



Table of Contents

AT&T Cloud Web Security Service.....	4
Service Description.....	4
SD-1. General.....	4
SD-1.1. AT&T Cloud Web Security Service	4
SD-1.2. Country Availability	4
SD-2. AT&T Cloud Web Security Service.....	5
SD-2.1. Overview	5
SD-2.2. Standard Service Components.....	5
SD-2.2.1. Web Filtering.....	6
SD-2.2.2. SafeSearch	6
SD-2.2.3. Malware Scanning	6
SD-2.2.4. Content Filtering.....	6
SD-2.2.5. Roaming and Mobile User Support	6
SD-2.2.6. Application Control.....	7
SD-3. AT&T Cloud Web Security Service – Features and Capabilities.....	7
SD-3.1. Integration with Customer's Data Loss Prevention System	7
SD-3.2. Log Data.....	7
SD-3.2.1. Anonymization of Log Data for International Privacy Regulations	7
SD-3.3. IPSec Support	7
SD-3.3.1. IP Sec Connection to Network Based Firewall (NBFW).....	7
SD-3.4. Explicit Proxy Support	8
SD-3.5. SSL Support.....	8
SD-3.6. User Authentication	8
SD-3.6.1. SAML 2.0 (Security Assertion Markup Language)	8
SD-3.6.2. Active Directory Integration	9
SD-4. Reporting and Administrative Portal	9
SD-4.1. Reporting.....	10

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SD-5. Responsibilities of the Customer	10
SD-5.1. Customer Responsibilities	10
SD-5.2. Customer Compliance Responsibilities.....	11
SD-6. Customer Care/Technical Support	11
SD-6.1. Maintenance Notification	11
SD-7. Use of Service	11
SD-7.1. Activation of Service	11
SD-7.2. Number of Subscribers.....	12
SD-7.3. Amount of Traffic	12
SD-8. End User License Agreement (EULA).....	12
SD-8.1. AT&T Cloud Web Security Service	12
SD-8.1.1. Customer Configuration	13
SD-8.1.2. Passwords	13
SD-8.1.3. Right to Access Service; Software License	13
SD-8.1.4. Use Restrictions.....	14
SD-8.1.5. Acceptable Use.....	14
SD-8.1.6. Reservation of Rights; Ownership	14
SD-8.2. Customer Data	15
SD-8.2.1. Definition of Customer Data	15
SD-8.2.2. Limited Use.....	15
SD-8.2.3. Obligations; Indemnification	15
SD-8.3. Open Source Software	15
Service Level Agreements (SLA).....	16
SLA-1. AT&T Cloud Web Security Service Level Agreement Terms	16
SLA-1.1. Definitions.....	16
SLA-1.2. SLA Exclusions.....	17
SLA-1.3. SLA Reporting and Claims.....	17
SLA-1.4. SLA Claims Limitations	18
SLA-2. SLA Availability	18
SLA-2.1. SLA Availability – Remedies	19
SLA-2.2. Chronic Failure	19
SLA-2.3. SLA Latency	19
SLA-2.4. SLA Latency Remedies	20

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T
Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

AT&T Business Service Guide
AT&T Cloud Web Security Service

Pricing (P)	20
P-1. AT&T Cloud Web Security Service Pricing	20
Country-Specific Provisions (CSP)	20
CSP-1. Country-Specific Provisions	20
CSP-1.1. Country Unique Terms	20

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T
Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

AT&T Cloud Web Security Service

Section Effective Date: 30-Jan-2015

The AT&T Cloud Web Security Service (Cloud WSS) Service Guide consists of the following parts:

- Service Description (SD)
- Service Level Agreements (SLA)
- Pricing (P)
- Country-Specific Provisions (CSP)

The Service (and any software included with the Service) and use of the Service (or software) indicates express acceptance of the End User License Terms. In addition, the [General Provisions](#) are incorporated and apply as specified therein.

Service Description

SD-1. General

SD-1.1. AT&T Cloud Web Security Service

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service provides network-based (cloud) web filtering, malware and content scanning of Customer-designated network users or devices, including roaming (not connected to Customer VPN) and mobile user support.

SD-1.2. Country Availability

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service is available in select countries in the regions and countries detailed in the table below.

