Copyrights

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 2020 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.
Symantec Web Security Service Policy Guide

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.

If the Web Security Service is the body, then the policy engine is the brain. While the Web Security Service by default provides malware protection (blocks four categories: Phishing, Proxy Avoidance, Spyware Effects/Privacy Concerns, and Spyware/Malware Sources), the additional policy rules and options you create dictate exactly what content your employees can and cannot access—from global allows/denials to individual users at specific times from specific locations.

This document provides policy concepts and describes how to use the Web Security Service portal to define policies. It includes high-level and use case examples. The document breaks out information in three areas:

- "About Web Security Service Policy" on page 9
- "Filter Content" on page 13
- "Malware Policy" on page 39
- "Web Application Policy" on page 77
- "SSL Policy" on page 97
- "Policy: How Do I?" on page 152
- "Policy Reference" on page 185

This document contains topics collected from the Web Security Service online documentation. For the complete doc set, see:

Symantec Support Site > WSS Documentation

---

Table Of Contents

Symantec Web Security Service Policy Guide ................................................................. 4
  Table Of Contents ......................................................................................................... 4

About Web Security Service Policy ................................................................................. 9
  About the Traffic Evaluation Order ............................................................................. 9

About Geolocation Policies ............................................................................................ 11
  Supported Methods ................................................................................................. 11
  Reporting ................................................................................................................. 11
  Exception Pages ..................................................................................................... 11
  User Privacy ........................................................................................................... 12
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Content</td>
<td></td>
</tr>
<tr>
<td>About Content Filtering</td>
<td>13</td>
</tr>
<tr>
<td>Control User Access to Web Content</td>
<td>14</td>
</tr>
<tr>
<td>About the Default Policies</td>
<td>16</td>
</tr>
<tr>
<td>Step 1—Review the current Content Filtering policies and adjust if</td>
<td></td>
</tr>
<tr>
<td>necessary.</td>
<td>16</td>
</tr>
<tr>
<td>Step 2—After the Web Security Service begins processing data,</td>
<td></td>
</tr>
<tr>
<td>monitor employee web use activity.</td>
<td>17</td>
</tr>
<tr>
<td>Step 3—(Optional) Configure an exception page that users see when</td>
<td></td>
</tr>
<tr>
<td>they browse to a blocked web destination.</td>
<td>17</td>
</tr>
<tr>
<td>About the Content Filtering Rule Editor</td>
<td>18</td>
</tr>
<tr>
<td>Content Filter Policy Construct</td>
<td></td>
</tr>
<tr>
<td>AND/OR Constructs</td>
<td>18</td>
</tr>
<tr>
<td>Group and Global Rows</td>
<td>19</td>
</tr>
<tr>
<td>Group A Rules</td>
<td></td>
</tr>
<tr>
<td>Group B Rules</td>
<td></td>
</tr>
<tr>
<td>Global Rules</td>
<td>20</td>
</tr>
<tr>
<td>Create Custom Content Filtering Rules</td>
<td>22</td>
</tr>
<tr>
<td>Construct and Editor Tutorials</td>
<td></td>
</tr>
<tr>
<td>Activate Policy</td>
<td>28</td>
</tr>
<tr>
<td>Exempt URLs from Permanently Blocked Categories</td>
<td>29</td>
</tr>
<tr>
<td>Modify the Default Exception Notifications</td>
<td>30</td>
</tr>
<tr>
<td>Troubleshooting Assistance</td>
<td></td>
</tr>
<tr>
<td>Customize the User Notification Template</td>
<td>33</td>
</tr>
<tr>
<td>Use Cases</td>
<td>34</td>
</tr>
<tr>
<td>Best Practices</td>
<td></td>
</tr>
<tr>
<td>Malware Policy</td>
<td>39</td>
</tr>
<tr>
<td>About Malware Scanning</td>
<td>40</td>
</tr>
<tr>
<td>Base Level</td>
<td></td>
</tr>
<tr>
<td>Basic Level Protection</td>
<td></td>
</tr>
<tr>
<td>Malware Analysis Standard Service</td>
<td>41</td>
</tr>
<tr>
<td>MASS License Protection</td>
<td></td>
</tr>
<tr>
<td>Malware Analysis Advanced Service</td>
<td></td>
</tr>
<tr>
<td>Supported Common Documents and File Types</td>
