Web Security Service

Release Notes

Preview of Expected NOV.07.2020 Service Update

Symantec
A Division of Broadcom

Symantec Web Security Service: Release Notes

This Release Note version provides a preview of the next Web Security Service **update—currently expected November 07, 2020 (subject to delay). All contents in this document are subject to change (including additional information) before** Symantec **posts the final version when the release goes live. Do not widely redistribute this preliminary version.**

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

With extensive web application controls and detailed reporting features, IT administrators can use the 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 service releases

Contents

Recent Features

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

WSS Feature Update—Expected NOV.07.2020

- The WSS portal receives a major redesign.
  - Eliminates the **Service** and **Solutions** modes.
  - The paradigm moves from a Top Navigation and tab-based design to a Left Navigation and menu-based design.
  - All pages are now accessible from six menu icons on the left side of the portal:
    - **Dashboards**—High-level reports for base and add-on WSS products.
    - **Reports**—Report Center.
    - **Connectivity**—Landing page for traffic steering, bypassing traffic, and agent configurations.
    - **Identity**—Landing page for user and group identity and authentication.
    - **Policy**—Landing page for Contenting Filtering, Threat Protection, SSL, and other base and add-on product policy configurations.
    - **Account Configuration**—Landing page for WSS administrative tasks, including user management, product integrations, alerts, and data privacy controls.

  With a few exceptions, the contents of the portal pages have not changed. This new design is more intuitive to navigate portal pages. Click the following link to view a brief introduction video.

  https://www.youtube.com/watch?v=alqjx7TTr0E&feature=youtu.be
- A new version of WSS Agent. Upgrade to version 7, which provides critical fixes and enhanced features.
  - Operates in Single Tunnel Mode by default.
  - Support for Application Bypass—Bypass thick applications, which are often problematic in certain deployments.
  - More information about this version.

  "Recent WSS Agent Releases" on page 31
- Support for CASB-only mode; integration with CloudSOC without full WSS/secure web gateway functionality. WSS provides the traffic steering, but web application analysis is performed and managed in CloudSOC.
- WSS-SEP-NTR—Network Traffic Redirection option for SEP client deployments, which negates the PAC File requirement. This deployment embeds and deploys selective WSS Agent technology into SEP. This yields the benefits of the full Network Traffic Redirection (NTR) and captures non-proxy applications. You can select what is captured by the agent. This method is beneficial if SEP clients frequently change from one network to another. The tunnel method

provides heightened security by encrypting traffic between the endpoint and the data center. The SEP documentation provides more information, including required versions and availability.

- "Recently Resolved Issues" on page 10
- "Help System Update Log" on page 20

WSS Feature Update—AUG.28.2020

- This service updated does not introduce any new features.
- "Recently Resolved Issues" on page 10
- "Help System Update Log" on page 20
- "Recent WSS Agent Releases" on page 31

WSS Feature Update—APR.25.2020

- This update provides an improved back-end infrastructure for the reporting service. The infrastructure allows for future holistic reporting updates. This initial update provides the following.
    - Executive Report—Admins can run a comprehensive monthly PDF report that provides protection insights and threat summaries. The report is presented in an aesthetically-pleasing design, which is more consumable for executive-level readers and presentations.

      http://portal.threatpulse.com/docs/sol/Solutions/ManageReports/exec-report.htm
    - If your account is provisioned with the Cloud Firewall Service, you can view centralized CFS reports on a new dashboard.
    - If your account is provisioned with the Malware Analysis Advance Service (MAAS) license, new reports provide insight into cloud sandboxing detonation reports, including risk rating, file hashes, and file attributes.
- By the end of April, the SAML Identity Provider (IdP) for Admin Single Sign-On access to WSS portal accounts is switching from Norton Secure Login (NSL) to Okta Identity Provider. Any existing customers who federate with a custom IdP will receive emails regarding how to modify it to work with Broadcom accounts. Also refer to the following Broadcom KB article.

  https://knowledge.broadcom.com/external/article?articleId=188607
- See the "Help System Update Log" on page 20 for more changes.

WSS Feature Update—JAN.31.2019

- The Cloud Firewall Service (CFS) is now available for order. Help topics—

  http://portal.threatpulse.com/docs/sol/Solutions/CFS/cfs-about.htm
- "Help System Update Log" on page 20

WSS Service Update—DEC.06.2019

- SEP with Roaming SAML Support.

  When SEP clients are not connected through a fixed location, SEP securely transfers the logged-in user ID and device information to the cloud-based or on-premises SAML Identity Provider (IdP).