Table of Regions	
Region	Countries within a Region
Americas	Argentina, Brazil, Canada, Chile, Colombia, Mexico, Panama, Peru, Venezuela
Asia Pacific (AP)	Australia, Hong Kong, Japan, New Zealand, Singapore, Republic of Korea, Taiwan, Thailand

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

Table of Regions	
Region	Countries within a Region
EMEA	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, United Kingdom
United States	United States

SD-2. AT&T Cloud Web Security Service

SD-2.1. Overview

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service is a network-based service which scans Customer Internet traffic in order to provide web filtering, which restricts user access to web sites, malware scanning, which checks web traffic for virus and malware attacks and other security capabilities on an as a service basis. The Service also helps to protect roaming and mobile device users when they are accessing the Internet when not connected to the Customer network VPN.

AT&T Cloud Web Security Service supports multiple types of Internet connections on an agnostic basis, including, without limiting the foregoing, AT&T VPN Service Customers using AT&T Network-based Firewall. AT&T Cloud Web Security may be installed on customer corporate mobile devices in order to permit filtering and scanning of traffic when the devices access the Internet using third-party networks.

SD-2.2. Standard Service Components

Section Effective Date: 30-Jan-2015

The following are the basic Service Components available using AT&T Cloud Web Security Service:

- Web Filtering
- SafeSearch
- Malware Scanning
- Content Filtering
- Roaming and Mobile User Support
- Application Control

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SD-2.2.1. Web Filtering

Section Effective Date: 30-Jan-2015

The Web Filtering service component permits language-agnostic filtering of web page traffic (encrypted or unencrypted) using predefined URL categorization and content analysis specified by Customer. Web Filtering permits configuration of customized access restriction policies (based on categories and types of content) by specific User groups. Web Filtering supports filtering by specific IP address or URL name. Web Filtering also provides dynamic rating algorithms that identify and categorize Web content in real time to provide URL filtering.

SD-2.2.2. SafeSearch

Section Effective Date: 30-Jan-2015

The SafeSearch service component provides blocking of explicit websites and images from appearing in search engine results. SafeSearch is supported with the following search engines: Google, Yahoo and Bing.

SD-2.2.3. Malware Scanning

Section Effective Date: 30-Jan-2015

The Malware Scanning service component uses inline scanning technology to examine Web content to identify in real time malicious and suspicious sites, bot-net traffic, and phone-home malware.

SD-2.2.4. Content Filtering

Section Effective Date: 30-Jan-2015

The Content Filtering service component enables Customer to define language agnositic content filtering policies to meet specific business requirements. Content filtering policies consists of a combination of blocked and allowed Web content categories and trusted and blocked sources and destinations that apply globally to all users (Basic Policy). Customer may also create more granular content filtering rules that may, for example, coach users on corporate policy (Advanced Policy). Content Filtering can be configured to block web searches based on keywords, and can also be implemented by IP address or URL name.

SD-2.2.5. Roaming and Mobile User Support

Section Effective Date: 30-Jan-2015

The Roaming and Mobile User Support service component provides the capability to set policy controls over group and individual user level access to the Internet to provide mobile or travelling users with the same protection as corporate users regarding Web Filtering and Malware Scanning.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SD-2.2.6. Application Control

Section Effective Date: 30-Jan-2015

The Application Control service component provides filtering controls for end user access to Web 2.0 applications, i.e., Video and Audio streaming, IM control, VOIP, Peer to Peer, Games. Application Control uses IPS protocol decoders that analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

SD-3. AT&T Cloud Web Security Service – Features and Capabilities

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service also provides, on an optional basis, the following additional features and capabilities.

SD-3.1. Integration with Customer's Data Loss Prevention System

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service integrates with customer's Data Loss Prevention system through redirect of traffic (on an encrypted basis) to permit the local DLP solution to inspect the network traffic.

SD-3.2. Log Data

SD-3.2.1. Anonymization of Log Data for International Privacy Regulations

Section Effective Date: 30-Jan-2015

Certain countries have privacy requirements for user data to be anonymized in reporting, which will anonymize the user ID in CWSS logs. The Service provides options to not log user ID, group ID and client IP address. The service also provides data retention policies.

SD-3.3. IPSec Support

Section Effective Date: 30-Jan-2015

The Service supports use of IPSEC tunneling. IPSEC tunnels transport traffic in an encrypted mode from the customer's site or network to the Cloud Web Security Gateways.

