AT&T Cloud Web Security Service: Release Notes

AT&T empowers enterprises to safely and securely choose the best applications, services, devices, data sources, and content the world has to offer, so they can create, communicate, collaborate, innovate, execute, compete and win in their markets. AT&T is trusted by a large percent of the Fortune® Global 500.

The AT&T Cloud Web Security Service solutions provide real-time protection against web-borne threats. As a cloud-based product, the Cloud Web Security Service leverages proven security technology, including the WebPulse™ cloud community.

With extensive web application controls and detailed reporting features, IT administrators can use the Cloud Web Security Service to create and enforce granular policies that are applied to all covered users, including fixed locations and roaming users.

This PDF version of the release notes provides information for the most recent major service releases (X.x). The online WebGuide version contains the full service record.
## Contents

**AT&T Cloud Web Security Service: Release Notes** ................................................................. 3

**Contents** ................................................................................................................................. 4

**Recent Features** ....................................................................................................................... 7

<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUL.26.2019</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>APR.26.2019</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>MAR.08.2019</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>NOV.16.2018</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>OCT.12.2018</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>SEP.07.2018</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>JUN.15.2018</td>
<td>WSS Feature Update</td>
</tr>
<tr>
<td>MAY.22.2018</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>MAR.13.2018</td>
<td>WSS Service Update</td>
</tr>
<tr>
<td>FEB.28.2018</td>
<td>WSS Service Update</td>
</tr>
</tbody>
</table>

**Recent Resolved Issues** ....................................................................................................... 14

<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>JUL.26.2019</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>APR.26.2019</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>MAR.08.2019</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>NOV.15.2018</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>OCT.12.2018</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>SEP.07.2018</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>MAY.22.2018</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>Mar.13.2018</td>
<td>Security Advisories</td>
</tr>
<tr>
<td>Feb.28.2018</td>
<td>Security Advisories</td>
</tr>
</tbody>
</table>

**Currently Known Issues** ..................................................................................................... 22

**Limitations** .......................................................................................................................... 27

**Compatibility Index** ............................................................................................................ 28

**Recent Unified Agent Resolved Issues** ................................................................................ 29

**Desktop Anti-Virus Compatibility** ........................................................................................ 33

**Supported Browsers** .............................................................................................................. 34
Supported Proxy Devices
AT&T ................................................................. 35
Microsoft ............................................................ 35

Supported SAML IDPs ............................................. 36

WSS Help System Update Log ..................................... 37
Edits—Access Methods WebGuide ................................ 39
Edits—Solutions WebGuide ........................................ 40
Edits—Access Methods WebGuide ................................ 40
Edits—Solutions WebGuide ........................................ 40
Edits—Access Methods WebGuide ................................ 41
Edits—Solutions WebGuide ........................................ 41
Edits—Access Methods WebGuide ................................ 41
Edits—Solutions WebGuide ........................................ 41
Edits—Access Methods WebGuide ................................ 42
Edits—Solutions WebGuide ........................................ 42
Edits .......................................................... 42
Edits .......................................................... 43
Edits .......................................................... 43
Edits .......................................................... 43
Edits .......................................................... 44
Access Methods WebGuide ........................................ 44
Recent Features

The following section describes the most recent features added to the Cloud Web Security Service.

WSS Service Update—JUL.26.2019

- WSS Agent.

  WSS Agent is the next generation of Unified Agent. Re-branded from Blue Coat to Symantec; ability to temporarily disable the agent; supports BNS with CloudSOC (see next feature).

  [WSS agent documentation](http://cloudwebsecurity.att.com/docs/sol/connectivity/endpoint/agent/conn-about-wssa.htm)
  [WSS agent documentation](http://websaas.dimensiondata.com/docs/sol/connectivity/endpoint/agent/conn-about-wssa.htm)

- Block Notification Service (BNS).

  Works in conjunction with the WSS Agent and the CASB CloudSOC. WSS Agents receive out-of-band notifications when content is blocked by CASB gatelet policies. This requires the WSS Agent; the Unified Agent is not supported.

  [Block Notification Service documentation](http://cloudwebsecurity.att.com/docs/sol/connectivity/endpoint/agent/conn-wssa-bns.htm)
  [Block Notification Service documentation](http://websaas.dimensiondata.com/docs/sol/connectivity/endpoint/agent/conn-wssa-bns.htm)

- Audit Log Expiry

  Previously, WSS Audit Logs (Service mode > Account Maintenance > Auditing) accumulated beyond the one-year required for GDPR compliance. With the exception of EULA agreement audit logs (when you or someone accepts the WSS EULA), the logs will now expire (be purged from the WSS database) after one year. The daily purge occurs at midnight UTC.

  To afford you time to download the audit logs before AT&T will not begin the mass deletion of 1-year-plus logs until one month after the date of this service update.

  The [Auditing page](http://cloudwebsecurity.att.com/docs/sol/Solutions/Admin/Account/adm_audit_ta.htm) also now allows to filter up to one year (a change from the previously afforded two weeks) and search by object type.

- Download APIs

  - If you use external systems to download WSS reporting access or audit logs or administer multiple location changes, you must now generate an API through the portal.

    [API documentation](http://cloudwebsecurity.att.com/docs/sol/api/api-keys.htm)

  - Automate audit log downloads through a REST API.

    [API documentation](http://cloudwebsecurity.att.com/docs/sol/api/api-audit-rest.htm)

- Auth Connector Page Revised.
The Auth Connector portal page (Service mode > Authentication > Auth Connector) is revised to provide more connection details and troubleshooting link.


- Anonymize the origin source IP address (XFF Header Controls).

You have the option to anonymize the origin source IP address.

http://cloudwebsecurity.att.com/docs/sol/Solutions/Admin/privacy/privacy-xff.htm

- Force English Translation in Notifications

You can force the Cloud Web Security Service to translate exception pages into English regardless of browser language version. The non-English browsers do not display the site review URL. Temporarily forcing English can aid with troubleshooting, including talking to Support Personnel who speak only English.

The option is on the Service mode > Notifications > Error Pages page.

- Allow or Deny Support Personnel Access

By default, AT&T Support Personnel can log in to customer accounts to assist with troubleshooting. Historically, this was approved through an email chain. Now you have the ability to allow or deny access.

The option is on the Service mode > Account Maintenance > Admin & Access page. The first row in the table (Support Operators) contains the option.

- New Access Log fields.

  - x-icap-reqmod-header(X-ICAP-Metadata)
  - x-icap-respmod-header(X-ICAP-Metadata)
  - x-random-ipv6

http://cloudwebsecurity.att.com/docs/sol/Solutions/Reference/accesslogformats-ref.htm

- New AClgon version—Provides a critical fix for dropped VPN connections.