<td>42</td>
</tr>
<tr>
<td>Protect Your Network From Web Threats</td>
<td>45</td>
</tr>
<tr>
<td>Proxy Analysis</td>
<td></td>
</tr>
<tr>
<td>Content Analysis</td>
<td></td>
</tr>
<tr>
<td>Malware Analysis</td>
<td></td>
</tr>
<tr>
<td>Malware Exemptions and Policy</td>
<td>46</td>
</tr>
<tr>
<td>Geolocation-Based Policies</td>
<td></td>
</tr>
<tr>
<td>Web Isolation</td>
<td>47</td>
</tr>
<tr>
<td>Threat Protection Policy Editor</td>
<td>48</td>
</tr>
<tr>
<td>Malware Policy From Risk Score</td>
<td>50</td>
</tr>
<tr>
<td>Web Isolation Policy Based on Risk Score</td>
<td></td>
</tr>
<tr>
<td>Risk Score Reporting</td>
<td>52</td>
</tr>
<tr>
<td>Exempt a Source From Malware Scan</td>
<td>54</td>
</tr>
<tr>
<td>Exemptable Sources</td>
<td></td>
</tr>
<tr>
<td>Exemption Levels</td>
<td></td>
</tr>
<tr>
<td>Procedures</td>
<td>54</td>
</tr>
<tr>
<td>Change Exemption Scanning Level</td>
<td>56</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----</td>
</tr>
<tr>
<td>Exempt a Destination From Malware Scan</td>
<td>58</td>
</tr>
<tr>
<td>Exemptable Destinations</td>
<td>58</td>
</tr>
<tr>
<td>Exemption Levels</td>
<td>58</td>
</tr>
<tr>
<td>Procedures</td>
<td>58</td>
</tr>
<tr>
<td>Exempt Files From Error Handling</td>
<td>61</td>
</tr>
<tr>
<td>About Web Isolation</td>
<td>62</td>
</tr>
<tr>
<td>What is Web Isolation?</td>
<td>62</td>
</tr>
<tr>
<td>Protect Endpoints from Attack</td>
<td>62</td>
</tr>
<tr>
<td>Topography</td>
<td>63</td>
</tr>
<tr>
<td>About the Two Web Isolation License Types</td>
<td>64</td>
</tr>
<tr>
<td>Geolocation—The Advanced Web Security Add-On</td>
<td>64</td>
</tr>
<tr>
<td>About Web Isolation and UPE</td>
<td>64</td>
</tr>
<tr>
<td>About Web Isolation Operations</td>
<td>64</td>
</tr>
<tr>
<td>Traffic</td>
<td>65</td>
</tr>
<tr>
<td>Enable Web Isolation</td>
<td>66</td>
</tr>
<tr>
<td>Procedure</td>
<td>66</td>
</tr>
<tr>
<td>Step 1—Enable Web Isolation</td>
<td>66</td>
</tr>
<tr>
<td>Step 2—Define an Isolation Policy Rule</td>
<td>67</td>
</tr>
<tr>
<td>Isolation Based on Risk Scores</td>
<td>68</td>
</tr>
<tr>
<td>Monitor Licensed Capacity</td>
<td>69</td>
</tr>
<tr>
<td>Web Isolation Reporting</td>
<td>69</td>
</tr>
<tr>
<td>Skype for Business Issue</td>
<td>70</td>
</tr>
<tr>
<td>About Web Isolation With UPE</td>
<td>71</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>71</td>
</tr>
<tr>
<td>Limitations</td>
<td>71</td>
</tr>
<tr>
<td>Supported Deployments</td>
<td>71</td>
</tr>
<tr>
<td>Web Isolation Policy Template</td>
<td>75</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>75</td>
</tr>
<tr>
<td>About the Policy Objects</td>
<td>75</td>
</tr>
<tr>
<td>UPE and Web Isolation Policy Template</td>
<td>75</td>
</tr>
<tr>
<td>About SSL Interception of Mobile Traffic (UPE)</td>
<td>76</td>
</tr>
<tr>
<td>About Failure Modes</td>
<td>76</td>
</tr>
<tr>
<td>Web Application Policy</td>
<td>77</td>
</tr>
<tr>
<td>About Controlling Web Application Access</td>
<td>78</td>
</tr>
<tr>
<td>Web Application Category Reference</td>
<td>80</td>
</tr>
<tr>
<td>About the CASB Integration</td>
<td>81</td>
</tr>
<tr>
<td>CASB Topography</td>
<td>81</td>
</tr>
<tr>
<td>About the Traffic Evaluation Order</td>
<td>82</td>
</tr>
<tr>
<td>Current Limitations</td>
<td>83</td>
</tr>
<tr>
<td>Integrate With CloudSOC (CASB)</td>
<td>84</td>
</tr>
<tr>
<td>Procedure</td>
<td>84</td>
</tr>
<tr>
<td>Access the CASB Audit App</td>
<td>85</td>
</tr>
<tr>
<td>Web Application Policy</td>
<td>87</td>
</tr>
<tr>
<td>View CASB-Related Reports</td>
<td>87</td>
</tr>
<tr>
<td>Add Reporting Users</td>
<td>87</td>
</tr>
</tbody>
</table>
About Web Security Service Policy

For the Symantec Web Security Service solution, policy refers to configuration controls that restrict or allow network and web elements such as IP addresses and content filtering categories. Only WSS users in the Admin Role can define the policies that comprise a Secure Web Gateway solution.

Policy controls are flexible and allow you to apply global settings or granular rules for web content categories, web applications, threat protection, and web isolation. For example, you can determine what happens to requests based on the role of requester. In the above example, WSS policy is defined to achieve the following:

- **A**—Allow a network subnet, which requires the highest performance level possible, to bypass WSS malware scanning, but explicitly block another specific destination. For example, you do not want Group B allowed access to sensitive locations that have company IP.