SD-3.3.1. IP Sec Connection to Network Based Firewall (NBFW)

Section Effective Date: 03-Apr-2015

IPSEC Connection to Network Based Firewall (NBFW)

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

Customers who purchase MSS-NB and CWSS may opt to use a IPSEC tunnel to connect MSS-NB to the CWSS provider. This option allows Internet browsing access with minimal workstation configuration changes because there is no browser proxy configuration required. Using a policy-based feature on MSS-NB, traffic that is destined to an IP address of “any” (i.e. 0.0.0.0/32) that has a destination TCP port of 80 or 443 can be sent to CWSS through the IPSEC tunnel.

When using the IPSEC option with CWSS, Customer understands there is neither a) monitoring of the IPSEC tunnel by AT&T, or b) automated failover to a secondary CWSS location. If the CWSS location is unreachable, it is the Customer responsibility to submit an expedited MACD and to notify the GCSC to change the IP address to a different CWSS node. The following example illustrates one scenario:

CWSS Public Address	
Primary	198.135.124.164
Secondary	199.116.171.164

In this example, if the Primary CWSS center was unreachable and the Customer was unable to browse to the Internet through CWSS, the customer would initiate a MACD request and call the GCSC operations center for an expedited change. The change would be a request to modify the destination of the IPSEC definition from 198.135.124.164 to 199.116.171.164. To make the request easier to implement, customer should maintain a list of primary, secondary, and tertiary IP addresses that can be used.

SD-3.4. Explicit Proxy Support

Section Effective Date: 30-Jan-2015

The Service supports Explicit Proxy Support. Explicit Proxy allows for simple integration with the browsing client. This configuration can be optionally managed using a PAC file from AT&T Cloud Web Security Service.

SD-3.5. SSL Support

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service allows for interception of SSL transactions specifically HTTPS. This enables CWSS to inspect, categorize and scan SSL transactions to help provide a safe Web experience.

AT&T Cloud Web Security Service provides an encrypted SSL session for roaming users so hackers can't eavesdrop on the User's session.

SD-3.6. User Authentication

SD-3.6.1. SAML 2.0 (Security Assertion Markup Language)

Section Effective Date: 30-Jan-2015

The Service supports SAML 2.0. SAML 2.0 is used to represent and exchange user identity and authentication data between parties. It provides web single sign-on (SSO) capability.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SD-3.6.2. Active Directory Integration

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service synchronizes with on-premises Active Directory systems through the use of the Authentication Agent (AA). Authentication Agent uploads the Active Directory user and group lists both daily and on-demand. The user and group names are used to populate the policy editing framework. All connections originate from AA and are encrypted outbound to the AT&T cloud infrastructure as needed. Alternatively, authentication can be enabled in which the service validates the user provided credentials back to the AD in real-time. AA can also act as a SAML IDP (Identity Provider).

SD-4. Reporting and Administrative Portal

Section Effective Date: 30-Jan-2015

The AT&T Cloud Web Security Service administrative portal allows Customer administrators to view their corporate policies and manage the Service using a graphical, web-based interface. Once the customer administrator makes and saves changes to their policies and selects the Deploy button, the change is pushed to the Web Security gateway, which is inspecting traffic. Management of users (add/delete users and user groups) will take place on the customer's Active Directory.

Using the portal, the administrator can:

- Set web filtering policies (block and allow categories, white list/black list)
 - Block or allow predefined categories such as "Personal Relationships", "Internet Radio and TV", etc. which contain the most common URLs (facebook.com, myspace.com, pandora.com, etc.)
 - Block or allow predefined classifications such as "Image Search", "Video Search", etc.
 - Block or allow custom categories created by the customer administrator containing specific URLs defined by the customer administrator
 - Manage identity based user group policies- add, change, delete and move rules,
- Manage Malware Scanning policies to control virus attacks, spam and spyware.
 - Allow administrators to view, create, change and delete Malware scanning profiles and file filter profiles.
- Manage Application Control List Profiles for IM, Audio and Video Streaming, etc.
 - Allow administrators to view, create, change and delete Application Control profiles and file filter profiles.
- Manage Web Content Control policies to control Java applets, Active X and Cookies.
- Allow administrators to view, create, change and delete Web Content Control profiles and file filter profiles.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

- Audit logging capability includes the individual(s) who made the change, what was changed and when it was changed. Audit logs can be searched by specifying a time period, category or type of log and type of action taken.
- Customize alert pages via direct input or file upload- dynamically generated HTML pages displayed to the end User when they attempt to access prohibited web content. Customer can choose a standard Block Alert Page or their own customized content, which can be uploaded via the portal.