- "Recent Resolved Issues" on page 14

**WSS Service Update APR.26.2019**

- May 27 Update—Notification of non-standard ports change.


- SSL Policy Editor/Mobile Decryption.

New editor to manage intercepting or bypassing SSL traffic. This allows you to create selective SSL exemption policies and define policy for mobile traffic. Introduces pre-populated exemption list of known mobile apps with SSL/TLS Interception incompatibilities, including bypassing mobile traffic known to break during intercepting because of certificate
pinning. (For any other apps that are not part of default mobile bypass, use the SSL policy editor to individually bypass them).

http://cloudwebsecurity.att.com/docs/sol/Solutions/ManagePolicy/SSL/ssl-policy.htm

- OCSP Toggle.

Enable/Disable OCSP Validation for server certificate revocation during SSL/TLS Interception.

Note: This option is disabled by default unless your account is provisioned for Universal Policy Enforcement (UPE). You must perform OCSP policy changes in the on-premises appliance policies.

http://cloudwebsecurity.att.com/docs/sol/Solutions/ManagePolicy/SSL/ssl-policy.htm


A viable method when an app-based solution is required rather than an agent installation, the CCD-WSS integration protects Windows 10/10S devices, enables comprehensive web security, ensures that users cannot access any malicious websites, and enforces already defined web use policies.

- Always connected VPN with full traffic redirection to the Web Security Service for web security, privacy and policy enforcement.
- VPN bypass based on IP addresses for personal traffic, such as video, music streaming, etc.
- SSL decryption support to benefit from greater network protections.
- Location awareness with active/passive mode.

The Symantec Cyber Defense Manager (CDM) console with enabled CCD provides a new WSS product switcher. If you’re an existing WSS user, the new product switcher accesses the WSS console; otherwise, it directs you to the WSS product page that has more information.

Note: This feature is currently in Early Access status. Symantec invites you to read the feature documentation before attempting configuration. If you experience any challenges, AT&T Technical Support is readily available to help you ensure a successful integration. (Find support contact details in the Help menu of the Cloud Web Security Service portal)


- Hosted Reporting—Direct Log Uploads.

This method uploads the ProxySG or Advanced Secure Gateway (ASG) appliance access logs directly to the Cloud Web Security Service, which negates having to deploy an intermediary staging server.


- Support for ChromeOS.
If your organization manages Chromebooks and other devices on the Google Approved Chrome Devices list, you can use the Google Admin Console to deploy the necessary Cloud Web Security Service proxy settings to each of your devices.

http://cloudwebsecurity.att.com/docs/sol/connectivity/endpoint/chromebook/conn-chromeOS.htm

- Web Security Service Help System redesign. Most connection-related topics have new best practices and are access with new URLs. See "WSS Help System Update Log" on page 37.
- "Recent Resolved Issues" on page 14

WSS Service Update MAR.08.2019

- Support for Universal Policy Enforcement (UPE) with Web Isolation.
  Use Symantec Management Center to manage Web Isolation criteria.
  http://cloudwebsecurity.att.com/docs/sol/Solutions/ManageMalware/about-upe-webiso.htm
- "Recent Resolved Issues" on page 14

WSS Service Update NOV.16.2018

- CASB Gatelet Integration
  The Cloud Web Security Service is now an integrated platform for Content Filtering, Threat Protection, DLP, and CASB deep-controls on cloud applications. After completing the one-time Cloud Web Security Service-to-CloudSOC integration, you can apply a combined policy enforcement to both platforms based on their respective configurations for all enabled Gatelets. No add-on license is required.
  http://cloudwebsecurity.att.com/docs/sol/Solutions/ManageWebApps/CASB/about-casb.htm
- Self-Manage Certificates
  By default, when intercepting and decrypting SSL traffic that traverses the Cloud Web Security Service, a self-signed Symantec certificate is used. To use your own AWS CloudHSM-hosted certificates with the Cloud Web Security Service, you can obtain the Self Managed Certificate add-on license.
  http://cloudwebsecurity.att.com/docs/sol/Solutions/ManagePolicy/SSL/Integrate_HSM.htm
- Apple iOS Mobile Device Service
  iOS device protection is now provided by SEP Mobile.
- Chromebook Roaming Captive Portal Plugin
  Temporarily unavailable.
- New Access Log Field
  r-supplier-country
WSS Service Update OCT.12.2018

- **WSS-SEP—Logged-In User Identification**
  
  A new integration token Symantec Endpoint Protection (SEP) clients use to send logged-in credentials to the Cloud Web Security Service. This *seamless identification* means employees do not have to re-login again when accessing internet through Captive/Roaming Captive Portal. This allows for per-user policy to be applied to traffic and also provides risk client context to the Cloud Web Security Service for logging and reporting.

- **SAML Authentication—Identified Provider Integration Services**
  
  For supported SAML Identity Providers (IdPs), configure SCIM to manage user and groups within your existing IdP and automate synchronization with the Cloud Web Security Service to populate users and groups. Requires SCIM 2.0. Currently, Azure is the only supported vendor.

- **Policy Editor**
  
  Fully redesigned Content Filtering, Threat Protection, and Web Isolation policy editors featuring simplified rule creation as well as logical combinations (for example: AND, OR).

- **Risk Level-based Threat Protection Policy**
  
  Accounts with the Advanced Web Security with Risk Controls and Web Applications add-on license have access to Symantec Global Intelligence Network Threat Risk Levels for dynamic risk score-based policies.

- **Geolocations**
  
  Accounts with the Advanced Web Security with Risk Controls and Web Applications add-on license can countries in the *Sources* and *Destinations* constructs.

- **Updated Ciphers**
  
  - As part of regular security updates for the Cloud Web Security Service 6.10.4.1 release, the following additional cipher support will be enabled:
    
    ecdhe-rsa-aes256-sha384
    ecdhe-rsa-aes128-sha256
ecdhe-rsa-aes256-gcm-sha384
ecdhe-rsa-aes256-gcm-sha256
ecdhe-rsa-aes128-sha
ecdhe-rsa-aes256-sha
aes128-gcm-sha256
aes256-gcm-sha384
dhe-rsa-aes128-gcm-sha256
dhe-rsa-aes256-gcm-sha384

Additionally, long-outdated ciphers will be fully disabled (currently deprecated):

des-cbc3-sha
rc4-sha
rc4-md5
des-cbc-sha

This change is not expected to have customer impact. All modern applications negotiate to the strongest available ciphers. For applications older than 2014, validate its supported ciphers.

- "Recent Resolved Issues" on page 14
- "Recent Unified Agent Resolved Issues" on page 29

WSS Service Update SEP.07.2018

This release did not introduce any new features.