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/sepclient/conn-sep-si-roam.htm

- Proxy Analysis Controls

  Two traffic control toggles: Restrict traffic flowing to WSS to standard web protocols. In conjunction, you can limit traffic on the server side to standard ports.

  http://portal.threatpulse.com/docs/sol/Solutions/ManageMalware/malware_sol.htm

- Minimum Bytes sent to DLP Service

  By default, any request that is fewer than 4096 bytes is not sent to DLP. This is dependent on the `Content-Length` header existing in the request. If this header is not present, policy sends the request to DLP. If circumstances necessitate a need to send fewer than 4K bytes, you can work with Symantec Technical Support to lower the threshold for your account.

- This update includes infrastructure to support the upcoming release of WSS Cloud Firewall Service. When the CFS is ready for trial and sale, Symantec will send a separate release announcement with more details.

- Features related to WSS Agent.

  - WSSA 6.1 will be available from the portal during the week of December 9th.
  - Enhancements include CFS support; block IPv6 IP addresses.
  - When the agent is available on the portal, click the Release Note link next to the download to review all enhancements, fixes, and issues.

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/agent/conn-wssa-security.htm

- Coming Soon—SAML Signed Certificate.

  The option to sign all outbound `AuthnRequests` in a SAML deployment, which was pre-announced as a feature, is receiving further modifications. It will be available in a future update.

- "Recently Resolved Issues" on page 10

- "Help System Update Log" on page 20—Revised authentication architecture.

WSS Service Update—SEP.17.2019

- This service updated does not introduce any new features.

- "Recently Resolved Issues" on page 10

- "Help System Update Log" on page 20

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).

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/agent/conn-about-wssa.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 mass deletion, Symantec will not begin the deletion of 1-year-plus logs until one month after the date of this service update.

  The **Auditing** page also now allows you to filter up to one year (a change from the previously afforded two weeks) and search by object type.

  http://portal.threatpulse.com/docs/sol/Solutions/Admin/Account/adm_audit_ta.htm

- 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.

    http://portal.threatpulse.com/docs/sol/api/api-keys.htm

  - Automate audit log downloads through a REST API.

    http://portal.threatpulse.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.

  http://portal.threatpulse.com/docs/sol/auth/ac/auth-conn-about.htm

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

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

  http://portal.threatpulse.com/docs/sol/Solutions/Admin/privacy/privacy-xff.htm

- Force English Translation in Notifications

  You can force WSS 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, especially when 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, Symantec 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://portal.threatpulse.com/docs/sol/Solutions/Reference/accesslogformats-ref.htm

- New ACLogon version–Provides a critical fix for dropped VPN connections.

  http://portal.threatpulse.com/docs/sol/auth/ac/auth-conn-deploy.htm

- "Recently Resolved Issues" on page 10

Recently Resolved Issues

This section describes the most recent Symantec Web Security Service user-visible resolved issues.

Expected NOV.07.2020

- **Custom Response Pages.**

  ISSUE: When triggered, some response pages did not display a custom logo.

  (WSSPOR-3371, 3388)

- **Executive Reports.**

  ISSUE: Resolved an issue that prevented a dialog indicating report progress. Also resolved an issue where **Your Services/More Services Available** did not match what was provisioned.

  (WSSPOR-3263, 1576)

- **Partner Portal.**

  ISSUE: A saved branding in the Partner Portal did not become active.

  (WSSPOR-3200)

- **New Bypassed Domains dialog.**

  ISSUE: Improved language.

  (WSSPOR-3085)

- **WSS Agent Connection Information.**

  ISSUE: On the **Agents** page, the portal displayed three entries for the same WSS Agent client.

  (WSSPOR-3063)

- **Refresh Button on Agents page.**

  ISSUE: The **Agents** page required clicking **Refresh** one or more times for the **Disable** action menu option to be visible.

  (WSSPOR-2962)

- **Changed Google QUIC to HTTP/3.**

  ISSUE: On the **Agents**page, the Google QUIC option was renamed to **HTTP/3**. This reflects industry labeling.

  (WSSPOR-2915)

- **Corrected Japanese language on localized Bypassed Domains page.**

  ISSUE: On a Japanese localized browser, the **Policy > Bypassed Traffic > Bypassed Domains** page displayed incorrect language.

  (WSSPOR-1801)

- **Okta Federation.**

  ISSUE: Resolved an issue where a user was not federated in Okta; then became federated.

  (WSSPOR-2598)

- **Threat Sites Blocked report categories.**

  ISSUE: The **Threat Sites Blocked** report displayed categories as **unknown**.

  (WSSPOR-2298)

- **Safe Search text.**

  ISSUE: Improved the text on the Search Restrictions dialog (enforcing safe searches).