SD-4.1. Reporting

Section Effective Date: 30-Jan-2015

Reports are provided via the AT&T Cloud Web Security Service portal. Automated reports are available on overall traffic, blocked URLs, spyware and web viruses stopped. Reports can be downloaded to PDF, PowerPoint, Excel or Snapshot.

SD-5. Responsibilities of the Customer

SD-5.1. Customer Responsibilities

Section Effective Date: 30-Jan-2015

Customer is required to implement the following requirements to qualify for use of the Service:

- Customer will supply AT&T with all technical data and any additional information required in order for AT&T to activate the AT&T Web Security Services. The AT&T Cloud Web Security Service does not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection.
- Customer agrees to undertake all necessary steps to keep confidential and not reveal or disclose to any third party, without prior permission from AT&T, any username or password information provided to Customer by AT&T. If for any reason AT&T believes that there has been a security related breach, AT&T may take whatever action AT&T deems appropriate to remedy the situation.

Customer is required to:

- Install AT&T-provided software for communication between customer-owned authentication servers and laptops and Cloud Web Security Service. Manage installation of the AT&T Cloud Web Security Service Client on all remote user laptops;
- Manage installation, if any, of software on all mobile devices;
- Notify AT&T of any unauthorized use of Customer's account;
- Implement recommended changes or service upgrades, as reasonably requested;
- Designate a Single Point of Contact (SPOC) to provide Customer Tier 1 helpdesk to internal Customer users; and this SPOC shall adhere to the roles and responsibilities as designated in the Agreement;

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

- Verify on a regular basis that the customer activated policies are displayed accurately in the administrative portal. Notify AT&T in writing, within 24 hours, if Customer notices a discrepancy between the functionalities displayed on the portal and the ones Customer deems to have activated;
- Create service policies for the features they have purchased, ex. “Web Filtering, Malware Scanning, Application Control.

SD-5.2. Customer Compliance Responsibilities

Section Effective Date: 30-Jan-2015

When using the Service, Customer is responsible for compliance with all applicable laws in the jurisdictions in which the Service is used. In certain countries, Customer may be deemed to be the importer of technology (e.g., the Client software). This technology includes encryption software that may be subject to restrictions with respect to its importation and/or use in certain countries. Customer agrees that it and/or its Users will not attempt to import such technology into any countries where AT&T does not offer the Service. Any violations of this provision shall entitle AT&T to immediately terminate Customer's Service Agreement.

SD-6. Customer Care/Technical Support

Section Effective Date: 30-Jan-2015

AT&T Cloud Web Security Service Customer Care/Technical Support is available to Customers by calling a toll-free (or paid) global service support telephone number.

SD-6.1. Maintenance Notification

Section Effective Date: 30-Jan-2015

AT&T will use commercially reasonable efforts to notify customers about larger service releases and data center maintenance at least two weeks in advance; and of all other maintenance releases at least seventy-two (72) hours in advance.

SD-7. Use of Service

SD-7.1. Activation of Service

Section Effective Date: 30-Jan-2015

Customer will be provided with an activation code via a welcome email (“Activation Code”). Customer may activate the AT&T Cloud Web Security Service at any time by using the Activation Code (“Activation” or “Activate”). The activation date shall be the date of the welcome email (“Activation Date”). Upon Customer’s request, AT&T will provide an onboarding session to assist the Customer in the Activation process. Billing will commence on the Activation Date.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

Customer will route web traffic to the AT&T Cloud Web Security Service in accordance with the number of users with subscribed licenses ("Subscriber(s)"). A Subscriber is defined as an individual Customer's employees, contractors, agents and other human users of Customer's network that establish a connection or login to AT&T Cloud Web Security Service through a local device such as a computer, laptop, phone, tablet or other mobile device. The maximum number of devices (e.g., computer, laptop, phone, tablet, or other mobile device) that a Subscriber may utilize to access AT&T Cloud Web Security Service is limited to four (4) devices at any given time.

SD-7.2. Number of Subscribers

Section Effective Date: 30-Jan-2015

AT&T may audit Customer use from time to time to determine if the number of seats on the Service has grown above the number of contracted seats. In the event the audit reveals that there are more users than Subscribers, additional charges will apply; amounts due in such event will be handled via the Change Control Process.

