepoint ONE cloud platform. Forcepoint ONE SWG monitors and controls any interaction with any website, including blocking access to websites based on category and risk score, blocking download of malware, blocking upload of sensitive data, detecting shadow IT, and optionally providing Remote Browser Isolation (RBI) with Content Disarm and Reconstruction (CDR) to safely interact with unsafe web content.

Forcepoint ONE SWG Architecture

Forcepoint ONE uses a distributed enforcement architecture so that organizations have more flexibility to meet changing business requirements. Forcepoint ONE SWG allows for enforcement using either the cloud-based forward proxy for sites and branch offices or the unique agent-based proxy for managed devices. With the cloud-based proxy, organizations can provide all users at sites, even guests and those on unmanaged devices, with Zero Trust Web Access. Locations can forward web traffic to the Forcepoint ONE SWG in the cloud using GRE or IPSEC tunnels. The unified policy manager makes it easy to apply per-network policies that can be used across sites. For example, organizations can set up guest internet access to be isolated using the optional Forcepoint RBI service for the ultimate in Zero Trust Web Access and easily apply this guest WI-FI policy to all locations. This option is ideal for branch offices and sites with public or customer WI-FI access, but Forcepoint also provides an ideal solution for remote workers on managed devices using the agent-based SWG.

The agent-based SWG enforces web policies locally for the best possible web performance. With agent-based enforcement the user and company data are protected no matter where the user is located: at home, in the field, or in the office. By design, the unified agent powering the SWG cannot be stopped by the user or uninstalled by the user without approval from a Forcepoint ONE tenant administrator, thus ensuring its function is not easily bypassed by the user. And, because the Forcepoint ONE agent also supports forward proxy CASB and ZTNA for non-browser clients, these capabilities can be enabled with the proper licensing and do not require additional software downloads or any other actions by the end user.

Forcepoint ONE's distributed architecture provides over 300 points of presence on AWS in major population centers, with each point of presence supporting auto-scaling. This means latency is reduced when the on-device agent needs to communicate with the Forcepoint ONE backplane on AWS or when site traffic is steered to the cloud proxy. Second, the agent-based SWG enforcement is performed on-device. This means that little traffic needs to pass through the Forcepoint ONE backplane on AWS when using the agent-based SWG, as shown in figure 1.

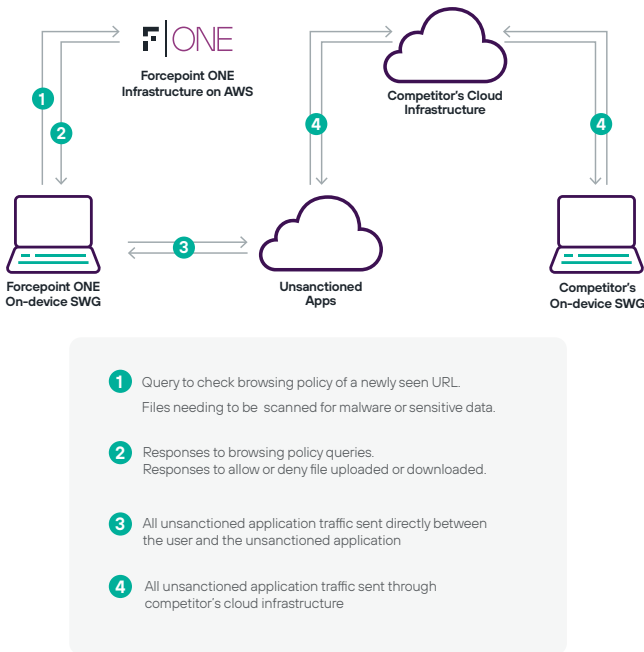


Figure 1: Forcepoint ONE SWG Traffic Routing vs. Competitors

As shown in the figure, the Forcepoint ONE on-device SWG, on the left, only needs to communicate with the Forcepoint ONE backplane on AWS in two situations: when first attempting to access a website not recently visited to determine access restrictions, and when attempting to upload or download files or other data that needs to be scanned for malware or sensitive data.

By comparison, the other vendor's on-device SWG, on the right, must send all web traffic through the vendor's cloud backplane for traffic inspection and forwarding. This routing of all web traffic through the other vendor's cloud infrastructure can cause up to a 50% loss in effective throughput, thus causing productivity issues for users in low bandwidth locations. Because file uploads and downloads are a small fraction of overall internet traffic for most users, the Forcepoint ONE SWG can typically support throughput of about 95% of total available internet bandwidth, while reducing latency, thus supporting greater user adoption.