  (WSSPOR-2220)

- **UPE/CFS.**

  ISSUE: In a UPE deployment, group policy failed when CFS group policy referred to the same group.

  (WSSPOR-2044)

- **Find usage in policy error.**

  ISSUE: The **Type** column did not populate in the Find Usage In Policy dialog.

  (WSSPOR-2042)

- **Last Action Rreport error.**

  ISSUE: Attempting to add filters in the **Last Action Report** caused a JavaScript error.

  (WSSPOR-2014)

- **Last Action report source.**

  ISSUE: The **Last Action Report** did not display the log source (Proxy versus CFS).

  (WSSPOR-1865)

- **Admin & Users rilter error.**

  ISSUE: On the **Administrators** page, attempting to add a **Custom** filter resulted in a gray box instead of the **Add Criteria** option.

  (WSSPOR-2005)

- **Report generation timeout.**

  ISSUE: Sessions timed out when WSS was generating reports with a large volume of data.

  (WSSPOR-2001)

- **API Credential Expiry.**

  ISSUE: After setting an API Credential Expiry as **Time-Based**, the portal displayed the status as **Never**.

  (WSSPOR-1985)

- **Audit Logs omitted bypassed actions.**

  ISSUE: The Audit Logs did not display actions from an admin who created, edited, or deleted **Bypass** entries.

  (WSSPOR-1946)

- **Hero Bar reports.**

  ISSUE: In the Hero Bar (top of dashboard), clicking a report failed to generate the report.

  (WSSPOR-1935)

- **Sites in new policy rule.**

  ISSUE: Resolved an issue that prevented a new policy rule from displaying available sites.

  (WSSPOR-1933)

- **Searching for multiple users.**

  ISSUE: Resolved an issue that prevented a search of multiple portal admin usernames.

  (WSSPOR-1927)

- **New policy from Site Report.**

  ISSUE: Resolved an issue that prevented selecting **Action > New Policy Rule** from the **Site** report.

  (WSSPOR-1927)

- **Response page translations.**

  ISSUE: Resolved an issue involving Response Pages (exceptions) not translating properly into Chinese and Arabic.

  (WSSPOR-1906)

- **Policy Usage link.**

  ISSUE: Resolved an issue that prevented the **Policy Usage** link in a report to go to the correct location in the portal.

  (WSSPOR-1887)

- **Leaving editor warning.**

  ISSUE: Attempting to change a portal page that contained non-activated policy changes did not warn the admin.

(WSSPOR-1885)

- **Custom rule editor.**

  ISSUE: Selecting a global rule before a custom rule prevented the editing of custom rule.

  (WSSPOR-1856)

- **Reviewer role SAML certificate and Report Center access.**

  ISSUE: A WSS user in the Reviewer Role was able to add or remove SAML certificates. They could also run reports in Report Center.

  (WSSPOR-1813, 1807)

- **CFS/Blocked User report.**

  ISSUE: Resolved a portal UI issue that prevented the **Blocked User** report to open when CFS is enabled.

  (WSSPOR-1805)

- **Unresponsive Add Alerts button.**

  ISSUE: Clicking **Add Alerts** resulted in no action.

  (WSSPOR-1804)

- **Report downloads.**

  ISSUE: Resolved an issue that prevented many reports from downloading.

  (WSSPOR-1453)

- **Auth Connector page.**

  ISSUE: Resolved issues that delayed the Auth Connector connection status and version number.

  (WSSPOR-789, 790)

- **Email Notification.**

  ISSUE: Resolved an issue in which WSS sent email notifications to disabled portal users.

  (WSSPOR-706)

- **Password Override.**

  ISSUE: Resolved an issue so that WSS properly evaluates a Content Filter block override password for format validity.

  (WSSPOR-674)

- **Internet Explorer browser issues.**

  ISSUE: Resolved an issue observed in Internet Explorer that prevented complete numbers in the **Only between the following times of day** field on a scheduled report.

(WSSPOR-622)

ISSUE: Resolved issues with the **Confirm Access** button and **More Information** link on coaching verdict pages.

(WSSPOR-609)

- **Threat Response Pages.**

  ISSUE: Resolved an issue with incorrect Error IDs in a Threat Protect response page received on clients.

  (WSSPOR-594)

- **NSL Certification.**

  ISSUE: When attempting to download a WSS product application (a binary file, such as WSS Agent), users could not select the **I certify...** option on their profiles.

  (WSSPOR-47)

AUG.28.2020

- **PII Suppression.**

  ISSUE: Removed text from the **Account Configuration > Data Retention and Privacy** page/**End User Privacy** area. This text indicated that PII was not suppressed for WSS Agents. The **Agents** page suppresses data from WSS Agents.