Number of seats is defined as the number of the customer's users and servers that can potentially send traffic through the service or the number of users and servers identified in the customer's Active Directory. The number of seats may differ from the number of Customer authorized Users utilizing the Service at any given time (Concurrent users).

SD-7.3. Amount of Traffic

Section Effective Date: 30-Jan-2015

AT&T may conduct monthly audits of the total amount of traffic passing through the AT&T Cloud Web Security Service, and to inform Customer of any material and/or persistent deviations to the expected amount of traffic. The average expected Cloud Service usage will be 166,667 Users per Gbps which is approximately 2 Gigabytes per User per month ("Baseline Traffic"). If AT&T determines material and/or persistent deviations to the Baseline Traffic, the parties will work in good faith to immediately resolve any traffic issues.

SD-8. End User License Agreement (EULA)

Section Effective Date: 30-Jan-2015

Use of the Service and any software downloaded as part of the Service is subject to and use of the service indicates acceptance of the End User License Agreement ("EULA"):

SD-8.1. AT&T Cloud Web Security Service

Section Effective Date: 30-Jan-2015

Subject to the terms and conditions herein, during the Service Term (as defined below) AT&T will provide the following AT&T Cloud Web Security software-as-a-service ("Service") to Customer: (i) inbound and outbound Web content security and filtering and malware detection

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

and filtering; (ii) hosted reporting of Subscriber (as defined below) traffic; in each instance of (i) and (ii) above based on Customer Configurations (as defined below) set by Customer; (iii) certain data, images, text, content, APIs, tools or other information or materials provided by AT&T in conjunction with the Service; and (iv) a software client that may be downloaded by Customer ("Software") for use by Subscribers (defined below) to access the Service. As used herein, "Subscriber(s)" means Customer's employee, contractor, agent and other human user(s) of Customer's network on an individual basis that Customer pays a fee to AT&T in order to allow a connection or login to the Service through a local device. The Software component of the Service includes any and all updates, upgrades, bug fixes, dot releases, version upgrades, or any similar changes that AT&T makes available to Customer from time to time.

SD-8.1.1. Customer Configuration

Section Effective Date: 30-Jan-2015

The Service does not include Customer configurations, policies and procedures implemented and set by Customer available through the Service, including, without limitation, the selection of filtered categories and web application controls (collectively, "Customer Configurations"). Customer acknowledges and agrees that Customer is solely responsible for selecting the Customer Configurations and assuring that the selection conforms to Customer's policies and procedures and complies with all applicable laws and regulations in jurisdictions in which Customer is accessing the Service.

SD-8.1.2. Passwords

Section Effective Date: 30-Jan-2015

As used herein, "Passwords" shall mean Customer established passwords, temporary passwords provided by AT&T, security credentials, or authentication keys provided or used in relation to the Service. Customer is solely responsible for monitoring and controlling access to the Service, maintaining the confidentiality of the Passwords and for any use of the Service that occurs using such Passwords.

SD-8.1.3. Right to Access Service; Software License

Section Effective Date: 30-Jan-2015

Subject to the terms and conditions herein and the express restrictions contained in this Section, AT&T grants to Customer (i) the right to access and use the Service (and any software provided by AT&T as part of the Service) during the Pricing Schedule Term for Subscribers' and for Customer's own internal business operations and not for the benefit of any other person or entity; and (ii) a personal, non-transferable, non-exclusive, non-sublicensable license during the Service Term to use and distribute the Software to Customer's Subscribers in object code form only, solely for the purpose of accessing the Service.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SD-8.1.4. Use Restrictions*Section Effective Date: 30-Jan-2015*

Customer shall not, and shall prevent Subscribers from using the Service to: (i) resell, rent, lend, lease distribute, or timeshare the Service (including on a “service bureau” basis), or otherwise provide third parties with access or grant third parties rights to the Service, (ii) alter or remove any marks or proprietary legends contained in the Service; (iii) circumvent or otherwise interfere with any authentication or security measures of the Service; (iv) interfere with or disrupt the integrity or performance of the Service; (v) send SPAM or any other form of duplicative and unsolicited messages, other than marketing and promotional messages to Customer's clients and prospective clients as contemplated by the Service; (vi) use the Service for proxy avoidance or anonymization; (vii) violate the terms of use or other agreements governing the use and access of third party websites; (viii) access all or any portion of the Service by means of any crawler, scraper, bot, spider, or any other similar script or automated process; (ix) transmit through or post on the Service unlawful, libelous, tortious, infringing, or defamatory material; or (x) transmit material containing software viruses or other harmful or deleterious computer code, files, scripts, agents, or programs. Customer shall not reverse engineer, decompile, disassemble or otherwise attempt to discover the object code, source code or underlying ideas or algorithms of the Software, and shall not modify, translate, or create derivative works based on any element of the Software.

