AT&T Cloud Web Security Service (Cloud WSS)  
Customer Expectation Guide

Activation  
*Key Information, Responsibilities and Milestones*

Last Update: 6/30/2017
Thank you for choosing the AT&T Cloud Web Security Service (Cloud WSS) and for allowing us the opportunity to serve you.

With AT&T Cloud Web Security Service you can set company policies which:

- Help protect your company against web-based viruses, worms and other malware threats
- Boost productivity and help avoid abuse of corporate resources (ex: bandwidth) by monitoring and controlling web site access.
- Control the use of applications on popular sites without restricting site access
- Monitor and control data leak prevention.
- Helps to provide web protection to roaming users

AT&T Cloud WSS service can be purchased as stand-alone or as part of a hybrid solution with the AT&T Proxy Firewall service.

At AT&T, we strive to provide you with a world-class user experience. We’ll work closely with you to help make your Cloud WSS installation as easy as possible. Please take a few minutes to review the following information, which identifies key requirements and responsibilities throughout the installation process. It provides important information that your Technical Point of Contact (TPOC) or Authorized Representative/Agent will need to know for your service installation. This information is provided in an attempt to summarize the key requirements and responsibilities to activate the Cloud WSS. It does not modify or supersede your agreement with AT&T.

Once again, thank you for choosing AT&T Cloud Web Security Service.
Table of Contents:

AT&T Cloud WSS Summary ............................................ Page 3
AT&T Cloud WSS Special Considerations ............... Page 3
Implementation Planning Requirements ............... Page 4
Key Contacts ................................................................. Page 6
Your Installation ......................................................... Page 6
Billing ................................................................. Page 9
Maintaining Your Cloud WSS Account ............... Page 9
Appendix A – Cloud WSS Billing Expectations ...... Page 11
Appendix B – Service On-boarding Planning Worksheet Page 12
Appendix C – Identifying your Service Subscription ID Page 13
Appendix D – Access Methods Summary .............. Page 14
Appendix E – Customer Portal Overview ............... Page 15
Appendix F - Bandwidth Limitation FAQ ............... Page 17
AT&T Cloud Web Security Service (Cloud WSS) Summary

AT&T Cloud Web Security Service helps to provide protection against malware and other Web-borne threats to your network security. The service also provides a Web-based interface or a Cloud WSS portal, to define advanced or basic content filtering policy, control specific Web Application access, and to generate reports on all Web-based activity. Refer to the following sections for more details.

Malware Protection

AT&T Cloud Security Service utilizes content analysis technology, which is designed to provide real-time protection against known and newly-arriving Web-borne threats. The service uses an ecosystem of content analysis and in-line scanning technology (from multiple vendors) to examine Web content. The resulting behavioral analysis identifies malicious and suspicious sites, bot-net traffic, and phone-home malware which are categorized in real-time.

Content Filtering

AT&T Cloud Security Service enables you to define a content filtering policy that can meet business requirements and can be tailored to support the local and global environment. The Basic Policy consists of a combination of blocked and allowed Web content categories and trusted and blocked sources and destinations that apply globally to all users. You also have the Advanced Policy option to create more granular rules. For example, you can coach users on company policy when a User attempts to access a restricted site; block unauthenticated Users; and create allow or block lists for specific Web destinations. The Advanced Policy also provides dynamic rating algorithms that identify and categorize Web content in real time to provide URL filtering.

Web Application Controls

AT&T Cloud Service provides policy options that control various aspects within certain Web applications. These options might include the ability to block post requests, attachments and downloads. The Cloud WSS portal displays the currently supported Web applications, including aspects within the application that are available to control. For example, you can allow employees to access Facebook, but prevent them from uploading video or pictures. Another example is to allow employees to access and use Webmail, but prevent them from sending attachments through Webmail. You can also enforce the browser SafeSearch feature and keyword search controls for all major engines, including media search engines.

Management, Policy, and Reporting

Access to AT&T Cloud Web Security Service is available through the Cloud WSS portal. This Web-based management tool allows you to navigate between the Content Filtering, Malware Scanning, and Web Application Control modules to define policies and generate reports. Your administrators can define roles that limit access for other users. For example, one role could support the addition of a Cloud WSS user who has access only to the Reporting interface, but not allow them to define policy or configure the service.