  (WSSPOR-2998)

- **Location API calls to /api/l failed.**

  ISSUE: Customers were unable to use the shortened location API path (`/api/l`) to create or update locations. Attempting to use this URL resulted in an HTTP `404` error.

  (WSSPOR-2760)

- **Audit log.**

  ISSUE: The **Audit** log did not include local users.

  (WSSPOR-2840)

- **UPE Policy Size.**

  ISSUE: Increases the maximum size of UPE policy allowed to 15MB. The fix also improves the error language that better indicates when the limit is exceeded.

  (WSSPOR-2796)

- **Edit link was invisible if the domain name was too long.**

  ISSUE: Improved the portal UI on the **Bypassed IP** and **Domains** tabs. The **Edit** links were not visible if entries were too long.

  (WSSPOR-295)

- **Continued refinement of the Agent Status page.**

  ISSUE: Resolved several portal UI issues on the **Connectivity > Agents** page. The fields now populate correctly. The **Agent Type** filter contains valid entries in the drop-down. The **Refresh** button was requiring several clicks to function.

  (WSSPOR-2901, 2962)

- **IPsec Connection Data.**

  ISSUE: On the **Locations** page, fixed data displayed from the **Data Center Connections** link. Previously, the values indicated negative bandwidth use.

  (WSSPOR-2764)

- **The duration of Password Override prompt reverted to "Every 60 Minutes" after a page refresh.**

  ISSUE: On a policy, if you changed **Password Override** from the default 60 minutes to another value, saved the change, then refreshed the portal, the value reverted to the default.

  (WSSPOR-2836)

- **Corrected Japanese language on localized Bypassed Domain page.**

  ISSUE: On a Japanese localized browser, **Policy > Bypassed Traffic > Bypassed Domains** page displayed incorrect language.

  (WSSPOR-1801)

- **Auth Connectors attempted connections to former co-located locations.**

  ISSUE: Following the move of WSS to GCP, some Auth Connectors attempted to connect to auth IP addresses in locations that do not exist.

  (WSSPOR-2829)

JUL.06.2020

- **WSS Agent Status page: Refresh button restored.**

  ISSUE: The **Refresh** button has been restored on the **Connectivity > Agents** page. You can immediately sync connection data.

  (WSSPOR-2827)

- **WSS Agent Status page: Agent Type.**

  ISSUE: You can sort by connected **Agent Type** (Android, iOS, WSS Agent).

  (WSSPOR-2872)

- **WSS Agent Status page: Sorting.**

  ISSUE: Sorting by column changed how the data was presented.

(WSSPOR-2840)

- **WSS Agent Status page: Filtering.**

  ISSUE: Search and filter options mixed in random data that did not match the search results.

  (WSSPOR-2838)

- **WSS-sent Emails.**

  ISSUE: Emails generated by WSS (for example, registration confirmation) always went to recipient's spam folder.

  (WSSPOR-2856)

- **Datacenter Names on Network > Locations page.**

  ISSUE: Adjusted the page format so that the portal better displays longer datacenter names and details.

  (WSSPOR-2763)

- **Hosted Reporting log retention.**

  ISSUE: Changes in the reporting architecture resulted in Hosted Reporting accounts storing access log data for a max of one year instead of three.

  (WSSPOR-2854)

JUN.05.2020

- **WSS Agent status page did not display agent connections.**

  ISSUE: The **Connectivity > Agents** page did not display any WSS Agent connections.

  (WSU-960)

- **UPE Policy not pushed to WSS.**

  ISSUE: Size limitation prevented the Management Center from pushing policy to WSS.

  (WSU-923)

APR.30.2020

- **Changing group by field that is sorted resulted in an empty report.**

  ISSUE: After running a summary report, attempting to summarize by another element (site, for example) resulted in an report with no data.

  (WSSPOR-2191)

- **Isolated Sites report requested unused column.**

  ISSUE: The Isolated Sites report requested values for the `categories_text` but returned '-' for every line because that data is not part of the report.

  (WSSPOR-1909)

DEC.17.2019

- **Report: Unknown Server Error.**

  ISSUE: Attempting to view policy usage for a URL in a report resulted in an **Unknown server error has occurred** message.

  (POR-2006)

- **Add Criteria button did not function.**

  ISSUE: The **Add Criteria** button was not accessible when you attempted to create a report filter on the **Account Configuration > Administrators** page. **Report Filters > Add Filter > Filter Type > Custom**.

  (POR-2005)

- **Hosted Reporting: Data source not set.**

  ISSUE: This applied to Hosted Reporting only; not an issue with WSS native reporting. Data sources were not set, causing blank dashboards and reports.