SD-8.1.5. Acceptable Use*Section Effective Date: 30-Jan-2015*

Subscribers shall not use the Service for any purpose other than as expressly authorized herein.

SD-8.1.6. Reservation of Rights; Ownership*Section Effective Date: 30-Jan-2015*

Except for the rights expressly granted herein, no other rights, express or implied, are granted to Customer under these terms. All right, title and interest in and to the Service, the Software and related Documentation are and shall remain the exclusive property of AT&T and its licensors. Customer acknowledges and agrees that: (i) the Service, the Software and related Documentation are protected under U.S. and foreign copyright and other intellectual property laws; (ii) AT&T and its licensors retain all copyrights and other intellectual property rights in the Service, the Software and related Documentation; (iii) there are no implied licenses under this license and any rights not expressly granted to Customer hereunder are reserved by AT&T; and (iv) Customer acquires no ownership or other interest in the Service, Software, or related Documentation (other than right to access the Service and the license rights expressly stated herein).

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SD-8.2. Customer Data

SD-8.2.1. Definition of Customer Data

Section Effective Date: 30-Jan-2015

In its provision of the Service, AT&T may receive, store and/or process network traffic data ("Traffic Data"), such as time of transaction, Subscriber IP address, username, URL, URL category, status (success or error), file type, filter result (allowed or denied), virus id, and other metadata (e.g. browser software used), and any other network traffic (and data related thereto) sent to or received from Customer through use of the Service, in detail and/or in an aggregate form. In such cases, AT&T is acting in its capacity as a data processor and will process the Traffic Data of Customer only on behalf of and under the direction of Customer (and its designees). In addition, AT&T may receive, store, process and retrieve other personally identifiable information uploaded through the AT&T Cloud Portal or other means ("Administrative Data"). Administrative Data includes, for example, administrator identifying information, Subscriber and group names, and other personally identifiable information. "Customer Data" means Traffic Data and Administrative Data.

SD-8.2.2. Limited Use

Section Effective Date: 30-Jan-2015

While Customer (and its Subscribers) retain all rights to the Customer Data submitted to the Service, AT&T may store, process, retrieve, and disclose Customer Data for the following purposes: (i) providing the Service to Customer; (ii) analyzing, maintaining and improving the Service; (iii) complying with legal, or governmental requirements if AT&T is required to do so; (iv) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service; and (v) anonymously aggregating and statistically analyzing malicious or unwanted content.

SD-8.2.3. Obligations; Indemnification

Section Effective Date: 30-Jan-2015

Customer represents and warrants that: (i) it will comply with all applicable privacy and data protection laws and regulations applicable to its business and its performance of its obligations under these terms with respect to any Customer Data uploaded to, submitted to, stored on, or processed by the Service; and (ii) it will provide any notices and obtain required consents related to its use of the Service and AT&T's provision of the Service, including those related to the collection, use, processing, transfer, monitoring and disclosure of Customer Data.

SD-8.3. Open Source Software

Section Effective Date: 30-Jan-2015

Software distributed with the Service may include open source software which is subject to the terms of the applicable open source software license agreement and not the terms and conditions herein. Customer may access the open source software copyright notices, terms and

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

conditions. All open source software is provided WITHOUT ANY WARRANTY INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Copyrights to the open source software are held by the copyright holders indicated in the copyright notices in the corresponding source files. Source code can be made available to Customer as required by the applicable open source software license agreement as set forth in <http://www.bluecoat.com/3PNoticesandTerms>.

Service Level Agreements (SLA)

SLA-1. AT&T Cloud Web Security Service Level Agreement Terms

Section Effective Date: 30-Jan-2015

AT&T has established performance objectives for AT&T Cloud Web Security Services. While AT&T does not guarantee performance objectives, AT&T will provide credits to an eligible Customer when a performance objective is not met. If a SLA states that a Customer is eligible for an AT&T Cloud Web Security SLA credit, this means that the Customer is eligible subject to the terms, definitions and any exclusions or limitations stated herein.