- **B**—Allow the **Sports** website category, but deny **Gambling** sites.

- **C**—Allow access the **Facebook** social networking web application but within Facebook block games; allow **webmail** applications.

About the Traffic Evaluation Order

The following summarizes how the WSS and CloudSOC prioritizes and evaluates traffic according to behavior. When possible, all behaviors are applied; the order addresses conflicts.
- Denial and blocking based on **policy rules** configured in the WSS portal or from Universal Policy Enforcement (UPE) uploaded policy rules.
  
  For security and compliance reasons, explicit denials (for Content Filtering or Threat Protection) must be applied.

- **SSL Intercept exemptions** configured in the WSS portal.
  
  Explicit SSL exemptions (for example, traffic to **Healthcare** categories) are assumed to be defined by an organization's legal compliance.

- **CASB Gatelet** processing of flows (with implicitly enabled SSL Interception).
  
  To properly function, CASB Gatelets automatically implement SSL Interception for specific destinations.

- **WSS-applied AV and DLP scanning.**
  
  DLP scanning occurs before the malware scanning.

- **Web Isolation** forwarding.
About Geolocation Policies

If your portal account has the Advanced Web Security with Risk Controls and Web Applications add-on license, the Source and Destinations constructs in the Content Filtering and Threat Protection policy editors contain the Geolocation construct. This allows you to create policy based on from what country or to what country a content request occurs.

**Tip:** Geolocations are supported with the Universal Policy Enforcement (UPE) solution if the on-premises ProxySG also is provisioned with the correct license.

Supported Methods

Because of how the Web Security Service determines the geolocation (country), this policy is best suited for the following Access Methods.

- Explicit Proxy
- Mobile Devices (iOS, Android)
- WSS Agent and SEP clients
- Roaming Captive Portal authentication option

Be advised of the following details.

- **Sources**—If the Access Method is Firewall/VPN or Proxy Forwarding, the WSS receives the IP address of the client system; therefore, the service cannot properly determine the geolocation. For these methods, define policy based on the fixed locations (as defined in **Service mode > Network > Locations**).

- **Destinations**—The WSS determines the geolocation based on a DNS resolution to an IP address. If the destination IP address resolves to a different IP address for the same URL, a different policy result might occur.

Reporting

The WSS provides pre-defined geolocation reports based on Sources only. You can create custom reports to see results based on Destinations.

Exception Pages

When a client request triggers a policy rule, the WSS displays an exception page.
- The exception details includes the source (Client Geolocation).

**Tip:** To provide Server Geolocation, create a custom exception page. See "Customize the User Notification Template" on page 161.

- The Error ID item informs you what policy rule triggered the exception.
  - In the above example, Content Filtering (CF) rule G1 is the trigger.
  - A TP-## indicates a Threat Protection a rule.

**User Privacy**

The add-on license allows you to suppress personal information based on geolocation. See Suppress Personal Information From Access Logs.

**Define Policies?**

- "Create Custom Content Filtering Rules" on page 22
- "Threat Protection Policy Editor" on page 48
- "Enable Web Isolation" on page 66
Filter Content

Configure the Web Security Service to apply content filtering policy to web requests and responses.

- "About Content Filtering" on page 14
- "Control User Access to Web Content" on page 16
- "About the Content Filtering Rule Editor" on page 18
- "Create Custom Content Filtering Rules" on page 22
- "Modify the Default Exception Notifications" on page 157
- "Customize the User Notification Template" on page 161
About Content Filtering

The Symantec Web Security Service leverages the Global Intelligence Network (GIN), which is driven by a community of tens of millions of users. As these users browse web content, GIN scans the content and assigns a category rating. The WSS policy checks against this database.

The WSS enables you to define a Content Filtering policy that meets your business requirements. Policy consists of a combination of blocked and allowed web content categories and trusted and blocked sources and destinations. You have the option to create global rules (basic policy) that apply to all users or create more granular rules (advanced policy).

In the above example, there are two types of users: Executive Staff and standard Employees. The WSS policy achieves the following:

- **A**—The Exec initiates two web destinations: a Gambling site and a Newsgroups/Forums site.
- **B**—Employees request Shopping, Sports, and Newsgroup/Forums sites.
- **C**—The WSS Policy and Content Filtering engines determine what happens based on who is allowed access to which categories.
  
  - The Exec is denied the gambling site, as Gambling is a globally blocked category. However, she is allowed access to the news forum because the Exec group is given permission to the Newsgroup/Forums category.
- Employees are allowed to the shopping sites (although they might receive a coaching message). They are blocked from accessing Sports sites, except for espn.com, which is configured as allowed. Another option here is to allow access only during specific days and times.

- Unlike the Exec group, employees are also denied access to sites rated as Newsgroup/Forums.

**Note:** All trademarks used herein are the property of their respective owners.
Control User Access to Web Content

By default, the Symantec Web Security Service blocks the most common web categories that are deemed inappropriate in the work environment or are known sources of malicious content. Furthermore, if High Risk Coverage was selected as the default policy during the Initial Configuration, the Web Security Service blocks additional web content. The Web Security Service enables you to alter the default Content Filtering policy to meet the needs for your business environment.