- "Recent Resolved Issues" on page 14
- "WSS Help System Update Log" on page 37

WSS Feature Update JUN.15.2018

- **JUN.15.2018**—New Access Method: SD-WAN.

SD-WAN is a new supported Access Method. The initial integrated Cloud Web Security Service solution comprises of the Symantec SD Cloud Connector Edge device and the Orchestrator management portal.

- The initial version does not provide support for virtual machine Edge versions or technology related to Gateways or AWS Edge models. The Symantec Orchestrator online help system might contain references to these subjects.


- "Recent Resolved Issues" on page 14
- "Recent Unified Agent Resolved Issues" on page 29
WSS Service Update MAY.22.2018

- PAC File Management System (PFMS)—A complete redesign of the Explicit Proxy/PAC file distribution method. You can now create multiple PAC files, each with unique bypass lists, and assign them to locations. Furthermore, you can use a dedicated PAC file and integrate Symantec Endpoint Protection (SEP) with the Cloud Web Security Service.
  

- Threat Isolation—Remote web sessions execution that prevents malware from reaching your network and devices. Requires an add-on subscription.
  
  [http://cloudwebsecurity.att.com/docs/Solutions/ManageMalware/about_threatiso_co.htm](http://cloudwebsecurity.att.com/docs/Solutions/ManageMalware/about_threatiso_co.htm)

- Enable Malware Analysis Advanced Service for Universal Policy Enforcement—If employing Universal Policy Enforcement (UPE), you can configure notifications for the Malware Analysis Advance Service (MAAS).

- "Recent Resolved Issues" on page 14

WSS Service Update MAR.13.2018

This release did not introduce any new features.

- "Recent Resolved Issues" on page 14
- "WSS Help System Update Log" on page 37

WSS Service Update FEB.28.2018

- Symantec WSS (Security Web.Cloud) to AT&T Cloud Web Security Service migration.

- Roaming Captive Portal—Used for Explicit Proxy access from unknown locations is now 24 hours between challenges (up from 60 minutes).

- Symantec DLP Infrastructure—Changes to (secure) ICAP from rest.

- Universal Policy Enforcement (UPE)—Allows you to enable Symantec Cloud DLP.

- For the Firewall/VPN Access Method, the Cloud Web Security Service now supports IKEv2 protocol from gateway devices. If you are experienced with firewall devices, you can test configurations. However, Symantec did not test specific vendor devices. Therefore, the documented procedures to configure firewall devices do not contain this option. Upon successful configuration validation, the documentation will be amended.

- "Recent Resolved Issues" on page 14
Recent Resolved Issues

This section describes the most recent AT&T Cloud Web Security Service user-visible resolved issues.

Security Advisories

Resolved: SAML Authentication Bypass


JUL.26.2019

- POST requests made through SAML were not authenticated.
  
  ISSUE: Example, where in a G3 policy blocked access to certain categories, such as Social Networking, but allowed access to those sites for certain users. However the allowed users were not actually allowed because the WSS did not authenticate the POST request.

  (CP-450)

- Unable to use Google Analytics when Safe Search is enabled.
  
  ISSUE: There was a certain domain that Google made requests to in Google Analytics that was not exempted from SafeSearch, which caused Google Analytics to not work properly.

  (CP-1335)

- Unified Agent: Groups of interest disappeared.
  
  ISSUE: Groups of interest sporadically disappeared, causing users to get randomly blocked by policy.

  (SG-9837)

- x-exception-id set to “threat_protection_denied” (instead of the category name).
  
  ISSUE: Exception IDs were renamed such that they all included the suffix denied in them.

  (CP-1507)

APR.26.2019

- Auth Connector response.
  
  ISSUE: If a Cloud Web Security Service tenant has authentication enabled and referenced groups in policy, there was a delay of for all web requests of 30 seconds when the Auth Connector became disconnected. The WSS was waiting 30 seconds for a response from the disconnected Auth Connector, and then timed out. That timeout has been significantly
lowered.

(DP-373)

- **IPsec: WiFi calls failed.**

  **ISSUE:** With IPsec over IPsec, WiFi calling from Android and iPhones failed.

  (DP-300)

- **DLP/CP-Link.**

  **ISSUE:** A large amount of packets were dropped.

  (DP-314)

- **SEP with Seamless Authentication.**

  **ISSUE:** After expired sessions, the Cloud Web Security Service returned a 401 error to SEP clients instead of sending a 407 to prompt re-authentication.

  (SG-8839)

- **Explicit Over IPsec/SAML.**

  **ISSUE:** In a deployment with Explicit Over IPsec (Trans-Proxy) and SAML authentication, applying Policy updates reset user SAML sessions.

  (SG-5171)

- **Referers with internal hostnames causes delays because risk score CPL triggered a DNS lookup.**

  **ISSUE:** Requests for websites took too long because the risk score policy had issues attempting to analyze internal hostnames.

  (CP-1209)

- **Google Drive and Safe Search.**

  **ISSUE:** Videos hosted on Google Drive failed to play when Safe Search policy is enabled.

  (CP-1195)

**MAR.08.2019**

- **SEP/Seamless Identification: Changing locations causes session error.**

  **ISSUE:** When a SEP client with Seamless Identification changed locations (the connected to one data center, the relocated or there was failover to another asset), the client received a session error: The specified Client-ID Agent session does not exist.

  (WSU-245)

- **SEP/Seamless Identification: Clients randomly failed while browsing to different websites.**

  **ISSUE:** SEP clients with Seamless Identification randomly failed when browsing websites. The client received the
following error:

Access Denied
Your credentials could not be authenticated
"Credentials are missing"

(WSU-167)

- Video hosted on Google Drive failed to play when Safe Search policy is enabled.

  ISSUE: With Safe Search enabled, clients could not play video files stored on a Google Drive. Other content was accessible.

  (WSU-101)

NOV.15.2018

- Policy did not display the most recent changes.

  ISSUE: An issue with WSS assets prevented the portal from displaying recent changes applied to policies.

  (B#264003, 263948)

- Reporting Role—Portal froze.

  ISSUE: When a portal user was created in a Reporter Role and it had an associated filter to not be allowed to view user data, the portal locked up after log in.

  (B#261725)

- OCSP error.

  ISSUE: Accessing websites with certificates signed by TWCA might have resulted in an OCSP error because of a trust package defect.

  (B#245732)

- Malware Licenses: Protocol Detection was not disabled.

  ISSUE: With SSL Interception enabled and either of the malware licenses activated (MAAS, MASS), access to certain sites caused certificate errors.

  (B#266770)

OCT.12.2018

- Incorrect category on exception pages

  ISSUE: Exception pages when a user was blocked access displayed incorrect category names.

  (B#264264)

- Reviewer Role—Could not view location policies.