You can define and configure policies to implement and use the Service in accordance with your own requirements and the applicable regulations to your company’s particular industry, geography and business. Depending on the mode or module, this can be very basic, such as globally blocking specific categories or Web Applications. In the Content Filtering module, administrators have the option to define more granular
policies, such as determining what times Users can access specific sites or categories. For Web Applications, they can select options such as allowing Facebook but blocking file/video uploads.

When Users begin sending traffic to the cloud service, the generated access logs provide the basis for extremely comprehensive and interactive reports. There are high-level reports, trend reports and specific reports—to enable full visibility on its network. Administrators can use this data to further manage policies and provide coaching when acceptable Web use policies are not followed.

Cloud WSS provides a network-based, fully managed solution that:

- Does not require additional equipment at the customer premises. You subscribe to, rather than purchase, Cloud Web Security. This reduces capital expenditure, risk of technological obsolescence and the need for additional staff.
- Allows you to monitor your Web traffic 24x7 for threats so appropriate measures can be taken to help secure your network(s)

**Cloud WSS Special Considerations**

There are no premises-based components managed by AT&T for the service.

You are responsible for configuring and maintaining your web and network components as well as web security policies.

**Implementation Planning and Requirements**

**Access Requirements:**

Customers are required to have Internet connectivity with sufficient bandwidth to handle inbound and outbound Web traffic load.

**Premises and Site Requirements:**

Prior to completing the service implementation, there are few items that you need to consider:

**Determining Connection Methods:**

AT&T Cloud Web Security Services allows you to route internet traffic using several connection methods:

- Firewall Internet Protocol Security (IPSec) or Virtual Private Network (VPN)
- Proxy Forwarding (using AT&T Proxy Service)
- Client Connector (for Roaming Users)
- Explicit Proxy
- Trans-Proxy (Explicit over IPSec)
- Mobile Device support
Please use this link for a more detailed description of each connection method:

(https://cloudwebsecurity.att.com/docs/am/AMDoc.htm)

You will select one or multiple access methods depending on their network architecture and requirements.

**Determining Authentication Requirements:**

If you need to manage policies and report traffic based on Groups and Users, you will be required to install and configure the Authentication Connector software, which will interface with your company’s Active Directory to obtain user’s information.

If you use a terminal server application, you will need to set up Captive Portal via the Customer Portal. Captive Portal is a challenge-based authentication option which presents a login screen to users trying to access the Internet.

**Implementation Preparation:**

You will need to complete the following steps in preparation for service implementation (on-boarding):

1. Identify and complete required network changes to allow selected access methods (See Appendix D for a detailed list of ports/protocols for each access method)
2. Once the service order is completed, AT&T will send you an e-mail containing information to complete the registration process.
3. Go to [https://cloudwebsecurity.att.com/Register](https://cloudwebsecurity.att.com/Register) to complete the service registration.
4. Depending upon the access method and authentication requirements, you will be required to install additional components:
   a. Install Client Connector to support Client access method. (Use the following link for detailed instructions: [https://cloudwebsecurity.att.com/docs/am/AMDoc.htm](https://cloudwebsecurity.att.com/docs/am/AMDoc.htm) (Remote Users Only Access Method)
   b. Install Authentication Connector to support integration with You AD (Use the following link for detailed instructions: [https://cloudwebsecurity.att.com/docs/am/AMDoc.htm](https://cloudwebsecurity.att.com/docs/am/AMDoc.htm) (User/Group Names in Policy)
5. An AT&T Sales Engineer will work with you to complete the Cloud Web Security Services On-boarding Worksheet (Appendix B)
6. An AT&T Sales Engineer will schedule the Service Turn-Up (On-boarding) with you and AT&T Support.
7. Complete the Service Turn-up process.

Customer Premise Equipment (CPE) Requirements

The following are the Firewall/VPN devices currently supported to connect to AT&T Cloud WSS:

- Checkpoint®
- Cisco ASA®
- Cisco 1941®
- Fortinet®
- Juniper SRX®
- Juniper SSG20®
- Refer to the following link for an up-to-date list of all the models and OS supported versions: https://cloudwebsecurity.att.com/docs/am/AMDoc.htm (Firewall/VPN Access Method)

The following are the devices currently supported for Proxy Forwarding:

- Proxy SGOS 4.3.x, 5.x and 6.x
- Microsoft®ISA and TMG

Client Support

To install the Cloud WSS Client

a. Windows® client must have the Entrust Root CA 2048 installed. For more information consult the Client installation guides: https://cloudwebsecurity.att.com/docs/am/AMDoc.htm (Remote Users Only Access Method)
- Mac® clients require OS version 10.6.x or higher.