Forcepoint ONE SWG Features

SWG connection policies

Let administrators restrict access to a range of websites or allow the connection to bypass the SWG forward proxy and not be decrypted, and optionally log each connection attempt. Criteria for policy enforcement include user group, device posture, domain category (predefined web categories from Forcepoint ThreatSeeker, Forcepoint ONE predefined enterprise app categories, or custom categories), host app (web browsers or non-browser applications), and host network (user's DNS server IP address or DNS suffix). Supports user privacy by allowing connections to personal healthcare or financial sites to pass unencrypted.

ID	Groups	Device (Agent only)	Location	Traffic Type (Cloud SWG only)	Domain Category	Host App (Agent only)	Host Network (Agent only)	Action
225221	Marketing	Any	Any	Any	Web (browsing) <ul style="list-style-type: none">AbortionAbused DrugsAdult and Pornography	Any	Any	Deny & Log

Figure 2: SWG connection policies

SWG content policies

Let administrators control access and activity across all websites based on web category. Criteria for policy enforcement include user group, device posture, location, traffic type, web category, and reputation/app score. Based on any combination of the above attributes actions can be taken to deny access altogether, isolate the session using RBI, provide secure app access, or provide direct access without content inspection.

ID	Groups	Device (Agent only)	Location	Traffic Type (Cloud SWG only)	URL Category	Reputation / App Score	Action
748201	Policy (Web)	Any	Any	Any	Any	Any	Deny (Web)
237427	Any	Any	Any	Any	Custom URL: <ul style="list-style-type: none">DesktopDesktop URL Categories: <ul style="list-style-type: none">Personal NetworkStorage and Backup	Any	Secure App Access (DLP) Download DLP Upload
246851	Any	Any	Any	Any	Custom URL: <ul style="list-style-type: none">LinkedIn Enterprise App: <ul style="list-style-type: none">Social Network URL Categories: <ul style="list-style-type: none">LinkedIn ConnectionsLinkedIn JobsLinkedIn MailLinkedIn Updates	Any	Secure App Access (DLP) Download DLP Upload

Figure 3: SWG content policies

When secure app access is specified in a SWG content policy, the administrator can specify multiple DLP upload and download policies for blocking download or upload of sensitive data or malware (using Forcepoint ONE's integrated DLP).

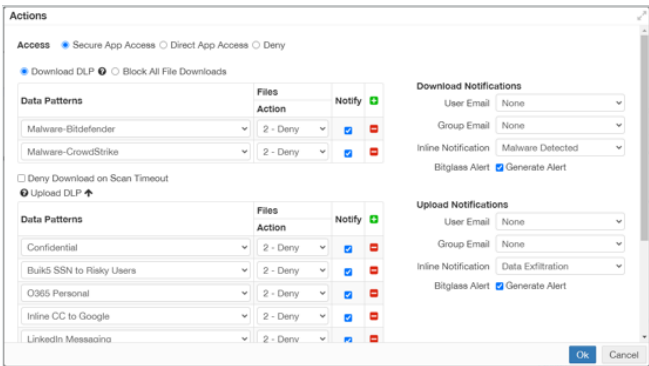


Figure 4: Secure app access SWG content policy

When an isolated access connection is specified by a SWG content policy, the administrator must also select an RBI profile from the dropdown menu.

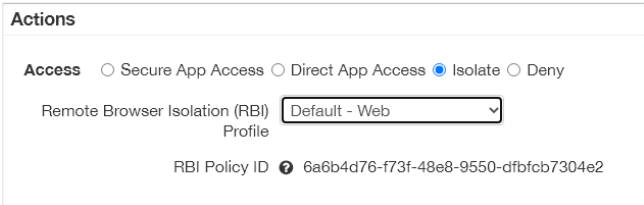


Figure 5: Isolated access SWG content policy

RBI profiles

Let administrators specify parameters for an RBI session that determine how restrictive the session is.