  (POR-2033)

DEC.06.2019

- **IPSec SAs rekeyed every hour for IKEv2/FQDN location types.**

  ISSUE: Despite any defined rekey interval settings, the connection rekeyed every hour.

  (WSU-145)

- **Error 500 returned when converting network location to IKEv2.**

  ISSUE: When changing a location type to IKEv2, the portal returned a 500 HTTP error, instead of the expected confirmation.

  (WSU-396)

- **Threat Protection exemptions resulted in unexpected website blocking.**

  ISSUE: Bypassing some URLs from malware scanning resulted in some of those exempted sites getting blocked because SSL tunnels were not detected as SSL; Detect Protocol triggered a block. This was observed through the Unified Agent connectivity method.

  (WSU-482)

- **Threat Protection exemption did not disable protocol detection.**

  ISSUE: When websites used non-standard services over standard ports, the work-around was to disable protocol detection. The policy now evaluates the order so that this no longer occurs.

  (WSU-526)

- **Bypassing Apple domains.**

  ISSUE: Apple users found that when WSS services (SSL Interception, Threat Protection) are subjected to connections with Apple sites, those connections fail. This list of IP addresses allows admins to bypass WSS scrutiny for Apple services.

  See https://support.symantec.com/us/en/article.TECH256932.html for the list of domains and instructions to add that list to your Bypass configuration.

  (WSU-572)

- **Vertical axis missing in reports.**

  ISSUE: When limiting rows to 120, the reports did not display the vertical axis.

  (WSU-159)

- **Special character causes MC error when installing UPE policy.**

  CONDITIONS: Management Center, Universal Policy (UPE), Auth Connector

  ISSUE: Installing policy for AD groups that use the **Ñ** character caused a policy installation error.

  (WSU-254)

- **Hosted Reporting upload from ProxySG failed.**

  CONDITIONS: ProxySG, Hosted Reporting

  ISSUE: ProxySG access log uploads to Hosted Reporting failed.

  (WSU-444)

- **Portal failed to display drop-down menu on mouseover.**

  ISSUE: When a user hovered over fields, the WSS portal failed to display the expected drop-down menu.

  (POR-1329)

- **Partner Portal failed when commenting.**

  ISSUE: Clicking the comment bubble to add a customer comment caused the Partner Portal to fail and display **Unknown Server Error**.

  (POR-1627)

- **Email field in SamlAuthenticationProvider is hardcoded.**

  ISSUE: The attribute name `email` in `SamlAuthenticationProvider` was hardcoded. The expectation is that all data comes from the customer SAML configuration.

  (POR-962)

SEP.17.2019

- **Group authentication errors (SEP).**

  CONDITIONS:SEP with Seamless Identification, Auth Connector, and group-based policies.

  ISSUE: Group authorization was not sent to Auth Connector after 15 minutes, resulting in random group policy failures. Group allow policies above the G4 (Block) policies were still blocked.

  (WSU-524)

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)

Help System Update Log

This topic lists updates to the 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.

Help System Version–122/Expected NOV.07.2020

> **Note:** In an upcoming WSS portal release, this Help System will enter into legacy mode. Help topics will be provided on the Broadcom documentation site, which is currently available.
> https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/web-security-service/Help.html
> If you routinely bookmark topics, you can begin to locate the identical topic on the Broadcom site and replace.

WSS Service Update–NOV.07.2020

- The Help System reflects the new WSS portal LeftNav redesign.

Help System Version–121/AUG.28.2020

WSS Service Update–AUG.28.2020

- **WSS Agent Status** page updated. Several resolved issues improve this page.

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/mobile/mobile-verify.htm

  > **Tip:** Because of a to-be resolved issue, manually click **Refresh** to see the **Actions** column link.

- Added Roaming Captive Portal troubleshooting tip.

  http://portal.threatpulse.com/docs/sol/auth/rcp/auth-enable-rcp.htm

Help System Version–120/AUG.14.2020

WSS Service Update–AUG.14.2020

- Proxy Forwarding policy slightly revised so that example policy matches ProxySG Management Console examples; updated category name.

  http://portal.threatpulse.com/docs/sol/connectivity/fixed/proxy/conn-fwdpolicy.htm

- Deploy a Self Managed Certificate topic revised with Broadcom email address and new FAQs.

  http://portal.threatpulse.com/docs/sol/Solutions/ManagePolicy/SSL/Integrate_HSM.htm

- Corrected section headers on the Help System dashboards. They were erroneously linked to a deprecated topic; clicking them caused 404 errors.

