

Cloud Secure Web Gateway (fka WSS)

This Notice describes how the above designated Product processes Personal Data. It provides the information relevant to assess and document privacy relevant aspects of the use of this Product. This Notice and the relevant terms of the [Broadcom Privacy Policy](#) are the authoritative statements relating to the Personal Data processing activities and privacy regulatory compliance aspects associated with the use of this Product.

About this Notice

Product version(s) covered by this Notice:	All time current
---	------------------

Prior versions of this Notice as applicable to earlier releases of the Product may be available in the Archives. Where this Notice references other Products marked with an asterisk (*), please refer to the separate Notices of such Products.

About the Product

For information on the purpose, features and technical characteristics of the Product, please refer to the documentation at <https://www.broadcom.com/products/cybersecurity/network/web-protection/cloud-secure-web-gateway>.

Product type:	<input type="checkbox"/> Hardware	<input checked="" type="checkbox"/> Software	<input checked="" type="checkbox"/> Service	<input type="checkbox"/> Other
Deployment model(s):	<input type="checkbox"/> On-premise	<input checked="" type="checkbox"/> Cloud-based	<input type="checkbox"/> Hybrid	<input type="checkbox"/> Other

About the Processing Operation(s) performed by / for the purpose(s) of the Product

This Product:	<input checked="" type="checkbox"/> Must process Personal Data to deliver its core feature(s)	<input type="checkbox"/> Does not require processing any Personal Data to deliver its core feature(s)
This Product:	<input checked="" type="checkbox"/> Has optional features that may process Personal Data	<input type="checkbox"/> Such optional features are active by default <input checked="" type="checkbox"/> Such optional features are inactive by default
This Product processes:	<input checked="" type="checkbox"/> Non-sensitive Personal Data	<input type="checkbox"/> Sensitive Personal Data <input type="checkbox"/> Not applicable
The Product involves:	<input type="checkbox"/> Profiling of individuals based on personal characteristics	<input type="checkbox"/> Automated decision making that produces legal or other significant impacts on individuals

About the Personal Data processed by / for the purpose(s) of the Product

Categories of Personal Data	Categories of Data Subjects	Purpose(s) of Processing	Categories of Data Recipients	Needed for core features (Yes/No)	Processing location(s)	CA Inc. acts as Processor (Yes/No)
Individual identifiers and contact details	Customer admins	Account management (optional: software downloads, export compliance checks)	Customer admins, hosting provider	Yes	U.S.	Yes
Online identifiers and trackers, network activity metadata, location data for service delivery	Customer's end-users	Security check of websites visited by end-user	Customer admins, hosting provider	Yes	Transiently in nearest of 50+ worldwide locations , purged immediately after the transaction	Yes
Personal data, potentially including sensitive categories, accessed or possessed by Customer end-users on websites they visit	Customer's end-users	User access to web content	Customer admins, hosting provider	Yes		Yes
Online identifiers and trackers, network activity metadata, location data for service logging	Customer's end-users	Transaction logging and audit	Customer admins, hosting provider	Yes	U.S., Belgium, Japan as closest to customer's billing location, or per customer preference.	Yes

Network activity data, electronic communications data	Customer's end-users	Data loss prevention, advanced malware sandboxing	Customer admins, hosting provider	Only if customer uses data loss prevention and advanced malware sandboxing	EU, UK, U.S.	Yes
---	----------------------	---	-----------------------------------	--	--------------	-----

About managing the Personal Data processed by / for the purpose(s) of the Product

Privacy Enhancing Technologies

Subject to more detailed information provided in the Product description and other customer literature e.g. on optional Product settings and configurations available, the Product has the following technical and organizational capabilities to enhance and protect the privacy of the Personal Data it processes:

Privacy Objective	Privacy Enhancing Technologies / Measures	Data at rest	Data in transit ^a
Data confidentiality	Access control measures	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Encryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data integrity	Anti-tampering technology	<input type="checkbox"/>	<input type="checkbox"/>
	Change logging	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data availability	Business continuity measures (e.g. failover)	<input checked="" type="checkbox"/>	NA
	Disaster recovery measures (e.g. backups)	<input type="checkbox"/>	NA
Data incident	Detection and flagging of incidents	<input type="checkbox"/>	NA
	Response mechanisms to incidents	<input type="checkbox"/>	NA
Current certification(s):	ISO 9001:2015, ISO27001, SSAE18 SOC 2, SOC 3		

^aData in transit encompasses traffic between client systems and SaaS endpoints.

Data Subject Rights

Customer admins can amend, rectify, or delete any information regarding their administrative portal login – except the login ID (an email address) itself. Other administrators of the same customer can delete admin accounts (removing the email address). Administrators can remove End-User usernames from configuration. End-user transactional logs cannot be edited or amended as that would compromise the integrity of historical event records.

Personal Data Retention Schedule

Customer Admin identifiers and contact information are retained for the duration of the subscription. The retention of location data, online identifiers and trackers and network activity data is defined per-license. The service includes features to permit the Customers to control the content of the transactional logs at creation, removing identifiers based on various trigger conditions. Transactional log data is stored for 1 year maximum. Communication data submitted to data loss prevention is transient only and not retained. Sample files processed for advanced malware sandboxing are deleted after detonation by clean-up process as storage space is required.

About Regulatory Compliance Matters

Data Processing Addendum

Where your use of the Product or of related services involves CA Inc., its parent and/or affiliates acting as a Data Processor on your behalf, the rights and obligations of both parties with respect to such Personal Data processing, including as regards disclosures and cross-border transfers of Personal Data to and/or by CA Inc., its parents and/or affiliates and any of their sub-processors, are defined in the applicable Data Processing Addendum available at <https://www.broadcom.com/company/legal/ca/data-transfers>.

CCPA Compliance

If you are subject to the California Consumer Privacy Act and require CA Inc., its parent and/or affiliates to enter into CCPA-based service provider terms with you, please use our CCPA Customer Agreement Supplement available at <https://www.broadcom.com/company/legal/ca/data-transfers>.

Sub-Processing

The specific sub-processor(s) involved in the delivery of this Product can be found below:

- <https://www.broadcom.com/company/legal/privacy/sub-processors>

This list is subject to change in accordance with the statutory requirements and contractual terms applicable.