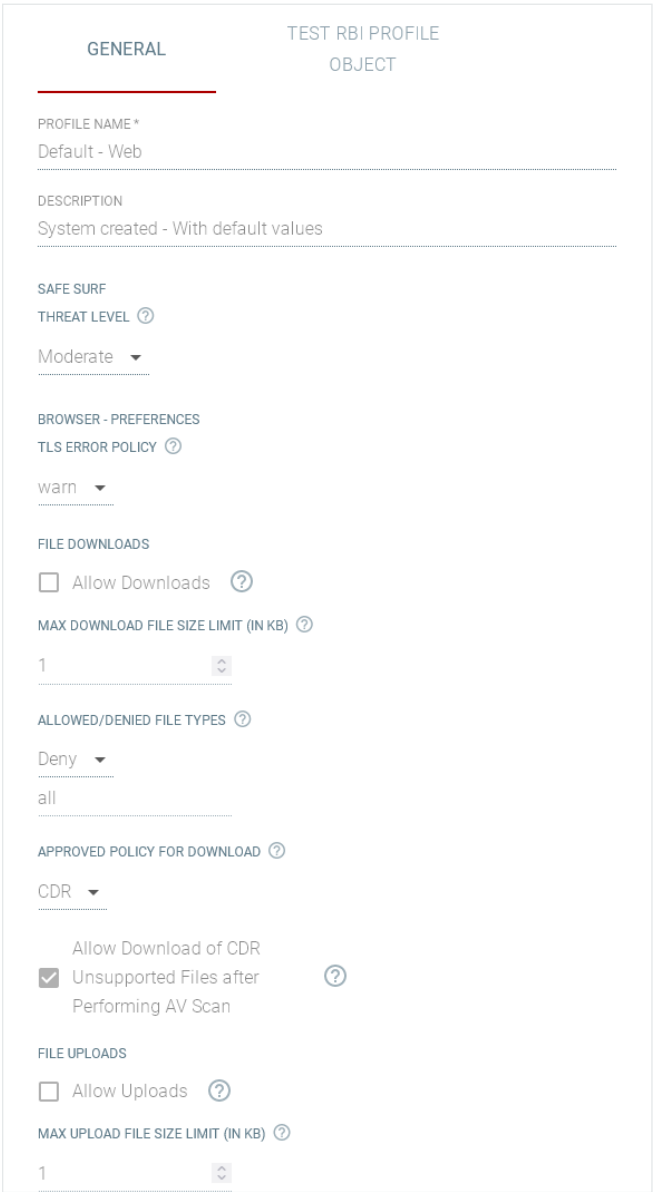


Figure 6: RBI Profile

The following table summarizes the allowed values and functions of the RBI profile parameters.

NAME	VALUES	DEFAULT	USAGE
Threat Level	Off (0), Moderate (60), High (80)	High	→ Renders site in read only mode if site threat level is higher than the specified value
TLS Error Policy	Fail, Warn, Ignore	Warn	→ Action the browser will take when navigating to bad TLS/Cert sites
Allow Downloads	Checkbox	Yes	→ Allow users to download files from websites
Max Download File Size limit (in KB)	Integer	100	→ Maximum file size for individual downloads is 500,000 KB (500 MB)
Allowed/Denied File Types (dropdpwn)	Allow or Deny	Allow	→ Allow or deny uploads based on file type
Allowed/Denied File Types (text list)	Comma-separated list of file extensions	All	→ Specify all or a subset of file types to allow or deny
Approved Policy for Download	CDR, AV Scan, No Scan	CDR	→ CDR: apply CDR → AV Scan: download after successful AV scan → No Scan: download without scan or CDR
Allow Download of CDR Unsupported Files after Performing AV Scan	Checkbox	Yes	→ If unchecked, and CDR cannot be performed due to file size > 250 MB or unsupported file type, block download. → If checked, and CDR cannot be performed, perform AV scan on file and download if scan passes
Allow Uploads	Checkbox	No	→ Allow users to upload files from websites
Max Upload File Size limit (in KB)	Integer	100	→ Maximum file size for individual uploads is 400,000 KB (400MB)

The Test RBI Object tab lets the administrator test the functionality of RBI and CDR for a specific website.

Figure 7: RBI Profile Test Profile Object tab

SWG web browsing dashboard

Displays graphical representations of web traffic patterns at the URL level and highlights risky activity, such as risky destinations visited, data downloaded from risky destinations, and data uploaded to risky destinations. Additional displays show web reputation categories and policy events per category, as well as top sensitive file uploaders, top domains receiving sensitive data, and top uploaded DLP patterns.



Figure 8: Web Browsing Dashboard



Figure 9: Web Dashboard

SWG Enterprise apps dashboard

Displays graphical representations of web traffic to SaaS apps and Shadow IT, shows total apps, risky apps, enterprise app categories, with insight into data uploaded to and downloaded from risky apps. Visibility into top policies by hit count, domains denied, users denied, domains receiving sensitive data, and top upload patterns all make it easier than ever to get control over shadow IT and improve the overall security posture of the organization to keep control of sensitive data.

SWG bypass prevention

Users cannot kill the SWG processes on their Windows or MacOS device, and users cannot uninstall the on-device agent powering the SWG without assistance from the Forcepoint ONE tenant administrator.