About the Default Policies

When you or someone in your organization performed the Web Security Service on-boarding, the Default Policy selection was presented. Based on that initial selection, the Web Security Service blocks categories.

The following policy controls provide a baseline policy against all other transactions:

- **Monitor**—Provides only malware scanning. Users are allowed to browse anywhere.
  - Child pornography
  - Malicious Outbound Data/Botnets
  - Malicious Sources
  - Phishing
  - Proxy Avoidance
  - Spam

- **Standard**—In addition to the Monitor categories, provides malware scanning plus blocks access to the most common questionable content, such as mature.
  - Adult/Mature Content
  - Controlled Substances
  - Gambling
  - Hacking
  - Nudity
  - Peer-to-Peer (P2P)
  - Piracy/Copyright Concerns
  - Placeholders
  - Pornography
  - Potentially Unwanted Software
  - Remote Access Tools
Scam/Questionable/Illegal
Suspicious

High—In addition to the Monitor and Standard categories, provides malware scanning plus blocks access to the most common questionable content and common categories that are not work-related, such as social networking sites.

Dynamic DNS Host
Extreme
Intimate Apparel/Swimsuit
Mixed Content/Potentially Adult
Sex Education
Sexual Expression
Software Downloads
Violence/Hate/Racism
Weapons

Regardless of this selection, you can further modify policy from the Web Security Service portal after completing the registration process.

Step 1—Review the current Content Filtering policies and adjust if necessary.

- "About the Content Filtering Rule Editor" on page 18—Describes the Policy Editor rows and elements.
- "Create Custom Content Filtering Rules" on page 22—Demonstrates how to create policy constructs and rules.
- "About Geolocation Policies" on page 11—Learn about how to execute policies based on countries (requests to and requests from).

Step 2—After the Web Security Service begins processing data, monitor employee web use activity.

- For a high-level summary, view the Content Filter Dashboard (in Solutions Mode, select Content Filtering > Dashboard).
- Generate a pre-defined report. Select Content Filtering > Reports. Click any link to generate a report.

Step 3—(Optional) Configure an exception page that users see when they browse to a blocked web destination.

- "Modify the Default Exception Notifications" on page 157.
- "Customize the User Notification Template" on page 161.
About the Content Filtering Rule Editor

The Symantec Web Security Service **Content Filtering Rules** policy editor allows you to accomplish the following:

- Create custom rules that, based on who requested it, allow or block access to web content.
- Quickly define global policy, or rules that apply to every employee that is not explicitly allowed or blocked by a custom rule.

To view the **Content Filter Rules** policy editor, in **Solutions** mode, select **Content Filtering > Policy**. The Policy Rules matrix comprises five columns—an Order column and four policy constructs—and a series of rows. The following sections describe how to interpret the editor and create new rules.

Content Filter Policy Construct

Policy Rules columns provide options for four constructs that shape the purpose of the rule.

By **Column** name—

- **Sources**—Applies to content requests. Users, Unauthenticated Users, Groups, IP addresses/Subnets, fixed Locations, WSS Agents, Mobile Users, and Geolocations (if your account has the license). The default is **Any**.

- **Destinations**—Applies to requested content Categories, Web Applications, IP addresses/Subnets, Domains/URLs, and Geolocations. The default is **Any**.

  **Tip:** See "About Geolocation Policies" on page 11 for more details.

- **Content and Limits**—Applies to content parameters. For example, set the policy to only apply to selected file types, browsers, or actions within web applications.
  
  - Actions, such as media uploads and downloads, joining meetings, games.
  - Specific browser vendors.
  - File Types
  - Schedule—Define when the policy rules apply, such as during core business hours.

The default is the rule applies to all contents at any time.
Note: Some Actions are valid only in Group A; others in Group B. For example, File Types are notated with a B. These items correspond to the rows that the WSS will place them. The Contents and Limits section below discusses this.

- **Verdict**–
  - Allow or block the request or content if any policy matches occur in the rule.
  - Advise (coach) employees that their internet activity is recorded
  - Redirect the user to another web location (such as an intranet site that lists appropriate web use guidelines).
  - Require a password to access content.

**AND/OR Constructs**

The Policy Editor enables you to create And/Or constructs. For example, you have a rule where the Sources are either of two users (an Or construct) if the request from a specific location (an And construct). The Add a Policy Rule section below demonstrates an example.

**Group and Global Rows**

The rules editor contains two distinct areas: **Group A** and **Group B**. As you add and modify rules, the Content Filtering Rules policy editor automatically places the rules in the correct group and correct order. Rules might contain conditions for a mix of inbound and outbound traffic; the actions and whether the elements in the request or the response triggers the policy dictates the appropriate rule grouping. Furthermore, the editor displays messages whenever a rule addition or change requires a rule to be moved. This section describes why rules are placed where they are.

Rules are evaluated in order. If a rule matches, no other subsequent rules are checked.