  ISSUE: Users in the Reviewer Role could view locations but could not view location-based policies in the Authentication
Rule Editor.

(B#261701)

- Some custom reports failed to email.
  
  ISSUE: The WSS failed to email custom reports.

(B#261738)

- Executable policy blocked some pages.
  
  ISSUE: File Type policy that blocked executables blocked websites that had .app in their URLs.

(B#243940, 243940)

- speedtest.net changed to WebSockets.
  
  ISSUE: The website speedtest.net now uses WebSockets, which caused a policy issue.

(B#260710)

- Report with Chinese or Japanese characters.
  
  ISSUE: Reports with Chinese or Japanese characters contained corrupted characters when the report was generated in PDF or CSV formats.

(B#242122)

- Incorrect colors in PDF reports.
  
  ISSUE: PDF reports with stacked bar or stacked column charts displayed incorrect colors in the chart legend when there were more than ten items on the chart.

(B#258732)

- Portal allows contains filter on subnet, but report builder did not support it.
  
  ISSUE: The report builder now supports contains or does not contains filter for subnets.

(B#260038)

- Overlapping row names in reports.
  
  ISSUE: Recent reporting format changes caused some row names to overlap.

(B#261698)

- Weekly reports with area charts in PDFs.
  
  ISSUE: The portal displayed weekly-generated reports properly, but PDF versions had the charts outside of the date ranges.

(B#261992)
■ Scheduled reports could not be modified.
   ISSUE: Reporting Users could not modify reports that are already scheduled.
   (B#262519)

■ Log retention portal issue.
   ISSUE: The Change Log Retention slider on the Service > Reporting > Log Controls page: Clicking Save displays a dialog, which was not properly displayed (reported in IE).
   (B#262804)

■ Reporting logged time out of order.
   ISSUE: Log lines had Ascending hours but Descending minutes.
   (B#262789)

SEP. 07. 2018

■ Reports displayed Total Bytes as 0.
   ISSUE: Reports displayed Total Bytes as 0.
   (B#262497)

■ Malware Analysis: Heuristics file denied.
   ISSUE: The Cloud Web Security Service denied transactions with an error stating that the download was a broken executable.
   (B#257505)

MAY. 22. 2018

■ Interrupted file downloads.
   ISSUE: When files larger than 3-4MB in size were downloaded through the Unified Agent, the file was interrupted. Some browsers allowed you to resume the download; however, most of the time you could not complete the file download.
   (B#242121, 257576)

■ PDF Report Export: Different graph.
   ISSUE: Generated PDF reports displayed incorrect graph and legend colors versus the portal display versions.
   (B#242121, 257576)

■ Audit Log: policy rule issue.
   ISSUE: The audit log contained erroneous policy rule information, such as ...created and the new Policy Rule is ???[ID=####].
   (B#256042)
- Non-responsive reporting searches.
  **ISSUE:** The portal would not execute searches for terms when entered the search bar on reports.
  *(B#255122)*

- Scheduling reports broken if report frequency is weekly and monthly.
  **ISSUE:** Scheduler failed to save the day when custom schedule times were set to run on a specified day on a weekly or monthly basis.
  *(B#255123)*

- Incorrect Date Filter and report data.
  **ISSUE:** After setting a **Reporter Filter Date** to **Previous 1 Week**, the report provided eight days of data.
  *(B#254581)*

- Subnet Filter did not function.
  **ISSUE:** Attempting to set the **Subnet** criteria in a filter resulted in an **Invalid IP notation** error.
  *(B#253749)*

- Emailed reports did not scroll.
  **ISSUE:** Scheduled and email reports did not contain a scroll bar.
  *(B#254765)*

- Cert-based: Time-based policy did not match with local time.
  **ISSUE:** In a Certificate-Based firewall deployment, policies based on time did not match actual local time.
  *(B#254409)*

- Japanese language in Chrome: Duplicated time zone.
  **ISSUE:** The **Add Criteria** option in **Filtering** contained duplicate time zone values.
  *(B#253854)*

- Browser error for some reports.
  **ISSUE:** Running resource-intensive reports caused a Chrome browser error message.
  *(B#254336)*

- Error when integrating CASB.
  **ISSUE:** After integrating the CASB license, the portal displayed an error regarding how many previous months were available for tracking.
  *(B#254977)*
UPE: Safe Search caused installation error.

**ISSUE:** Installation failed when the on-premises ProxySG appliance has Safe Search enabled and you attempted to push the policy through Universal Policy Enforcement (UPE).

(B#252021)

Object Library: Sorting did not function.

**ISSUE:** Attempting to sort in the Object Edit dialog worked the first time, but remained unresponsive if tried again.

(B#248557)

Object Library: Sorting/Ascending columns did not function.

**ISSUE:** Attempting to click the column sorting toggle in the various Object Library columns did not work.

(B#253749)

User-Defined URL Objects.

**ISSUE:** The portal did not display an error if a user entered invalid characters when defined custom URLs in the Object Library.

(B#249374)

Admin Users: Could not scroll.

**ISSUE:** The portal did not provide a scrolling mechanism for Account Maintenance > Users. If you had a large number of Admins, you had to search.

(B#255352)

Time schedule not consistently applied or evaluated.

**ISSUE:** This issue resulted in two anomalies.

- Time restrictions started and ended one hour later.
- If there were multiple time restrictions in place for the day, the time restrictions matched out of bounds

(B#251440)

Mar.13.2018

SAML Certificate Warning.

**ISSUE:** Tunneled SSL requests should have been bypassed from authentication; however, users received certificate warning when browsing to HTTPS sites.

(B#255708)

Certificate-based VPN.

**ISSUE:** Intermittent connections with certificate-based Firewall/VPN Access Method.
When DLP is enabled, a URL was rewritten causing a DNS failure.

**ISSUE:** Universal Policy Enforcement with DLP enabled. ICAP request scanners that responded with the schema as part of the URL were affected by proxy forward tunnel termination handling.

IPsec location indicated disconnected status.

**ISSUE:** In the portal, an IPsec location displayed the disconnected status despite the active tunnel.

Feb.28.2018

Could not remove reporting alerts.

**ISSUE:** Corrected an issue that prevented you enabling, disabling, or deleting reporting alerts from the portal.

NSL onboarding.

**ISSUE:** Service providers could not onboard their customers through NSL.

SAML requests.

**ISSUE:** SAML did not authenticate HTTP methods that were not GETs or POSTs.

Pulse Connect Secure Server and SAML.

**ISSUE:** SAML authentication failed if Pulse Connect Secure Server is used as the IDP.

IE 11/Reporter Filter.