Key Contacts

Your Role:

- Local Contact (LCON), the individual at the site who is the main AT&T contact for access and site information. An alternate LCON should also be identified by you. The LCON should be kept aware of all local access/Local Exchange
- Billing Contact (BCON), the person who processes AT&T invoices
• Technical Contact, the individual who provides information regarding the order, and who would be responsible for completing an On-Line Technical Provisioning Document (OLTPD)
• Maintenance Contact, the individual who will engage AT&T technical support to report any trouble with the service (will be the same as the Technical Contact)

AT&T Role:

• AT&T Technical Support: will assist you with any issues during the implementation planning, service turn-up and maintenance. Specialized resources manage all Service Requests.
  – AT&T Cloud WSS Technical Support is available 24x7
  – Please use the following link to contact Support: https://cloudwebsecurity.att.com/#help|contactSupport
• AT&T Sales Engineer: Will work directly with you during the evaluation, implementation and maintenance phases. They will guide you on technical issues and interfacing with other AT&T supporting functions.

Service Installation:

Once service ordering is complete, you need to:

• Complete the service registration process
• Complete the service On-boarding session
• Perform the Service Activation Health Check

Service Registration

• Once the service order is processed, all contacts, including your primary administrator, will receive a service activation e-mail (E-Fulfillment E-Mail) containing instructions to complete the registration.
• This e-mail will contain the link and credentials to login into the AT&T Cloud Web Security Portal, which will present a self-guided wizard to complete the registration.

Service On-Boarding

Once you have completed the service registration process, the service is ready. In addition to the extensive online technical documentation available in the Customer Portal to assist you with configuring and managing the service, a AT&T Sales Engineer (SE) will coordinate the planning and delivery of an On-boarding online session, where AT&T Technical Support resources will guide you to set up the services and respond to any activation questions.
The On-boarding session will be completed as follows:

- Once the service order is received, the AT&T Sales Engineer (SE) will contact your Technical Contact to plan for the service installation
- The AT&T SE will provide you with the On-boarding Planning Worksheet (Appendix B)
- Your Technical Contact is responsible for completing the On-boarding Planning Worksheet with all required technical information and to deliver it to the AT&T SE, who will submit it to AT&T Technical Support in preparation for the On-boarding session
- AT&T SE will request and schedule the On-boarding session with AT&T Technical Support
- The On-boarding session will take place over a web conference
- During the On-boarding session, AT&T Technical Support will show you how to configure all applicable access methods, manage policies, set-up authentication, schedule and run reports, etc.
- At the end of the On-boarding session, a Service Health Check will be scheduled in two weeks.
- Note that your participation in this process is crucial. **Failure to participate and provide information in a timely manner will negatively impact your Activation Date.**

At the end of the On-boarding session, you should be able to start sending traffic to the service for the selected access methods.

Once you complete the Service Registration and On-boarding process, all service administration functions are also available via the Customer Portal (portal.threatpulse.com). Please refer to Appendix E for a more detailed description of the functions available in the Customer Portal.

**Service Health Check**

Upon the completion of the On-boarding session, you will start using the service and continue configuring required features. The primary objectives for the Service Health Check are:

- **Solicit and Understand** your experience to date and satisfaction with the Cloud Service
- **Address and Resolve** any outstanding questions, problems or Service Requests
- **Provide** actionable optimization and improvement recommendations where possible
- **Enhance and Expand** your knowledge of Cloud Service features and functionality
- **Overcome** any impediments to expanding the Cloud footprint within your organization

**Customer Responsibilities for Installation**

- Complete all required documents (e.g. Planning Sheets, network diagrams, etc.) and make them available to AT&T Sales Engineer no later than the scheduled appointment time
• Make available necessary personnel and resource(s) as specified by AT&T during the duration of Service
• Obtain all necessary change control approvals and to have scheduled required change control windows prior to AT&T service commencement
• Ensure internal business applications work with AT&T Cloud WSS
• Provide a static IP address for service implementation

Billing:

Account & Billing Information at:


Billing Inquiries – For billing questions, please call the toll-free number that appears on your bill