**Group A Rules**

As the service executes the rules in this group first, the only conditions available are those that test the request and the only actions are those that can be enforced on the request. The rules in **Group A** cannot **depend** on the content returned from the web destination. This is because for this group of rules the WSS must check the policy **before** the request reaches the content server.

If traffic matches a **Group A** rule, the **request** never reaches the **server**. Keep this in mind as you develop policy. For example, you might prefer to put rules in **Group A** when possible for security reasons.
Group B Rules

If no rule in Group A triggers a policy action, the WSS checks rules in Group B. As such, while Group A cannot depend on returned content, Group B might. Rules in Group B can execute on traffic before it reaches the web destination, such as a blocked IP address or content filter category. However, if any rules contain actions that must execute on returned content, they are placed in Group B. This includes actions such as policy based on file type, an Allow verdict with web use coaching, and Block verdicts with password override.

Global Rules

There are hard-coded rule rows that cannot be deleted. They are designated as G1, G2, G3, and G4. Primarily, these rules are in place to enforce pre-defined, default policies. Where applicable for the rule, the columns contain links. Click the link to display an editor dialog from which you can specify or select policy objects that apply to everyone (unless they are allowed or blocked by other custom policy).

- **G1**—Designated row for permanently blocked categories, such as Child Pornography.
- **G2**—An Allow rule that applies to source IP addresses/subnets. The policy check occurs on the request.
**G3**—An **Allow** rule that applies to specific trusted, or safe, destination URLs, IP addresses/subnets, and web applications. For actions, such as uploading and downloading content, the policy occurs on the response.

**G4**—A **Block** rule that applies to specifically blocked destination categories and web applications, URLs, and IP addresses/subnets.

In the editor, mouse-over the **text bubble** icons and the **G**-numbers in the left column to view these descriptions in text pop-ups.

**Create a new rule?**

- "Create Custom Content Filtering Rules" on page 22
Create Custom Content Filtering Rules

You will more than likely need to create policy rules that accomplish your corporate web use guidelines while ensuring the web resources required for your business remain available. For example, you might have applied a global block to a specific content category or web application, but now need to allow specific users or groups access.

Tip: To save time, create policy objects (Overview > Object Library page) that you know you will use multiple times. For example, a set of allowed domains or a group of categories.

To launch the rule wizard, click Add Rule.

- The Conditions area is where you define the constructs of the policy rule. From who or where did the request originate? To where is it going? And does it apply to specific content or based on a time frame?
- The Verdict area is where you define the action to take if the rule is triggered.

Construct and Editor Tutorials

The Editor and a Sources Construct

This example demonstrates what you can add to the Sources construct of the rule, including how to use the editor. Click Add Sources.
The policy editor is flexible, allowing you to select objects and existing lists as well as create new lists from objects within. Refer to the screenshot.

a. Select from objects that the WSS currently detects, such as usernames and group names provided by the authentication methods (Auth Connector or SAML IDP), IP addresses, and fixed locations. You can also select a Geolocation, which means the request originated from a specific country.

Tip: Geolocation policy requires an add-on license. See "About Geolocation Policies" on page 11 for more details.

b. If you have previously created custom lists in the Object Library (Overview > Object Library) or previously in the policy editor, select a List item.

c. The policy editor provides static objects that apply to all connections from those sources.
   - **Unauthenticated Users**—A username that is not part of your corporate username database.
   - **Mobile Devices**—Users who log in through a smartphone or tablet.
   - **Unified Agents**—Users who log in from remote client systems that have the Symantec Unified Agent installed. These are connections from beyond the corporate network.

Select any construct to display its options. Show screen...
• The editor displays all of the objects that are available for this rule. Select one or more and click the right-arrow to assign them to the rule.

• You can also click New and select to create a new list in applicable constructs a new object.

After completing your selections, perform one of the following.

• If this rule is intended for these sources only, click Save.

• To add different source constructs, click the back-arrow (upper-left); repeat to add sources and click Save.

  This creates an OR construct; the rule triggers if the content request originates from a source associated with any of the objects.

You can also continue to add sources that create an AND construct. Consider the following example.

The Admin clicked Add "AND" Group and added two fixed Locations as Sources. Now the rule is triggered by any user belonging to the events or pr groups AND from the specified Locations, one through a firewall device and one through explicit proxy.
The Destinations Construct and Creating Lists

This example demonstrates what you can add to the Destinations construct of the rule, plus how to create lists within.

Click Add Destinations. Select to what internet elements this rule applies. As with the Sources construct, you can create AND/OR policies.

- **IP/Subnets and URLs/Domains**—You might have a need to trigger policy when the destination is a specific server, such as a testing server, or a specific URL path.

- **Category**—Policy applies when the request is for websites that belongs to a specific content category. The Symantec Global Intelligence Network (GIN) continuously rates and classifies websites as they come online.

- **Web Application**—Policy applies when the request is for one or more of the thousands of web applications the Web Security Service detects. This is also known as a Cloud Access Security Broker (CASB) discovery and policy solution.

Create a List

On many policy editor screens, there is an option to create a list from objects you select. Show screen...

![Add Destinations](image)

After you name, create, and save the list, it becomes available for future selection in other rules.