**ISSUE:** Internet Explorer 11: Was unable to set the value for *Report Filter Criteria—Hour of Day*—when reports were run.
Currently Known Issues

AT&T is aware of the following issues in the Cloud Web Security Service.

Android Device

- **Cannot download O365 apps.**
  
  **ISSUE:** Attempting to download Office365 apps, such as Outlook, results in a 491 error. Disabling SSL Interception for the tenant is a workaround.
  
  (B#240588)

- **Blocked Android device.**
  
  **ISSUE:** If you select the Block action, the portal displays the Connection Status as Disconnecting; the app on the Android device indicates it is connected. The device is blocked, but the device is not receiving the status.
  
  (B#240588)

Authentication

- **Roaming Captive Portal and Coaching.**
  
  **ISSUE:** With Roaming Captive Portal enabled, Firefox and Internet Explorer browser return certificate errors (Secure Connection Failed) when a Coaching or possible Password Override policy is triggered. Chrome authenticates, but then also returns an error. Users can reload the page and receive the content.
  
  (B#265322)

Block Notification Service

- **Using 'redirect' option in Content Filtering breaks BNS.**
  
  **ISSUE:** BNS continuous pop-up occurs when there are lot of files to be synced with OneDrive.
  
  Workaround—Prevent OneDrive process from auto-starting at Windows log in.
  
  OneDrive Settings > General; clear the Start OneDrive automatically when I sign in to Windows option.
  
  WSSP-1003

- **Using 'redirect' option in Content Filtering breaks BNS.**
  
  **ISSUE:** The WSS Agent fails to connect when a Content Filtering policy contains a URL redirect rule in Group B. Any tenant policy that redirects BNS domain requests (symcwss.cloud) breaks the BNS functionality for those requests. This is not expected to be an issue unless tenant policy uses a wildcard character that inadvertently captures requests to the
CASB

- Formats-based policies.
  
  **ISSUE:** When saving files to SharePoint, One Drive from Word, PowerPoint, Excel thick clients or online versions, CASB Content Inspection/DLP for risks and file formats-based policies do not work.

  *(Wssp-1004)*

Common Policy

- Default Block Categories not copying to on-premises proxy.
  
  **ISSUE:** Following an update, not all blocked category policies correctly propagated.

  *(B#238438)*

DLP

- CASB + DLP—Expected Block action does not occur.
  
  **Cause**—A DLP Policy that belongs to the Policy Group for the REST detectors but does not contain a Response Rule is modified, which causes a mis-match between DLP and CASB.

  **Workarounds**
  
  - Update (save without editing) any DLP Policy with a Response Rule for the REST detector Policy Group.
  - This issue is resolved is Enforce v15.5] and will be resolved in 15.1MP2.

  *(WSSP-340)*

Hybrid

- SSL interception mismatch.
  
  **ISSUE:** A hybrid policy downloads to an on-premise proxy, which does not have SSL interception enabled. The hybrid policy matches a DENY rule for ssl://traffic, yet the transaction is allowed.

  *(B#225136)*

IPsec
- **IKEv2 tunnels.**
  
  **ISSUE:** Child SAs (phase 2 tunnels) from IKEv2 FQDN sites expire one hour after the time of creation.
  
  **WORKAROUND:** To ensure that there is no loss of connectivity, configure the firewalls to have child SA (or phase 2) lifetime of less than an hour to ensure that a new SA is in place before the old SA expires.
  
  (DP-310)

**Office 365**

- **SEP/Seamless ID and Explicit Proxy—Direct-to-net required.**
  
  **ISSUE:** To be compatible with the SEP with Seamless Authentication solution in Explicit Proxy deployments, the Office 365 client requires a Direct-to-Net route to allow connection to some servers without going through the Cloud Web Security Service.
  
  (B#263977)
  
  - **SEP/Seamless ID and Explicit Proxy—Outlook profile creations.**
    
    **ISSUE:** With the SEP with Seamless Identification solution, Outlook profile creations fail. Existing Outlook profiles function normally.
    
    (B#263982)

**Policy**

- **Incorrect Verdict in policy trace for non-intercepted HTTPS.**
  
  **ISSUE:** This issue is visual-only in nature and has no functional impact. When observing a policy trace, there might be some transactions with messaging that they were SSL intercepted, yet they were not.
  
  (SG-12397)
  
  - **Dropbox not supported.**
    
    **ISSUE:** Because of some required SSL interception intricacies, the Cloud Web Security Service does not support policy enforcement, such as file uploading, for the Dropbox application.
    
    **WORKAROUND:** Navigate to Solutions mode > Content Filtering > Policy and click Activate.
    
    (B#214531)
  
  - **Google SafeSearch policy causes images and other elements of Google’s search results page not to display.**
    
    **ISSUE:** In some instances, Google searches and displays a specific website, but with some elements (such as images or Google maps) missing. After refreshing the page, the browser displays everything correctly.
    
    (B#222782)
  
  - **PDF file is blocked as an Executable because of Content-Type.**
    
    **ISSUE:** Cloud Web Security Service policy blocks PDFs served with Content-Type: application/octet-stream
because it is viewed as an executable.

(B#238911)

- HTTPS policy evaluation.

**ISSUE:** Following a Cloud Web Security Service datacenter infrastructure upgrade, some accounts noticed some content that was supposed to be blocked by a policy rule was allowed through. This is because of a policy evaluation change and is under investigation.

(B#240186, 240361)

- HTTPS policy evaluation.

**ISSUE:** Following a Cloud Web Security Service datacenter infrastructure upgrade, some accounts noticed some content that was supposed to be blocked by a policy rule was allowed through. This is because of a policy evaluation change and is under investigation.

(B#240186, 240361)

**Reporting**

- **Portal displays Slice instead of No Group.**

**ISSUE:** When you create a new report and select *More > Group* from the *Category* drop-down, the generated report labels the *No Group* section as *Slice*.

(B#199257)

- **Scheduled report for previous months shows the previous 30 days rather than the previous month’s data.**

**ISSUE:** Also, the report contains dates of this month and the date range is only 15 days. The Report should contain only the dates and information of the previous month.

(B#179098)

**SAML**

- **Misleading SAML error.**

**ISSUE:** The following SAML error is incorrect and not indicative of the root problem.

Account Restricted, you cannot log in, because your account is locked out

The Service Provider (saml.threatpulse.net) and the proxy authentication realm exceptions should provide meaningful information, such as:

- The assertion was signed by an unknown CA.
- The date/time on the assertion did not match the time on the data pod.

(B#215445)
SEP Client

- SEP with Seamless Identification.

**ISSUE:** When a SEP client with Seamless Identification changes locations, it retains policy but coaching/password override exception pages do not correctly display.

*(SG-10573)*
Limitations

Add your text here.