Maintaining Your Cloud WSS Account

How to Contact AT&T Cloud WSS Support

AT&T Cloud Web Security Service Customer

All AT&T Cloud Web Security Service customers will receive an operational welcome email shortly after the purchase of the AT&T Cloud WSS has been processed. This email will contain very important information regarding options for accessing operational support throughout the lifecycle of the AT&T Cloud WSS service that has been purchased. Operational support options are also outlined here:

Managed Security Service Operations Help Desk

Call: 800.727.2222, prompt 8, 2

Email: Managed.security@ems.att.com (Do not use this email for escalation)

For all support requests, you’ll be required to provide your Subscription ID (see Appendix C for details of how to obtain your ID in the Customer Portal).
Appendix A – AT&T CLOUD WSS Billing Expectations

How is your service billed?

Additional Fees and Taxes – Sales, excise and gross receipts taxes apply to AT&T Cloud Web Security. Other applicable taxes, fees, surcharges and shipping and handling fees may apply. Please consult your contract for details.

Disconnects - Disconnection of a Service Component(s) may be permissible. Please consult your contract for details.

Termination Fees – termination fees may apply. Please consult your contract for details.

Billing Inquires – For billing questions, please call the toll-free number that appears on your bill.

Payment Methods:
- U.S. Mail
- Overnight Mail
Appendix B – Service On-boarding Planning Worksheet

Each access method provides specific configuration planning worksheets available online.

Plan the Service Initial Configuration:
http://cloudwebsecurity.att.com/docs/am/AMDoc.htm

Plan Firewall/VPN Access Method:

Plan Proxy SG Forwarding Access Method:
http://cloudwebsecurity.att.com/docs/am/Content/Deployment/Tasks/Proxied/sg_fwding_plan_ta.htm

Plan Explicit Proxy
http://cloudwebsecurity.att.com/docs/am/Content/Deployment/Tasks/PACFiles/pac_plan_ta.htm

Plan for Client Connector
http://cloudwebsecurity.att.com/docs/am/Content/Deployment/Tasks/RemoteClients/client_planning_ta.htm
Appendix C – Identifying your Service Subscription ID:

- Login to Customer Portal
- Click on Services – Account Maintenance
- Select Account Provisioning
Appendix D – Connection Methods Summary


Please use the following link for an up to date description of access methods and required ports:

https://cloudwebsecurity.att.com/docs/am/AMDoc.htm
Appendix E – Customer Portal Overview

The following sections provide a high level description of the key functions available in the Customer Portal. Selected number of Customer users will have access to this website to perform multiple service administration and reporting tasks.

Modes: The Portal User Interface (UI) has two modes – Solutions and Service. To switch between modes click on the desired link in the upper right corner of the interface. You can easily tell which mode you are in by taking note of the background color. Solutions mode has a light blue background and Service mode has a tan colored background.

- **Solutions Mode:** The default mode when logging into Portal. Contains the following four tabs:
  - **Overview** - Contains the following menu items:
    - **Dashboard:** Displays commonly used built-in reports. The Dashboard is customizable by the Admin.
    - **Report Center:** Shows what reports are available and scheduled to be run. Reports can be downloaded, e-mailed, and archived in PDF, CSV, and XML formats.
    - **Object Library:** Allows an Admin to create policy objects. Global Objects apply to every user whereas User Defined Objects apply to individual users or groups of users.
  - **Content Filtering** - Contains the following menu items:
    - **Dashboard:** Displays commonly used built-in reports that apply specifically to Content Filtering.
    - **Reports:** Shows available reports that apply specifically to Content Filtering.
    - **Policy:** This is where policy rules can be created and modified.
  - **Threat Protection** - Contains the following menu items:
    - **Dashboard:** Displays commonly used built-in reports that apply specifically to Threat Protection.
    - **Reports:** Shows available reports that apply specifically to Threat Protection.
    - **Policy:** Allows an Admin to specify Trusted Sources and Trusted Destinations
  - **Search Engines** - Contains the following menu items:
    - **Dashboard:** Displays commonly used built-in reports that apply specifically to Search Engines.
    - **Reports:** Shows available reports that apply specifically to Search Engines.
    - **Policy:** Allows an Admin to enforce “Safe Search” on various search engines regardless of the settings in the Browser.