Help System Version–119/JUL.06.2020

WSS Service Update–JUL.06.2020

- WSS Agent port information updated.

  http://portal.threatpulse.com/docs/sol/reference/ref-openports.htm

- WSS Agent connection page updated.

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/mobile/mobile-verify.htm

Help System Version–118/JUN.05.2020

WSS Service Update–JUN.05.2020

See "Recently Resolved Issues" on page 10.

Help System Version–117/MAY.22.2020

WSS Service Update–MAY.26.2020

- The move of WSS to Google Cloud Platform (GCP) changes various IP addresses used to connect WSS components, such as Auth Connector and WSS Agent.

  http://portal.threatpulse.com/docs/sol/reference/ref-openports.htm

- Technical correction–WSS Agent connections default to TCP when UDP is not available; previous version stated a fallback to DNS.

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/agent/conn-wssa-man.htm

- Access/CFS Log Download Update

  http://portal.threatpulse.com/docs/sol/Solutions/ManageReports/rpt_dwnload_log_ta.htm

- Removed links to Symantec training videos as the training platform is migrating to Broadcom's system from Symantec.

- EULA link updated to Broadcom's site. Search for `Web Security Service`.
- Minor edits.

Help System Version–116/APR.30.2020

WSS Service Update–APR.25.2020

- With the move from Norton Secure Login to Broadcom/Okta IdP for admin portal access, the initial registration topic was edited.

  http://portal.threatpulse.com/docs/sol/Solutions/Admin/Account/register_ta.htm

- The Okta process also changes how admin personal information changes occur.

  http://portal.threatpulse.com/docs/sol/Solutions/Admin/Account/user_chng_info_ta.htm

- The Okta process also changes how to you register your account for enterprise compliance, required to download applications such as the Auth Connector and WSS Agent (example link).

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/agent/conn-wssa-man.htm

- More KB links transitioned to Broadcom site.
- Minor edits/cross-reference fixes.

Help System Version–115/APR.25.2020

WSS Service Update–APR.25.2020

- CFS with WSS Agent–select forward all ports option. See the Best Practices section.

  http://portal.threatpulse.com/docs/sol/Solutions/CFS/cfs-policy-editor.htm

- Replacement DNS/IP addresses for Hosted Reporting > Direct SCP method.

  http://portal.threatpulse.com/docs/sol/Solutions/HostedReporting/hosted-scp-direct.htm

- More KB links transitioned to Broadcom site.
- On-premises DLP is deprecated; removed Help System topics.
- Updated version of WSS Agent macOS diagnostic application.
- Minor edits.

Help System Version–114/MAR.06.2020

WSS Service Update–JAN.31.2019

- New step for Auth Connector when Windows Server 2019 is employed.

  http://portal.threatpulse.com/docs/sol/auth/ac/auth-conn-deploy.htm

- Support links from Symantec to Broadcom. Be advised that some article redirects might not function yet. You can search the Broadcom support site for relevant terms.
- New version of WSS Agent MacOS diagnostic script.
- Minor edits.

Help System Version–113/JAN.31.2019

WSS Service Update–JAN.31.2019

- Bypass Domains–Clarity regarding simple matches.

  http://portal.threatpulse.com/docs/sol/Solutions/ManagePolicy/adm_bypassdomain_ta.htm

- SEP with Seamless Identification topic–Removed a firewall rule best practice.

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/sepclient/conn-sep-si.htm

- Proxy Forwarding–Removed the step to clear the **Verify SSL Server Certificate** option.

  http://portal.threatpulse.com/docs/sol/connectivity/fixed/proxy/conn-prxyfwd-symapp.htm

- Minor edits.

Help System Version–112/DEC.17.2019

WSS Service Update–DEC.06.2019

- Corrected broken cross references in authentication topics.
- Minor edits.

Help System Version–111/DEC.06.2019

WSS Service Update–DEC.06.2019

- Authentication revisions.
  - Authentication topics revised to provide method by connectivity method information, plus current best practice information.
  - These are new topics in the Help System. If you have previous HTML tabs bookmarked, be advised of the changed URLs.

New home topic.

http://portal.threatpulse.com/docs/sol/auth/auth-about.htm

- Updated IPsec Cert-Based topic with two updates requested from support:
  - New workflow in the portal for creating a set of API credentials.
  - New section added to the bottom of the topic to cover re-registering expired entrust certs.

"Recently Resolved Issues" on page 10

Help System Version–110/SEP.17.2019

WSS Service Update–SEP.17.2019

- Roaming Captive Portal–Added the Technical Requirement to install WSS certificate on all clients.
- New version of macOS diagnostic script for WSS Agent.

Help System Version–109/JUL.26.2019

WSS Service Update–JUL.26.2019

- Left-Nav menus revised with more topic inclusion.