- **Plus (+) signs in report names (not Firefox).**
  
  **ISSUE:** The prompt to open or save Japanese-language reports contains plus (+) signs between words in report names.

  *(B#205510)*

- **Some CRL URLs are blocked.**
  
  **ISSUE:** Some configured policy might block CRL URLs.

  *(B#180357, SR 2-479877708)*

- **Java error when saving a user list from Users In Reporting.**
  
  **ISSUE:** In the Advanced Policy editor, attempting to create a User List in an existing rule and use it in the rule generates a Java-based error (Java version 7, update 11).

  **WORKAROUND:** Use users instead of user lists.

  *(B#184432, SR 2-538925851)*

- **Multiple domains are unreachable through iOS8.1.3 VPN + 3G/4G.**
  
  **ISSUE:** iPhone with the following configuration only: (iOS8.1.3 + 4G/3G + VPN profile). The browser cannot reach multiple domains.

  *(B#214945)*
Compatibility Index

Configuring and administering the AT&T Cloud Web Security Service requires using third-party technologies. This page provides an index to those supported technologies.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Agent</td>
<td>&quot;Recent Unified Agent Resolved Issues&quot; on page 29</td>
</tr>
<tr>
<td>I will install the Unified Agent for remote users. What are the desktop</td>
<td>&quot;Desktop Anti-Virus Compatibility&quot; on page 33</td>
</tr>
<tr>
<td>anti-virus (AV) compatibilities?</td>
<td></td>
</tr>
<tr>
<td>What browsers can I use to access the Cloud Web Security Service?</td>
<td>&quot;Supported Browsers&quot; on page 34</td>
</tr>
<tr>
<td>I will use the Proxy Forwarding Access Method to route web traffic to the</td>
<td>&quot;Supported Proxy Devices&quot; on page 35</td>
</tr>
<tr>
<td>Cloud Web Security Service. What proxy appliances and operating systems</td>
<td></td>
</tr>
<tr>
<td>are supported?</td>
<td></td>
</tr>
<tr>
<td>I want to employ SAML authentication.</td>
<td>&quot;Supported SAML IDPs&quot; on page 36</td>
</tr>
</tbody>
</table>
Recent Unified Agent Resolved Issues

This topic lists the recent Unified Agent versions and the resolved issues for each version.

VPN Client Compatibility

The WSS Agent/Unified Agent cannot compete with multiple VPN clients, such as Cisco AnyConnect, that might be installed on client systems. You can configure full or split tunnel with additional configurations.

- **Full Tunnel**—This is possible if the VPN server's egress IP address is configured as an IPSec Location in the Cloud Web Security Service (Service mode > Network > Locations). This enables the Unified Agent to enter Passive mode when on the Location network.
- **Split Tunnel**—White-list the IP address of the VPN server to prevent connection flapping.

Release Date: JUN.13.2019

Supported Client Operating Systems:

- Windows 7 32/64 bit (excluding home editions)
- Windows 8.x 32/64 bit (excluding home editions)
- Windows 10 32/64 bit (excluding home editions)
- Apple OS X 10.10+

Resolved Issues:

- IPv6 traffic was interrupted when the agent is in passive or fail open modes.
- Resolved a macOS kernel panic triggered during upgrade.
- Resolved issue that set Username format back to its default value.
- Resolved compatibility issue with third party VPNs and UA passive mode.
- Resolved delay in connecting tunnel on networks with non-standard PAC.
- Resolved an issue on macOS where the operating system was prevented from displaying the captive portal login.

Release Date: OCT.22.2018

Supported Client Operating Systems:

- Windows 7 32/64 bit (excluding home editions)
- Windows 8.x 32/64 bit (excluding home editions)
Resolved Issues:

- Resolved an issue where UA does not roll over to next site in CTC connect list on failure.
- Resolved an issue where UA failed to fall back to DNS when it received an HTTP 500 error from CTC.
- Resolved a notifier crash on macOS.
  - On failure to connect, the Unified Agent did not roll over to next site in the CTC connect list.
  - The Unified Agent failed to fall back to DNS when it received an HTTP 500 error from the CTC.
  - Resolved a notifier crash on MacOS.

Release Date: JUN. 15. 2018

Supported Client Operating Systems:

- Windows 10 32/64 bit (excluding home editions)
- Apple OS X 10.10+

Resolved Issues:

- Unified Agent displayed high CPU utilization on High Sierra.
- The OS X agent did not attempt to connect through UDP.
- Resolved a compatibility issue with the Cisco Umbrella client.
- Resolved an issue related to a race condition during network change events.
- Resolved an issue related to a race condition during network change events.
- Resolved a issue might have occurred when Unified Agent was shutdown unexpectedly by an external source.
- Updated ZMQ to address an issue in the ZMQ library.
- Resolved an issue where delays contacting the CTC prevented the agent from entering passive mode.
- Resolved an issue where Unified Agent would prematurely enter failure mode in specific captive network situations.

Release Date: 2/2018

Supported Client Operating Systems:
Windows 7 32/64 bit (excluding home editions)
Windows 8.x 32/64 bit (excluding home editions)
Windows 10 32/64 bit (excluding home editions)
Apple OS X (Mavericks (version 10.9.x))
Apple OS X (Yosemite (version 10.10.x))
Apple OS X (High Sierra (version 10.13.x))

Features
- Added adaptive protocol support to improve Unified Agent performance.
- The agent evaluates network conditions to attempt a UDP connection; if the conditions are not met, the connection reverts to TCP.
- Added support for Mac OS X: High Sierra (10.13).

Resolved Issues:
- The Unified Agent failed to reconnect from the passive state after disconnecting from a third-party VPN.
- Resolved a service crash related to situations where a network interface might not be available when the service starts.
- Unified Agent 4.8.1 on OS X did not honor the bypassed domains from the portal.
- Unified Agent did not connect to the service when connecting over a USB data card connection.
- Unified Agent stopped attempting to connect to the service before the network became available. For example, when a NAC scan occurs on start up.
- Unified Agent woke systems from sleep mode.
- Unified Agent prevented internet access after disconnecting from one docking station and connecting to another.
- Unified Agent would not establish a user tunnel on systems using an OpenOTP solution.

Release Date: 10/2017

Supported Client Operating Systems:
- Windows 7 32/64 bit (excluding home editions)
- Windows 8.x 32/64 bit (excluding home editions)
- Windows 10 32/64 bit (excluding home editions)
- Apple OS X (Mavericks (version 10.9.x))
- Apple OS X (Yosemite (version 10.10.x))
- Apple OS X (High Sierra (version 10.13.x))

Features
Added adaptive protocol support to improve Unified Agent performance.

- The agent evaluates network conditions to attempt a UDP connection; if the conditions are not met, the connection reverts to TCP.

