Cloud Secure Web Gateway

SaaS Listing

The definitions set out in the Agreement will apply to this SaaS Listing document.

The CA software program(s) ("CA Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the CA quote or other transaction document entered into by you and the CA entity ("CA") through which you obtained a license for the CA Software (hereinafter referred to as the "Agreement"). These terms shall be effective from the effective date of such ordering document.

This SaaS Listing describes Cloud Secure Web Gateway (previously known as Web Security Service). All capitalized terms in this SaaS Listing have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

Table of Contents

Cloud Secure Web Gateway

SaaS Listing

1: Technical/Business Functionality and Capabilities

Service Overview

Cloud Secure Web Gateway ("Service") enforces granular access and security policies that manage web internet usage by application, device, user, or location.

Service Features

- The Service helps to protect web traffic, users and devices via cloud-delivered security service.
- Customer can access the Service through a self-service online portal ("Portal"). Customer may configure and manage the Service, access reports, and view data and statistics, through the Portal, when available as part of the Service.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.
- Reporting for the Service is available through the Portal. Reporting may include activity logs and/or statistics. Customer may choose to generate reports through the Portal, which can be configured to be sent by email on a scheduled basis, or downloaded from the Portal.
- The Service includes one hundred (100) days of reporting. Longer log retention options are available for a fee.

Service Software Components

- The Service includes the following optional software components:
    - Auth Connector: This software is required to import users, groups information to the Service.
    - WSS Agent: This software can be deployed on endpoints to connect to the Service.
    - Symantec Enterprise Agent: This software can be deployed on endpoints to connect to the Service.

2: Customer Responsibilities

CA can only perform the Service if Customer provides required information or performs required actions, otherwise CA's performance of the Service may be delayed, impaired or prevented, and Customer may lose eligibility for any Service Level Agreement.

- Setup Enablement: Customer must provide information required for CA to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist CA in delivery of the Service.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Transaction Document within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the subscription Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, CA is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

Cloud Secure Web Gateway

SaaS Listing

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under one of the following License Metrics as specified in the Transaction Document:

- CA may count any and all of the following as a "User": (a) any employee of the Customer, (b) any agent, partner/contractor resource, or other non-employee (i.e., each individual person) authorized by Customer to use and/or benefit from the use of the Service, and (c) each 8 gigabytes of Customer's total Service activity/traffic transferred per month, excluding activity/traffic of any person already counted as a "User" under subsections (a) and (b). A User may have up to four (4) devices.
- "Unit" means the number of instances of Cloud-HSM that are integrated with Cloud SWG (previously known as WSS) and are managed by Customer. This Unit meter is available for the Self-Managed Certificate Service as an add-on feature (separate purchase required).

4: Customer Assistance and Technical Support

Customer Assistance

CA will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If CA is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support for Services will be performed in accordance with the published terms and conditions and technical support policies published in the “Broadcom Software Maintenance Policy Handbook” at: https://support.broadcom.com/external/content/release-announcements/CA-Support-Policies/6933.

Maintenance to the Service and/or supporting Service Infrastructure

CA must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.broadcom.com/. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, CA will provide seven (7) calendar days’ notification.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. CA will provide a minimum of one (1) calendar day notification. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times CA will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, CA will provide fourteen (14) calendar days’ notification. CA may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

Cloud Secure Web Gateway

SaaS Listing

CA may modify the Service and/or the corresponding SaaS Listings at any time: (a) due to changes in applicable laws or industry standards; and (b) for any other reason, if the modification does not materially reduce the level of performance, functionality, security or availability of the Service during the Term.

- Additional terms and conditions that may apply to the Service are available at: https://docs.broadcom.com/doc/blue-coat-products-third-party-en
- Excessive Consumption. If CA determines that Customer's aggregate activity on the Service imposes an unreasonable load (Customer's average per User usage is greater than the average per User usage generated by 95% of inline Users of the Service on a monthly basis) on bandwidth, infrastructure, or otherwise, CA may impose controls to keep the usage below excessive levels. Upon receiving Service notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with its reseller to enter into a separate fee agreement for the remainder of the Subscription Term. CA reserves the right to manage bandwidth and route traffic in a commercially optimal way, including without limitations, diverting traffic from well-known media streaming, trusted software update sites and cloud-based backup sites to the extent not posing any material security threat to Users, and providing guidance to Customer on ways that Customer can control bandwidth usage by bypassing such sites.
- User Count. In the event that Customer exceeds its authorized Users (as measured in CA's reporting system or as otherwise calculated by CA), Customer agrees to promptly pay the amounts invoiced for the excess usage and/or submit a new order for the excess use. In addition, the parties agree to meet in good faith to determine the number of new User subscriptions required by Customer for the remainder of the Subscription Term.
- Optional add-on services may be available with the Service and will be provided in accordance with their documentation.
- WSS Agent. If Customer installs the WSS Agent software, CA will install a TLS root certificate authority ("RCA") on each device. The RCA permits the Service to intercept and inspect encrypted traffic, and is necessary for the Service to operate with encrypted (HTTPS) traffic. If WSS Agent is uninstalled, the RCA will be removed. CA will use intercepted traffic to authenticate traffic as originating from a valid User of the Service, carry out processing of traffic as configured within the Service and for delivery of error responses.
- Symantec Enterprise Agent. If Customer installs the Symantec Enterprise Agent software, CA will install a TLS root certificate authority ("RCA") on each device. The RCA permits the Service to intercept and inspect encrypted traffic, and is necessary for the Service to operate with encrypted (HTTPS) traffic. If Symantec Enterprise Agent is uninstalled, the RCA will be removed. CA will use intercepted traffic to authenticate traffic as originating from a valid User of the Service, carry out processing of traffic as configured within the Service and for delivery of error responses.
- Symantec Endpoint Protection. Customers that have both a Symantec Endpoint Protection ("SEP") subscription and Service subscription are given access to use the Web and Cloud Access Protection feature. If Customer enables the Web and Cloud Access Protection feature, CA will install a TLS root certificate authority ("RCA") on each authorized device (as defined in the SEP Specific Program Documentation). The RCA permits the Service to intercept and inspect encrypted traffic, and is necessary for the Service to operate with encrypted (HTTPS) traffic. If the RCA was installed by SEP, the RCA will be removed when the Web and Cloud Access Protection feature is disabled. CA will use intercepted traffic to authenticate traffic as originating from a valid User of the Service, carry out processing of traffic as configured within the Service and for delivery of error responses. Use of the Web and Cloud Access Protection feature is intended only for Customers who have valid subscriptions for both SEP and the Service. CA makes no claim of support or viability for the Web and Cloud Access Protection feature to be used for any other purpose.