The Contents and Limits Constructs

The final trigger Construct bases the rule on the following elements.

- **Schedule**—If you set a schedule, the rule applies only on the specified days and during the specified hours. For example, you might want certain content restriction rules to apply only during core business hours.

- **Browser**—Your company might elect to employees to use the most recent versions or even one specific browser vendor.

- **File Type**—Trigger the rule if the request is for specific types of files, such as Databases or Audio and Music.
Actions—When paired with Web Application Destinations, you can provide a robust, granular policy. For example, you might allow access to various social networking sites, but want to prevent the uploading or downloading of photos and videos for specific applications.

This page provides an additional Filter field from which you can select a specific application and view what actions the Web Security Service detects.

Conflicts with Actions and File Types

- Notice that some Actions are amended with an A. Rules that contain specific actions, such as File Upload, must be enforced during request before the actual upload request reaches the server. Such objects require the rule to be created in Group A.

- Notice that all File Types are amended with a B. For rules that contain specific actions, such as Executable, the Web Security Service must see the contents of the response so that it can detect whether it is actually an executable. Such require the rule to be created in Group B.

If you attempt to create a construct that contains incompatible elements, the Web Security Service displays a red exclamation mark to indicate an error. You can roll over the letters to read an explanation. You must create separate rules to achieve your policy goal.

The Verdict Construct

Now that you have created the conditions that trigger the policy rule, the final configuration is to instruct the Web Security Service what action to take. This is called the Verdict.
Allow

- **Allow: Completely**—Users are allowed access to the content.
- **Allow: Coaching**—Before allowed content access, users must click a message that acknowledges their request for such content and that they understand their web activities are monitored. You can also change the interval between coaching message re-displays.

Block

- **Block**—Users are denied access to the content.
- **Block: Password Override**—You can specify a password that you can distribute to users who request access to a blocked content. You can also change when the coaching message re-displays.
- **Redirect**—In addition to blocking access to the content, you can enter a URL that redirects users to a specific web resource. For example, when a user attempts to browse inappropriate content, redirect them to an internal web page that describes your corporate web use guidelines.

**Activate Policy**

Now the that rule is complete, click **Add Rule**.

Based on the constructs, the Web Security Service automatically inserts the rule to the bottom of **Group A** or **B** accordingly on the **Content Filtering Rules** page. However, you might elect to rearrange the rule. For example, you have a rule that takes an action based on a group membership but want to take some other action for a specific user.

To move that rule above the group rule, select the rule number to display a menu.
The orange triangles indicate that the policy is not yet activated. The Web Security Service also displays policy discrepancies, which you must first resolve.

Click **Activate** to implement the policy.

**Exempt URLs from Permanently Blocked Categories**

The **Group A G1** rule provides a construct for **Permanently Blocked Categories**. By default, **Child Pornography** is permanently blocked (others might be added in the future). It cannot be changed.

But you might have a requirement for specific users or groups to be able to access URLs that belong to a **Permanently Blocked Category**.

1. In the editor menu bar, click **Settings**.
2. In the dialog, select **Allow exemptions to Permanently Blocked Categories in Content Filtering**.
   
   The editor adds a new row designated as **P1**.
3. Click the **Permanently Block Source Exemptions** and/or the **Permanently Block URL Exemptions** links and add exemptions as required.

**Tip**: This topic provides a high-level description of the rules editor. See "**Policy: How Do I?**" on page 152 for use case examples.
Modify the Default Exception Notifications

By default, the Symantec Web Security Service displays an notification page to users when the transaction triggers an exception event, such as a policy violation page when a user attempts to access a website or web application protocol that WSS policy is configured to block. The content of the page includes the result message, such as Access Denied, along with other details, such as the client IP address and the reason (for example, a blocked content filter category).

The WSS allows you to modify this page, including selecting a color scheme, adding contact information and changing the displayed logo and company name. For example, add your IT group email address so that users can contact IT to dispute a rating or ask a question about the policy.

If your WSS account includes the Advanced Web Security with Risk Controls and Web Applications add-on license, the exception includes the Client Location, or country of origin as determined by the service. For more details, see "About Geolocation Policies" on page 11.

The Error ID indicates which policy rule triggered the exception. CF-XX is a content filter rule. TP-XX is a threat protection rule. The exception displays N/A if it cannot determine the rule. Other operations, such as a password override, might cause an N/A.

Tip: You can also modify the template for this page. See "Customize the User Notification Template" on page 161.
Additionally, English, French (European), German, Italian, Japanese, and Spanish (European) language web browsers displays these pages in their respective languages.

**Procedure**

This task requires WSS portal Admin Role credentials.

1. **In Service mode, select** **Notifications**.

   ![Customize contact information.](image)

   a. Select which additional text options to include on the page. In addition to letter and numbers, only spaces and plus signs (+) are valid characters.

   b. Select the page style and color.

   c. Click **Save**.

2. **Enter the** **Company Name** **field** that replaces the current name on notification pages.