WebGuide Version–108/JUL.01.2019

WSS Version: 6.10.5.1 APR.26.2019

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

  http://portal.threatpulse.com/docs/sol/auth/ac/auth-conn-deploy.htm

- Corrected CLI command for testing Hosted Reporting direct-to-WSS uploading.
- Skype for Business–bypass hostnames and IP addresses best practices.

  http://portal.threatpulse.com/docs/sol/O365/Office365_ta.htm

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

  http://portal.threatpulse.com/docs/sol/connectivity/endpoint/sepclient/conn-sep-sa.htm

- Full Access Log string added to reference topic.

  http://portal.threatpulse.com/docs/sol/Solutions/Reference/accesslogformats-ref.htm

Currently Known Issues

Symantec is aware of the following issues in the WSS.

All Ports License

- **Post Jan-31-2020 update, certificate firewall incompatible.**

  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)

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)

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)

Cloud Firewall Service

- **SAML User Groups currently not supported.**

  ISSUE: SAML User Groups currently not supported.

Common Policy

- **Default Block Categories not copying to on-premises proxy.**

  ISSUE: Following an update, not all blocked category policies correctly propagated.

(B#238438)

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)

Office 365

- **SEP/Seamless ID and Explicit Proxy–Direct-to-net required.**

  ISSUE: To be compatible with the SEP with Seamless Identification 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 WSS.

  (B#263977)

Policy

- **Dropbox not supported.**

  ISSUE: Because of some required SSL interception intricacies, the WSS 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)

Portal

- **EarIngestionSnapshotJob not logging**

  ISSUE: The Elastic Analytics & Reporting Service job, **EarIngestionSnapshotJob**, is not logging anything to the portal log (on success or failure).

  (POR-1421)

- **Import VPN Gateway Firewall Locations UI issue**

  ISSUE: Issue: Import VPN Gateway Firewall Locations has a gray box around the Browse button.

  (POR-1713)

- **Bypassed Domains page provides inconsistent Japanese translation**

  ISSUE: The Japanese translation of **Service** mode **> Network > Bypassed Sites > Bypassed Domains** provides incomplete information.

  - The English version reads: Traffic sent to these domains bypasses the Web Security Service only when sent from Unified Agent clients, WSS Agent clients and Explicit Proxy locations.
  - Whereas the translation reads: Traffic sent to these domains bypasses the Web Security Service only when sent from** Explicit Proxy locations.

  (POR-1801)

Reporting

- **CFS Reports not displaying for accounts not migrated to EA&R.**

  ISSUE: Cloud Firewall Service reports not displayed if the customer has not migrated to Elastic Analytics & Reporting service.

  (POR-1207)

- **Status for migrating to EA&R incorrect/inconsistent.**

  ISSUE: Migration Status displayed for customers moving to the Elastic Analytics & Reporting Service is inconsistent; displays **Data Migration Complete** when it is not.

  (POR-1355)

- **Manipulating report widget leads to unexpected results**

  ISSUE: Collapsing and then re-expanding a report widget removes the View Full Report link

  (POR-1356)

- **Archive Executive Summary provides no progress alert**

  ISSUE: Generating an archived Executive Summary results in no progress or completion notification.

  (POR-1506)

- **Several reports fail to download as PDF**

  ISSUE: Reports for applications by Client IP, Applications By Users, and Top Malware Source Countries fail to generate PDFs for download.

  (POR-1453)

- **Firefox displays modified column order inconsistently.**

  ISSUE: When modifying column sort order, Firefox fails to display report columns in the requested order. No issue on other browsers.

  (POR-1004)

- **Last Access report column fails to sort**

  ISSUE: Sorting reports by the Last Access column, the UI reports that a sort has taken place when it has not. The data remains unsorted.

  (POR-1477)

- **Archive Report fails on large report**

  ISSUE: Archive report fails on a large report (>1,000,000 rows).

  (POR-1492)

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 ID.**

  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)

Unified Agent

- **English strings are not translated to Japanese.**

  ISSUE: Many strings in the WSS do not translate when the browser is set to Japanese.

  (B#177889)

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 Web Security Service requires using other Symantec and third-party technologies. This page provides an index to those supported technologies.

Technology	Reference
WSS Agent	"Recent WSS Agent Releases" on page 31
I will install the Unified Agent for remote users. What are the desktop anti-virus (AV) compatibilities?	"Desktop Anti-Virus Compatibility" on page 34
What browsers can I use to access the WSS?	"Supported Browsers" on page 35
I will use the Proxy Forwarding connectivity method to route web traffic to WSS. What proxy appliances and operating systems are supported?	"Supported Proxy Devices" on page 36
I want to employ SAML authentication.	"Supported SAML IDPs" on page 37

Recent WSS Agent Releases

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

> **Note:** You must use the fully-patched vendor-provided versions of the operating systems. All attempts to install on an unsupported OS fail.