Forcepoint ONE Platform Features

The Forcepoint ONE SWG additionally supports these features built into the Forcepoint ONE platform:

- **Contextual access control.** Users cannot browse the internet unless they are authenticated by Forcepoint ONE and permitted to login based on login policies which access can be controlled by forcing authentication and applying specific policies for unauthenticated access and more granular controls for authenticated users, based on user location, network, device type, posture, user group, and more.
- **Data Loss Prevention (DLP).** Files and text are scanned upon upload or download for sensitive data, reported, and blocked as appropriate.
- **Field Programmable SASE Logic (FPSL).** Any HTTP/S request method can be logged and optionally blocked based on the content in any part of the request method.
- **Malware scanning.** Files are scanned during upload or download for malware, using scanning engines from CrowdStrike or Bitdefender, and blocked when detected.
- **Unified management console for configuration, monitoring, and reporting for SWG, CASB, and ZTNA.** Lets administrators reuse DLP match patterns across SWG, CASB, and ZTNA for private web applications.
- **GRE and IPSEC support.** For agentless enforcement at sites and branch offices connecting to the cloud proxy.
- **Unified on-device agent.** For Windows or macOS with unique auto-generated and auto-rotated certificates.
- **Cloud Firewall.** Add-on to SWG to secure all internet traffic and safeguard against attacks designed to exploit vulnerable branch sites.
- **99.99% service uptime.**

Forcepoint ONE SWG Features and Benefits

FEATURE	BENEFIT
Auto-scaling, distributed architecture on AWS with over 300 POPs worldwide.	<ul style="list-style-type: none"> → 99.99% uptime. → Minimal latency; often even faster than direct application access.
Integration with any SAML-compatible IdP. SAML relay or ACS proxy mode. Optional built-in IdP using Microsoft ADFS.	<ul style="list-style-type: none"> → Flexible deployment. → Denial of service protection when using SAML relay mode.
SCIM Provisioning and AD Sync Agent. Synchronizes your Forcepoint ONE users and groups with Azure AD or Microsoft AD, respectively.	<ul style="list-style-type: none"> → Leverages your existing Azure AD tenant or Microsoft AD instance to quickly onboard users and manage the groups they are in.
Contextual access control based on user group, device type, location, or time of day, with escalation to Multi-Factor Authentication based on "impossible travel," unauthorized location, or unknown device. Additional layer of access control for individual websites or applications based on user group, device type, or location.	<ul style="list-style-type: none"> → Detects and blocks suspicious login attempts. → Reduces risks associated with stolen passwords. → Segments users based on risk and need to access.
Single unified agent for on-device SWG, CASB forward proxy, and ZTNA or nonweb applications. Includes support for deployment through MDM systems and uses self-generated auto-rotated certificates.	<ul style="list-style-type: none"> → Simplifies agent deployment. → Enhances security. → Reduces IT overhead.
Single administrator console for managing all system capabilities across all applications, users, and devices.	<ul style="list-style-type: none"> → Reduces complexity and time to value. → Increases visibility and control.
DLP and malware scanning for data in motion. Scans file attachments downloaded from or uploaded to any web-based app or website for malware or sensitive data and logs and blocks the transfer as appropriate.	<ul style="list-style-type: none"> → Stops data leakage and spread of malware in transit between users and any web application or website.
Field Programmable SASE Logic. Monitors, logs, and optionally blocks any HTTP/S request method based on any portion of the request method.	<ul style="list-style-type: none"> → More fine-grained control of app usage. → Ability to block upload of sensitive data as message posts.
Monitors, logs, and controls data and access to any website from any device at sites and branch offices, or from corporate Windows and Mac endpoints located anywhere—including inline DLP and malware scanning.	<ul style="list-style-type: none"> → Enforces acceptable use policy. → Monitors and controls shadow IT. → Blocks upload of sensitive data to unsanctioned websites. → Blocks download of malware from any website.
Distributed SWG architecture.	<ul style="list-style-type: none"> → Balances traffic across cloud and endpoint proxies to push enforcement as close to the edge as possible and deliver maximum performance.
Web domain classification and reputation scoring supplemented with Forcepoint ONE enterprise app classification and risk scoring.	<ul style="list-style-type: none"> → Constantly updated classification and riskscoring databases simplify access and content policy creation.
Custom URL categories allowing URL entries that include full directory path.	<ul style="list-style-type: none"> → Allows blocking of only certain directories within a website such as specific subreddits within reddit.com.
Cloud Firewall	<ul style="list-style-type: none"> → Complements SWG to extend protection to non-web ports and protocols with firewall and Intrusion Prevention System (IPS) protections. → Safeguards against attacks designed to exploit vulnerable branch sites.
Optional RBI with CDR	<ul style="list-style-type: none"> → RBI applies a Zero Trust approach of treating all web pages as compromised and rendering them in a remote, disposable environment, enabling people to use the web without being attacked or having data stolen and applies content disarm and reconstruction of files before downloading them including the removal of malware embedded in an image file using steganography.
SWG Web Browsing and SWG Enterprise Apps dashboards.	<ul style="list-style-type: none"> → Allows administrators to see access attempts, malware download attempts, and sensitive data upload attempts at a glance.