   ![Enter your company name.](image)

3. **(Optional) Change the logo** (.png file, 190 pixels x 35 pixels) that displays on exception pages. The default is the Symantec company logo; however, if your company obtained the WSS from a third-party service provider, their logo
might display instead. The logo you add here overrides that configuration.

a. In the **Current Logo** area, click **Change**. The service displays Upload Error Log dialogs.

b. **Browse** to the stored image; select it and click **Open**.

c. Click **Save** in the Error dialog.

To revert to the default file, click **Change** and select **Reset**.

4. Click **Save**.
Note: If the WSS has other pending policy changes, a dialog displays to inform you of this. You can accept to activate all pending policy or navigate to the various policy pages and verify that you want those changes (then return here to save the notification changes).

5. Configure Content Filtering Policy.

Troubleshooting Assistance

You can force the 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, including talking to Support Personnel who speak only English.

- Select Show English Translation Only and click Save.
- When assistance is complete, clear the option.
Customize the User Notification Template

As configured on the Error Pages tab (Service mode > Notifications > Error Pages), the Symantec WSS displays notification pages to users when a browsing action triggers an exception, such as a denied content category. The page contains default information, including the exception reason. You can also select to display information, such as contact information and a custom logo. These notification options should prove sufficient for most enterprise requirements. This information comes from a template, which you can also customize.

Use Cases

- You do not want the notification page to contain specific elements, such as the logo or contact email.
- You want to change the background color or add additional text to an area on the page.

Best Practices

- Symantec considers customizing the notification template an advanced feature. As such, only admin-level WSS users are able to modify the template contents.
- Symantec recommends considerable knowledge of HTML and CSS before performing edits beyond simple string replacements.
- Symantec recommends that you perform only small, deliberate changes to the template rather than recreating a completely new template.
- To avoid display issues, keep the template code compatible with any browser vendor used by employees in your enterprise.
- Certain sections of the template are critical for the page to function properly with other policy elements, such as the Password Override feature. Avoid these clearly marked code sections in the template.
- Do not load content from servers that are outside of your control.
  - JavaScript is running in the page under the context of the page that was blocked and might in some cases have access to sensitive user cookies meant to be kept private. For this reason, avoid loading any third-party hosted JavaScript.
  - Requests to other resources (such as images) might have the Referrer HTTP header present from the page that was blocked, revealing what page the user was visiting when the block page was served. For this reason, avoid loading anything from a 3rd party server.
- When possible, directly include content in the template rather than hosting it on the Internet. This decreases load time and guarantees that a resource is reachable.
  - Base64 images can be encoded directly in the HTML.
  - The template can contain CSS stylesheets.
- The WSS displays the exception page for both HTTP and HTTPS connections. If an image (or some other resource) is referenced in your template using the http:// protocol and the template is used for a page loaded over HTTPS, some browsers might display a warning to inform the user that insecure content was loaded within a secure page. The same might apply in the reverse situation where an https:// resource loads on a page over HTTP. For this reason, Symantec advises to either include the content inline as previously mentioned earlier or perform one of the following.
Host your content both over http:// and https:// and

Use a protocol-less URL to reference it; for example http://example.com/aResource becomes //example.com/aResource. This loads the image over whichever protocol used to load the original page.

The Editor

To view the Custom Notification editor, select **Service mode > Notifications > Custom Error Pages.**

![Custom Error Pages Editor]

- **A**—The **Preview** option allows you to view code changes before they are implemented.
B—Click **Show Replacement Variables** to display all of the code elements that the service uses to populate data.

The variables that begin with `$(config.` are the ones that comprise the default **Error Pages**. These are ones that you can elect to remove from the template.

C—If you run into problems with your edits or you want to start over and create a new template, click Reset to Default HTML, which reverts the template to its default state.

D—When you click **Enable custom error pages**, the system might override any custom edits to the **Notifications > Error Pages**. For example, if you add contact telephone number to the field on that page, but comment out the field in the **Custom Error Page** template, the service does not display the entered phone number. If you clear the **Enable custom error pages** option, the service returns to the default page and any customizations that exist there.

### Examples

The following examples illustrate how you can edit the template.

### Add Text

Supplement the notification with custom text. The following example adds a new line to **Tech support information** drop-down (accessed by clicking **more**).
Click **Preview** to see how the service will display the page.

---

**Remove an Element**

Enter HTML code to comment out an element. For example, you do not want the notification to include detailed transaction information/link. Locate the element in the template and add the comment out code: `<! -- text -- >`. 
IMPORTANT: Some span tag contain the localize attribute. Regardless of any customized text, this attribute instructs the WSS to overwrite with a localized version of the text (including English). To display custom text in a span, you must remove the localize attribute. However, doing so prevents localization.

This line retains the default value because of the localize attribute.

```html
<p id="httpCode"><span localize="[techSupport]">Tech support information</span>: $(exception.id)
```

This line provides the custom text: Tech support information.

```html
<p id="httpCode"><span>Tech support information</span>: $(exception.id)
```

**Customize the Style**

You can enter CSS code to change the appearance of the page. Locate the Symantec styling section.

```html
<!-- This loads default Symantec styling -->
<style type="text/css">
body {
    background-color: blue !important;
    font-color: white;
}
$(bluecoat-template-default.css)
</style>
```

You can also add javascript (above the style section) to add more complex HTML elements.
Malware Policy

Configure the Web Security Service to exempt specific sources, destinations, or web applications from malware scanning.