VPN Client Compatibility

The WSS 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 WSS (**Connectivity > Locations**). This enables the WSS 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.

WSS Agent 7.1.1

Supported Operating Systems:

- 64-bit Windows 10 Professional, Enterprise or Education version 1803 and later (Semi-Annual Servicing Channel)
- macOS Mojave+

Features:

- Single Tunnel Mode by default.
- Support for WSS-SEP-NTR (Network Traffic Redirection).
- Installs new WSS root certificate on endpoints.

Resolved Issues:

- WSS Agent UI was out of sync with the background service.
- QUIC traffic was occasionally allowed despite the Block setting in the portal.
- IPv6 domain bypasses were not correctly honored.
- Improved stability and performance.

Technology Notes:

- On a Windows machine that is accessed through Microsoft RDP, WSS Agent 7.x+ must be installed with the Multiple Concurrent Users (`MCU`) option set. Failure to do so results in WSS Agent clients receiving an error: `No user logged on at physical console`.
- WSS Agent v7.x+ does not support Captive Portal.

WSS Agent 6.2.1

Supported Operating Systems:

- 64-bit Windows 10 Professional, Enterprise or Education version 1703 and later
- macOS High Sierra+

Resolved Issues:

- Resolved a security issue. The best practice for any customers with WSS Agents 6.1.1 through 6.1.3 deployed is to upgrade to 6.2.x.
- Resolved issue where the notifier prompted for update, even if **Prompt For Updates** was disabled in the portal.
- Resolved issue where an update always required a reboot on macOS Catalina.
- Resolved issue where the macOS update progress UI could not be dismissed.
- Improved automatic update process.
- Resolved Kernel panic during startup on high-end hardware.
- Mixed cases in domain bypass lists.
- Updated the links on the **About** tab to point to Broadcom's license repository.
- Switch to passive network required two reconnects.
- Resolved an issue that causes unnecessary DNS requests.
- Signed with Broadcom certificates. Broadcom's Organization Identifier on macOS is `Y2CCP3S9W7`.

WSS Agent 6.1.1

Supported Operating Systems:

- 64-bit Windows 10 Professional, Enterprise or Education version 1703 and later (Semi-Annual Servicing Channel)
- macOS High Sierra+

Features:

- Supports the Cloud Firewall Service.
- Full support for HDN.
- Block IPv6 Packets.

- BNS Events in Windows Event Log.
- Real-time statistics v2.
- Improved macOS diagnostics.
- UI enhancements.

Desktop Anti-Virus Compatibility

If you plan to install the WSS Agent application onto employee systems to support remote access to the 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 Symantec; 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. The best practice is to test 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 WSS 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 Web Security Service portal.

- 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 Symantec.

Furthermore, browsers requires Javascript and cookie support.

Supported Proxy Devices

The Web Security Service Proxy Forward connectivity method requires you to configure the network egress proxy device to forward web-bound requests to the service.Symantec tested the following proxies; however, all proxy models and SGOS versions released since are supported.

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

SGOS Versions

- 6.5.x (not with UPE)
- 6.7.x
- 7.x

Supported SAML IDPs

Currently, Symantec tested and supports the following Identity Providers (IdPs).

- The Symantec Auth Connector–Instead of a third-party vendor SAML Identity Provider (IdP), the Auth Connector can function as the IdP.

  http://portal.threatpulse.com/docs/am/AMDoc.htm#Deployment/Tasks/Auth/SAML/saml_authconnIdP_sol.htm

- Active Directory Federation Services (AD FS) 2.0

  http://portal.threatpulse.com/docs/am/AMDoc.htm#Deployment/Tasks/Auth/SAML/saml_3rdparty_sol.htm

- Symantec VIP Access Manager

  http://portal.threatpulse.com/docs/am/AccessMethods/auth/SAML/saml_symIdP.htm

- Google G Suite

  http://portal.threatpulse.com/docs/am/AccessMethods/auth/SAML/saml_azureIdP.htm

- Microsoft Azure

  http://portal.threatpulse.com/docs/am/AccessMethods/auth/SAML/saml_azureIdP.htm

- Okta

  http://portal.threatpulse.com/docs/am/AccessMethods/auth/SAML/saml_azureIdP.htm

- Ping

  http://portal.threatpulse.com/docs/am/AccessMethods/auth/SAML/saml_azureIdP.htm

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