SLA-1.1. Definitions

Section Effective Date: 30-Jan-2015

The definitions below apply to the Service Level Agreements described in this Service Guide.

- “Outage” is (unless stated otherwise) measured in minutes and is the time a Service or Service Component is unavailable on an unscheduled basis. An Outage does not include time when the Service or Service Component is unavailable during a scheduled period for maintenance, repair or upgrade.
- “Maintenance” time or “Planned Down Time” can be either for “Scheduled Maintenance” or “Emergency Maintenance”. “Scheduled Maintenance” is maintenance, repair or updating activities that are performed during a maintenance window established by AT&T or a maintenance window agreed to by AT&T and Customer. AT&T may also perform Scheduled Maintenance by providing Customer a minimum of five (5) business days’ notice prior to the day the Scheduled Maintenance will occur. “Emergency Maintenance” is unscheduled maintenance, repair or updating activities that are necessary in order to protect AT&T facilities, network services or the security of Customer equipment or property. AT&T will attempt to provide reasonable notice to the Customer when AT&T determines that it is required to perform Emergency Maintenance prior to the maintenance activity being performed.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
 See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
 AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

SLA-1.2. SLA Exclusions*Section Effective Date: 30-Jan-2015*

Notwithstanding any other clause herein, no commitment is made hereunder with respect to: (i) the Service being used in conjunction with hardware or software other than as specified in AT&T's published documentation located at <http://cloudwebsecurity.att.com/docs/am/AMDoc.htm>; (ii) alterations or modifications to the Service, unless altered or modified by AT&T (or at the direction of or as approved by AT&T); (iii) defects in the Service due to accident, hardware malfunction, abuse or use other than in accordance with AT&T's published documentation (unless caused by AT&T or its agents); (iv) an evaluation of the Service or other trial provided to Customer at no charge and (v) any problems or issues of connectivity due to the network or internet connection of Customer.

SLA-1.3. SLA Reporting and Claims*Section Effective Date: 30-Jan-2015*

To file a claim or termination notice with refund claim, as applicable, Customer must include in a written notice the following details:

- Downtime information detailing the dates and time periods for each instance of claimed downtime or Average Latency failure, as applicable, during the relevant month (or calendar quarter for termination with a refund claim).
- An explanation of the claim made under this Service Level Agreement, including any relevant calculations.

Claims may only be made on a calendar month basis and only for the previous calendar month or part thereof. All claims must be made within 10 days of the end of each calendar month. A termination notice with a refund claim must be made within 10 days of the end of a calendar quarter.

All claims will be verified against AT&T's system records. Should any claim submitted by Customer be disputed, AT&T will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide to Customer a record of Service availability for the period in question. The record provided by AT&T shall be definitive. AT&T will provide records of Service availability in response to valid Customer claims upon Customer's request. AT&T shall respond to a Customer claim within 10 days of claim submission.

All remedies referred to herein are subject to Customer having paid all applicable fees and fulfilled all of its obligations hereunder.

Notwithstanding any other clause herein, the remedies herein do not apply to any matters arising due to any of the following:

- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.
- Excused Outages.
- Hardware, software or other data center equipment or services not in the control of AT&T or outside the scope of the Service.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

- Hardware or software configuration changes made by the Customer without the prior written consent of AT&T.

SLA-1.4. SLA Claims Limitations

Section Effective Date: 30-Jan-2015

Customer may only receive Service Credits equal to up to one (1) month's AT&T Cloud Web Security Service Monthly Service Charges during any calendar quarter. Service Credits do not include installation charges, Monthly Recurring Charges for Services not included in the Service Level Agreement for which a Service Credit is paid, or charges related to additional services. Any SLA credit paid to Customer shall constitute the sole and exclusive remedy available to Customer for a failure by AT&T to meet a performance objective.

SLA-2. SLA Availability

Section Effective Date: 30-Jan-2015

The performance objective for Service Availability for AT&T Cloud Web Security Service is that the Service is available 99.999% of the time and the configuration portal of the Service will be available 99.9% of the time, except as provided below. If AT&T does not meet this performance objective in a given calendar month, Customer is eligible for remedy as described herein.