- Added support for Mac OS X: High Sierra (10.13).

Resolved Issues:

- The Unified Agent failed to reconnect from the passive state after disconnecting from a third-party VPN.

- Resolved a service crash related to situations where a network interface might not be available when the service starts.

- Unified Agent 4.8.1 on OS X did not honor the bypassed domains from the portal.

- Unified Agent did not connect to the service when connecting over a USB data card connection.

- Unified Agent stopped attempting to connect to the service before the network became available. For example, when a NAC scan occurs on start up.

- Unified Agent woke systems from sleep mode.

- Unified Agent prevented internet access after disconnecting from one docking station and connecting to another.

- Unified Agent would not establish a user tunnel on systems using an OpenOTP solution.
Desktop Anti-Virus Compatibility

If you plan to install the Unified Agent application onto employee systems to support remote access to the AT&T Cloud Web Security Service, some desktop anti-virus (AV) applications might cause various results. The following list describes which AV applications were tested to work by AT&T; additional behavior noted where applicable. Other vendor products might or might not function with the product. As more are tested, they will be listed here. AT&T recommends testing non-supported vendors during a trial on a non-production basis.

**Tip:** Trend Micro is a known vendor product that is *not* officially compatible. However, the following Knowledge Base article discusses a possible workaround. [KB Link]

**AVG Internet Security 2012**

Windows XP; 7 (32-bit and 64-bit):

After the client system reboot, the client attempts to connect to the cloud service. The AVG Firewall asks for confirmation to allow Cloud Web Security Service permission to connect to the Internet. Grant permission; the client successfully connects to the cloud service, establishes tunnels, and applies policies.

**Kaspersky Internet Security**

The Unified Agent must be configured as a trusted application.

**McAfee Total Protection 2012**

Windows XP; Windows 7 (32-bit and 64-bit):

Following the client system reboot, tunnels connect and policies applied with no further issues reported.

**Sophos**

Cannot install Unified Agent on Windows 8 after Sophos Antivirus has been uninstalled.

**Symantec Endpoint Protection: 11.0.6005.562**

Update to the latest definitions.

Windows XP; Windows 7 (32-bit and 64-bit):

Following the client system reboot, tunnels connect and policies applied with no further issues reported.

**ZoneAlarm**

Update to the latest databases.

The Unified Agent must be configured as a trusted application.
Supported Browsers

Use one of the following browsers to access the AT&T Cloud Web Security Service interface.

- Microsoft Internet Explorer 9.x, 10.x, 11.x
- Mozilla Firefox 51.x-
- Google Chrome 56.x-
- Apple Safari 9

Newer versions should function correctly, but might not have been officially qualified by AT&T.

Furthermore, browsers requires Javascript and cookie support.
Supported Proxy Devices

The AT&T Cloud Web Security Service Proxy Forward Access Method requires you to configure the network egress proxy device to forward web-bound requests to the service. AT&T tested the following proxies.

AT&T

ProxySG appliances (all are Proxy Editions)

- SG210
- SG810-(5-25 only)
- SG300
- SG900
- SG510
- SG9000
- SG600

SGOS Versions

- 6.5.x
- 6.7.x

Microsoft

- Internet Security and Acceleration (ISA)™ 2006 -- 32-bit
- Forefront Threat Management Gateway™ (TMG) -- 64-bit
Supported SAML IDPs

The AT&T Cloud Web Security Service supports Security Assertion Markup Language (SAML) authentication, which enables you to deploy the cloud solution and continue to use your current SAML deployment for Authentication.

**REQUIREMENT:** Only the Firewall/VPN and Explicit Proxy Access Methods with Captive Portal enabled support SAML integration.

Currently, AT&T tested and supports the following Identity Providers (IdPs).

- The Auth Connector—Instead of a third-party vendor SAML Identity Provider (IdP), the Auth Connector can function as the IdP.
- Active Directory Federation Services (AD FS) 2.0
  
  [http://portal.threatpulse.com/docs/am/AMDoc.htm#Deployment/Tasks/Auth/SAML/saml_3rdparty_sol.htm](http://portal.threatpulse.com/docs/am/AMDoc.htm#Deployment/Tasks/Auth/SAML/saml_3rdparty_sol.htm)
- Symantec VIP Access Manager
  
- Google G Suite
  
- Microsoft Azure
  
- Okta
  
- Ping
  

**Tip:** Other IdPs might work. When attempting to configure, verify that the assertion contains the signing certificate. Some IdP implementation do not by default.
WSS Help System Update Log

This topic lists updates to the AT&T Cloud Web Security Service Help System. Periodic documentation updates occur to inform you about enhances to existing features, address user feedback, clarify information, and improve overall quality. The Help System version displays at the bottom of each page. Click a date to view recent major updates and corrections.


Cloud Web Security Service Service Update—JUL.26.2019

- Left-Nav menus revised with more topic inclusion.

See "Recent Features" on page 7.

WebGuide Version—61/JUL.01.2019


- New ACLogon version—Resolves an issue where the backup Auth Connector was contacted only if the primary server is running.
  

- Corrected CLI command for testing Hosted Reporting direct-to-WSS uploading.

- Skype for Business—bypass hostnames and IP addresses best practices.


- SEP with Seamless Identification—Updated SEP client screenshot with newer version and removed one option.


- Full Access Log string added to reference topic.

  http://cloudwebsecurity.att.com/docs/sol/Solutions/Reference/accesslogformats-ref.htm

WebGuide Version—60/MAY.27.2019


- SAML Azure IdP—Removed Optional from Step 8.

  http://cloudwebsecurity.att.com/docs/sol/AccessMethods/auth/SAML/saml_azureIDP.htm

- Added domains to bypass authentication in all SAML IdP topics except for Symantec.
Connectivity: Additional technical requirements in VPN/IPsec topics. Certificate Authentication topic has link to reference configuration KB.


Cloud Web Security Service Documentation Refresh.

- New skin with expanded side navigation; revised styles.
- The Solutions WebGuide, which is called from help buttons within the Cloud Web Security Service portal, is now the Web Security Service Help System. This system includes all of the Cloud Web Security Service documentation content from the separate WebGuides—Release Notes; Access Methods/Connectivity; Hosted Reporting; and Solutions.
- This revision phase renovates the Cloud Web Security Service connectivity topics. These topics include new best practices.
- Notification of non-standard ports change.


**Tip:** If you have topic URLs bookmarked for easy access, be advised that these URLs have changed. Locate the content in the new system.


Cloud Web Security Service Version: 6.10.4.3 MAR.08.2019

Grammatical edits; help button on SAML page fixed.

- Updated IP address information for the PAC File Management System.
  

- Explicit Over IPsec (Trans-Proxy) IP address revisions.
  