- **Services Mode:** Enter this mode by clicking “Service” in the upper right corner of the Portal. Contains 6 tabs:
  - **Network** – Contains the following menu items:
    - **Locations:** Allows an Admin to create or remove locations and displays the link for the “pac” file for Explicit connections.
    - **Mobility:** Allows an Admin to configure settings for mobile devices, download the Installer, and enable or disable Captive Portal. Displays the link for enrolling IOS Devices.
• **Authentication**: Allows an Admin to configure settings for Auth Connector, download the Installer, and enable or disable Roaming Captive Portal.

• **Bypassed Sites**: Allows an Admin to designate traffic to be bypassed from the Cloud WSS Service.

• **SSL**: Allows an Admin to enable or disable SSL Interception.

  – **Notifications** – Allows an Admin to customize error page content.

  – **Account Maintenance** - Contains the following menu items:

    • **Users**: Allows the Admin to Add, Delete, Enable, or Disable users.

    • **Report Filters**: Allows the Admin to control which users have access to reporting data.

    • **Account Provisioning**: Allows the Admin to view account information including client name, the supported number of users, and the account expiration date.

    • **Auditing**: Allows the Admin to review logged transactions like user logins and logouts.

    • **MDM, API Keys**: Allows an Admin to generate an MDM identifier and add API keys.

  – **Reporting** – Contains the following menu items:

    • **Cost Calculations**: Allows an Admin to change the currency and cost values for the Cost Calculations.

    • **Log Download**: Allows an Admin to download Log data.

  – **Appliance Monitoring** – Contains the following menu item:

    • **Setup**: Allows Admins to monitor the PDM statistics of their ProxySG appliances.

  – **Troubleshooting** – Contains the following menu items:

    • **Mobile Clients**: Allows an Admin to troubleshoot mobile client connections.

    • **iOS Devices**: Allows an Admin to troubleshoot iOS device connections.

    • **Common Policy Revisions**: Displays the date and time of the most recent common policy change.

For more information about Customer Portal usability, please use the following link:

http://cloudwebsecurity.att.com/docs/sol/SOLDoc.htm
Appendix F – Bandwidth Limitation FAQs

Why does Cloud WSS Service have a baseline traffic limit and how do you monitor?

The primary goal behind the limit is to make sure that there is no “run-away” or “rouge” usage of the Cloud WSS Service. This limit provides information that the service meets and exceeds the Service Level Agreement (SLA) for all our users. To enable our SLA, we constantly monitor our system performance at each of our global data centers. We also monitor traffic and numbers of users who connect via the web and through mobile connections for each customer account. This is part of our normal operations. This monitoring is automated, anonymous and available to our operations team. The baseline traffic limits enable our operations team to flag any anomalous usage patterns that has or could lead to system degradation. We are looking for “material and/or persistent” overages or overages that impact overall service quality. In the event of any material and/or persistent deviations from the Baseline Traffic, we will work in good faith to immediately resolve any traffic issues.

Are usage audits performed automatically or reactively?

The logs are collected automatically. The usage audit is performed quarterly, but it could also be triggered when we see sudden service degradation or abnormal load events. The audit is a manual process. The goal of this investigation is to get to the root cause of any unusual activity. We are typically looking for dramatically different usage patterns. If our preliminary assessments point to a certain customer site/ user, AT&T works with our account teams and that will trigger a customer notification.

How does the customer know he is approaching or exceeding usage?

The portal includes a report named “Bandwidth Used by Month” in Overview->Report Center (see screenshot) that will let you monitor the use in previous months.
What is the exact calculation for determining usage? Provide an example.

AT&T Cloud Web Security Service “Baseline Traffic” is expected to be approximately 6kbps average bandwidth per user calculated across the customer's population (this equates to approximately two Gigabytes of data per month per user). For example: a customer with 100 users licensed for the Cloud WSS would be expected to transfer approximately 200 Gigabytes of total data per month.

Under what conditions will action be taken to throttle / degrade or limit customer’s use of the service based on excess usage?

If a particular account or individuals are using greater than five times expected usage consistently or is producing other forms of excessive load considered to be impacting service quality (examples may include: number of connections, requests, error producing events, and any other abnormal or abusive use), then technical means to throttle/degrade the account or user may be implemented. Throttling is an extreme step. Resolutions may include Supplier’s throttling of the traffic or otherwise take actions to mitigate load while it addresses the issue with AT&T and the Customer.