Availability will be calculated per calendar month as follows:

Total – Non-excluded – Excused Outages X 100 > (99.999% general availability; 99.9% availability of the configuration portal) Total – Excused Outages

- “Available” or “availability” means (a) with respect to general availability of the Service, that requests for web pages are completed and web pages are returned regardless of Latency; and (b) with respect to availability of the configuration portal, that the portal is available for log on. Service unavailability will not be assessed due to: i) a failure of Customer to correctly configure the Service in accordance with AT&T's policies or instructions; (ii) the unavailability of a specific web page or data center outage; or (iii) unavailability of one or more specific features, functions, or equipment hosting locations within the Service, while other key features remain available.
- “Total” means the number of minutes for the calendar month.
- “Non-excluded” means unplanned downtime.
- “Excused Outages include:
 - Planned downtime. With respect to planned downtime, AT&T shall provide Customer with as much notice as practical under the circumstances and strives for a minimum of 72 hours or more of advance notice. In all cases, AT&T shall provide a minimum of 24 hours' advance notice of planned downtime. AT&T shall make commercially reasonable efforts to schedule planned downtime in off peak hours. Customer acknowledges that AT&T may, in certain situations, need to perform emergency maintenance (unplanned downtime) on less than 24 hours advance notice.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
 See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
 AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

- Any unavailability caused by circumstances beyond AT&T's reasonable control, including, without limitation, acts of God, acts of government, flood, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (excluding those involving AT&T employees), computer or telecommunications failures or delays involving hardware or software not within AT&T's possession or reasonable control, and network intrusions or denial of service attacks.
- For any partial calendar month during which Customer subscribes to the Service, general availability will be calculated based on the entire calendar month, not just the portion for which Customer subscribed.

SLA-2.1. SLA Availability – Remedies

Section Effective Date: 30-Jan-2015

In the event that any Service is not Available for reasons other than an Excused Outage and subject to the requirements of Section 5 below, AT&T will provide an extension of the current term of subscribed Services at no charge to Customer in an amount equal to 3 days of additional Services for each 1 hour or part thereof that the Service is not available, subject to a maximum of a full month of extended Services for any one year of subscribed Services.

SLA-2.2. Chronic Failure

Section Effective Date: 30-Jan-2015

Subject to the exclusions and limitations stated in this Service Level Agreement section, if the Service is not Available, for reasons other than an Excused Outage, and such non-availability is attributable solely to AT&T and not to Customer, in whole or in part, for more than thirty-six (36) hours in any calendar quarter, Customer may terminate the Service upon thirty (30) days' written notice to AT&T. In the event that AT&T validates the conditions of the termination under this Section, AT&T shall refund to Customer a pro-rata portion of the Service fees paid in advance and not yet used within forty-five (45) days from termination.

SLA-2.3. SLA Latency

Section Effective Date: 30-Jan-2015

The performance objective for Average Latency for the Service is 100 milliseconds. If AT&T does not meet this performance objective in a given calendar month, Customer is eligible for remedy as described herein.

"Latency" refers to the web page load time attributable to the Service.

"Average Latency" refers to the average time it takes for the Service to scan, process and apply the Customer policy to the web content data, assuming a 100KB web page, and DOES NOT include the time required to download the web page from the origin content server (OCS) to the Service.

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016

Average Latency is determined by the monthly average among samples taken by AT&T in a given month.

SLA-2.4. SLA Latency Remedies

Section Effective Date: 30-Jan-2015

Subject to the requirements of Section 5 below, in the event that the Latency commitment is not met in any month for reasons other than an Excused Outage or actions attributable to Customer, AT&T will provide an extension of the current term of subscribed Services at no charge to Customer in an amount equal to an additional one week of Services, subject to a maximum of a full month of extended Services for any one year of subscribed Services.

Pricing (P)

P-1. AT&T Cloud Web Security Service Pricing

Section Effective Date: 30-Jan-2015

Applicable rates, prices, discounts and other terms for the Service are set forth in the Pricing Schedule attached to the Customer Services Agreement.

Country-Specific Provisions (CSP)

CSP-1. Country-Specific Provisions

Section Effective Date: 30-Jan-2015

Except where indicated, the following terms are in addition to the terms stated in the Service Guide.

CSP-1.1. Country Unique Terms

Section Effective Date: 30-Jan-2015

None

End of Service Guide

*The AT&T Business Service Guide is subject to change by AT&T from time to time.
See <http://serviceguidenew.att.com> for current version.*

© 2016 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

This document reflects the Service Guide in effect as of March 09, 2016