- CASB-Web Isolation policy order refinement.
  

WebGuide Version—57/MAR.08.2019

Cloud Web Security Service Version: 6.10.4.3 MAR.08.2019

Grammatical edits.

Cloud Web Security Service Version: 6.10.4.2 NOV. 16.2018

Minor edits.

- Firewall wall rule added to–
- SAML Okta IdP topic now includes SCIM process.
  http://cloudwebsecurity.att.com/docs/am/AccessMethods/auth/SAML/saml_olktaIdP.htm
- Proxy Forwarding SGOS topic screenshot incorrectly contained port 443 instead of 8443.
- Incorrect UDP port number in the Required Ports and Protocols topic.
- Two-Factor Auth for admin portal access procedure.
  http://cloudwebsecurity.att.com/docs/sol/Solutions/Admin/NSL/sym_secure_login.htm


Cloud Web Security Service Version: 6.10.4.2 NOV. 16.2018

Trust Blue Coat site replaced by https://wss.status.symantec.com/ references changed.

Minor edits.

- CASB Limitation clarification.
- Explicit Proxy sample PAC file.
- SAML—Erroneous reference to Proxy Forwarding.
- Auth Connector—More details about the ACLogin App.

WebGuide Version—54/DEC.10.2018

Cloud Web Security Service Version: 6.10.4.2 NOV. 16.2018

Edits—Access Methods WebGuide

- Added authentication requirements to SEP-Mobile topics.
- Added authentication note to WSS-SEP with Seamless Identification topic.
Edits—Solutions WebGuide

- Issue added to Deploy a Self Managed Certificate for SSL Interception topic.
  
  http://cloudwebsecurity.att.com/docs/sol/Solutions/ManagePolicy/SSL/Integrate_HSM.htm


Edits—Access Methods WebGuide

- Fixed link to Microsoft article in SAML Azure IdP topic.

WebGuide Version—52/NOV.05.2018

Edits—Access Methods WebGuide

- Removed all reference tables to datacenter, egress, and authentication IP addresses. The reference topics now point to Knowledge Base articles, which are maintained by Cloud Web Security Service Operations.
- ClientLogonApp zip file now contains the .md5 and release note text file.
- Added Okta SAML IdP, which revises content in the previous PDF version.
- To avoid confusion regarding authentication, the WSS-SEP logged-in user solution renamed from Seamless Authentication to Seamless Identification.


Edits—Solutions WebGuide

- Added Active Content to the File Extensions reference topic.
  
  http://cloudwebsecurity.att.com/docs/sol/Solutions/Reference/advpol_filex10sions_ref.htm
- Added Access Log Field Reference topic.
  
  http://cloudwebsecurity.att.com/docs/sol/Solutions/Reference/accesslogformats-ref.htm

WebGuide Version—51/OCT.12.2018

Cloud Web Security Service Version: 6.10.4.1 OCT.12.2018
Edits—Access Methods WebGuide

- Edit to ProxySG/SGOS Forwarding Services.
- Minor Trans-Proxy edit.

Edits—Solutions WebGuide

- Office 365 Web Applications policy selections updated.

WebGuide Version—50/SEP.07.2018

Cloud Web Security Service Version: 6.10.3.2 SEP.07.2018

Edits—Access Methods WebGuide

- Edit to Local IP visibility per Access Method.
  - [http://cloudwebsecurity.att.com/docs/am/AccessMethods/Concepts/AuthDetail/about_authentication_co.htm](http://cloudwebsecurity.att.com/docs/am/AccessMethods/Concepts/AuthDetail/about_authentication_co.htm)
- Minor Trans-Proxy edit.

Edits—Solutions WebGuide

- Office 365 Web Applications policy selections updated.

WebGuide Version—49/AUG.27.2018

Cloud Web Security Service Version: 6.10.3.1 MAY.15.2018

Edits—Access Methods WebGuide

- SEP-WSS edits.
- Trans-Proxy conceptual, open ports, and configuration edits.
- Datacenter VIP updates.

Edits—Solutions WebGuide

- Added Default Policy categories to the Registration and Content Filtering Solution topics.
Edits—Access Methods WebGuide

- New ALogon download for the Auth Connector integrations for large enterprises with many domain controllers spread out across locations. See the Release Notes included with the download for a list of fixes.
- Datacenter VIP updates.
- Proxy Forwarding CPL template corrected.
- Revisions to the SD Cloud Connector topic, including the Orchestrator IP address.

Edits—Solutions WebGuide

- PAC File Management System—Minor revisions, including a note about bypass files limited 256 KB.
- (Web) Threat Isolation—Then you must exempt the private SfB/Lync URLs from Threat Isolation policy to prevent the SfB from becoming unresponsive.

Edits

- Threat Isolation—Added link to training video.
- Datacenter VIP updates.

Edits

- Remote Clients and Required Ports topics: corrected to client.threapulse.net for DNS fallback.
- Threat Isolation—Refined some language.
- Supplemental information that IKEv2 with FQDN and PSK supports NAT-T.
- Cert-based ASA topic—Revised the root cert step.
Edits

- Edits. See [New Features](#).

WebGuide Version—44/MAY.07.2018

Cloud Web Security Service Version: 6.10.2.6 Mar.13.2018

Edits

- SAML Federation topic—Clarified step for obtaining metadata.
- Clarified **Ignore Proxy Settings** definition for Unified Agents.
- Corrected:
  - Proxy Forwarding Policy template.
  - Broken Web Application Reference link.
  - Updated links on the Resource Portal.


Cloud Web Security Service Version: 6.10.2.6 Mar.13.2018

Edits

- Corrected erroneous authentication headers in the Proxy Forwarding sample policy.
- The PDF icon on the About Migrating From Symantec Web.cloud topic linked to the Unified Agent PDF.
- The TopNav menus did not drill-down past three levels.
- New SAML IDP support: Google G Suite.


Cloud Web Security Service Version: 6.10.2.5 Feb.28.2018

Edits

- General Edits.

WebGuide Version—41/FEB.12.2018

Cloud Web Security Service Version: 6.10.2.1 Nov.11.2017
Edits

- Broken links from Tiles and cross-references.

Access Methods WebGuide

- New SAML IDP: PingID
- Checkpoint topics: Added Trans-proxy step.
- Auth Connector: Previously stated that you can install on a Domain Controller or member server. For security reasons, this is now changed to member server only.
- Proxy Forwarding:
  - For Microsoft ISA/TMG topics: You must manually add the X-Forwarded-For header to the filter .ini file.
  - Updated the Proxy Forwarding CPL example template; enhanced with option to send authentication detail for local SSL intercept bypassed traffic.
- Reference: Supported Cipher Suites for the portal.