6: Definitions

"**Administrator**" means Customer's designated personnel to manage the Service on behalf of Customer.

"**Service Credit**" means the number of days that are added to Customer's current Term.

"**Service Infrastructure**" means any CA or licensor technology and intellectual property used to provide the Services.

"**Cloud Secure Web Gateway Subscription**" means the base entitlement required for all services sold under the Cloud SWG umbrella.

Exhibit-A

Service Level Agreement(s)

Cloud Secure Web Gateway

SaaS Listing

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this SaaS Listing only. If CA does not achieve these SLA(s), then Customer may be eligible to receive a Service Credit. Service Credits are Customer's sole and exclusive remedy and are CA's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the data in transit to and from Customer to the Internet. Cloud Secure Web Gateway is an Inline Service that includes Content-Filtering and Anti-Malware scanning.

Inline Service Availability	**99.999%**

- **Non-inline Service Availability** is access to the controls that govern the features of the Service that do not impact data in transit to and from the end-user to the Internet (e.g., reporting tools used by the administrator. Examples of Non-Inline Service for this Service include: Reporting and Advanced Malware sandboxing.

Non-Inline Service Availability	**99.5%**

b. **Other SLAs**:

- **Average Latency**: Average latency for transactions passing through the Service is based on the processing time attributed to the Cloud SWG infrastructure. Average latency for the Service is defined as the average time it takes for the service to scan, process and apply the Customer's policy to the web content data, assuming a 1MB web page, and does not include 1) the time for communications outside the service data center, or 2) traffic that egresses from a POP separate from the POP the user is connected to due to Customer policy settings.
- . Average Latency is 100 milliseconds or less and is determined by the monthly average among samples taken by CA in a given month.

Latency SLA: Average Round Trip	**100 Milliseconds or less**

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of 100% total minutes per calendar month as follows:

$$\frac{\text{Total Minutes in Calendar Month – Excused Outages – Non-Excused Outages*}}{\text{Total – Excused Outages}} \times 100 > \text{Availability Target}$$

**Non-Excused Outages = Minutes of Service disruption that are not an Excused Outage*

Note: The availability calculation is based on the entire calendar month regardless of the Service start date.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Customer's account.

CA will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24 hour period. A Customer may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Service Credits:

- May not be transferred or applied to any other CA Online Service, even if within the same account.
- Are the only remedy available, even if Customer is not renewing for a subsequent term. A Service Credit is added to the end of Customer's current Subscription Term.

- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Customer may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Customer must submit the claim in writing via email to CA Customer Support. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for CA to review the claim. Each claim must include the following information:

(i) The words "Service Credit Request" in the subject line.
(ii) The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
(iii) An explanation of the claim made under this SaaS Listing, including any relevant calculations.

All claims will be verified against CA's system records. Should any claim be disputed, CA will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Customer.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

- Planned Maintenance and Unplanned Maintenance as defined in the SaaS Listing.
- Force Majeure as defined in the Agreement.
- Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

- Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
- Customer has not paid for the Service.
- Third party, non-CA branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of CA or within the scope of the Service.
- Any item that is not a Service Component that is provided for use with the Service.
- Technical support provided with the service.
- Failure of Customer to correctly configure the Service in accordance with this SaaS Listing.
- Hardware or software configuration changes made by the Customer without the prior written consent of CA.
- Unavailability of a specific web page or a third party's cloud application(s).
- Individual data center outage.
- Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Unavailability or performance impact caused by acts of government or intermediate carriers
- Failure of Customer's internet access connections.
- Suspension and termination of Customer's right to use the Service.
- Alterations or modifications to the Service, unless altered or modified by CA (or at the direction of or as approved by CA
- Defects in the Service due to abuse or use other than in accordance with CA's published Documentation unless caused by CA or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
- Customer web traffic that egresses from a POP separate from the POP the user is connected to due to Customer policy settings.

END OF EXHIBIT A