Malware Policies

- "About Malware Scanning" on page 40
- "Protect Your Network From Web Threats" on page 45
- "Threat Protection Policy Editor" on page 48
- "Malware Policy From Risk Score" on page 50
- "Exempt a Source From Malware Scan" on page 54
- "Exempt a Destination From Malware Scan" on page 58

Web Isolation Solution

- "About Web Isolation" on page 62
- "Enable Web Isolation" on page 66
About Malware Scanning

The Symantec Web Security Service has three levels of malware protection. The first level, Basic, is a tenant of the Web Security Service. The second two require additional licenses and provide deeper malware analysis. The following sections describe these levels for your malware protection consideration.

Tip: For a client-less option, see "About Web Isolation" on page 62.

Base Level

Without any additional configuration, the Symantec Web Security Service provides protection against malware and malicious web content designed to harm networks or obtain private user information. The service leverages the Symantec® Global Intelligence Network™ (GIN), which is driven by a community of users that numbers into the tens of millions. As these users browse web content, scanned content receives a category rating. The database is updated in real time. The Web Security Service policy checks against this database.

The default and unalterable Content Filtering policy prevents access to malicious content websites. These blocked categories are located in these sub-groups:

- Security > Security Concerns: Spam
- Security > Security Threats: Malicious Outbound Data/Botnets, Malicious Sources/Malnets, Phishing, Proxy Avoidance
- Legal Liability > Liability Concerns: Child Pornography

No additional configuration is required. The Web Security Service does, however, enable you to designate trusted sources and destinations that are never scanned for malware.
In the above example, there are two types of users: standard Employees and a Security Specialist. The Web Security Service policy achieves the following:

- An employee makes a request to a site the service rates as a known Phishing site.
- The Security Specialist operates on a subnet (a Trusted Source), which is used to test anti-virus software, that bypasses the default content filtering and malware inspection policy.

Basic Level Protection

- ProxySG/Secure Web Gateway
- Dual Anti-Virus Scanning
- Global Intelligence Network
- URL Filtering and Categorization
- Comprehensive Reporting
SSL Interception/Policy-Based Decryption

(Optional) CASB Audit Integration for web application analysis.

Malware Analysis Standard Service

The Malware Analysis Standard Service (MASS) prevents infection from unknown malware. It blocks malicious content in real-time based on sandboxing resources (Malware Analysis + Content Analysis) that are hosted in Symantec datacenters. This functionality requires an additional license added to your current Web Security Service account. After this entitlement is added to your account, relevant Threats report provides indications of which technology blocked the malware: the standard service Threat Protection (AV) or Malware Analysis (sandbox).

MASS License Protection

In addition to the Base Level, the MASS license provides the following malware analysis.

- Static Code Analysis
- YARA Rules Analysis
- Behavioral Analysis
- Emulation of Windows Processes
- Inline, Real-Time Blocking
- File and URL Reputation

Tip: For this initial standard service, the sandboxing results are from scans against exe and dll content.

Malware Analysis Advanced Service

The Malware Analysis Advance Service (MAAS) license adds more malware analysis capability. While the MASS license provides functionality that always returns results in real-time, the MAAS license adds detonation services that can extend past the real-time sandboxing period.

If the MASS mechanisms (included in MAAS) do not detect malware, the sample is sent to a datacenter for detonation. If malicious behavior is detected within the real-time sandboxing period, the service blocks the file and sends the user an error page.

Because detonation can take longer than the sandboxing period, the service delivers the file to the user after this time while detonation continues in the background. Any post-download detection triggers an administrative alert (email) with the details of the potential client infection (if Malware Analysis Notifications are enabled in the portal; see link below).

Supported Common Documents and File Types

- Windows Installers
- MS Word, Excel, PowerPoint, and Visio files/documents
- Adobe Portable Document Format
- Rich Text Format
- Java Archives
- Android Application Packages
- iOS Application Archives
- Debian/iOS

**Note:** Symantec continues to evaluate and might add more types.

There are no additional configuration options. After the Malware Analysis Standard Service (MASS license) or the Malware Analysis Advanced Service (MAAS license) is added to your account, the relevant **Threats** report provides indications of which technology blocked the malware: the standard service Threat Protection (AV) or the MASS/MAAS (sandbox).
Tip: For this initial standard service, the sandboxing results are from scans against exe and dll content.
Protect Your Network From Web Threats

Without any additional configuration, the Symantec Web Security Service provides a level of protection against malware, or malicious web content designed to harm networks or obtain private user information. The service leverages the Symantec® Global Intelligence Network™ (GIN), which is driven by a community of users that numbers into the tens of millions. As these users browse web content, scanned content receives a category rating. The database is updated in real time. The WSS policy checks against this database.

The WSS provides various levels of malware protection (add-on subscriptions are required for some features). For other details about the service levels, including what is blocked per level, see "About Malware Scanning" on page 40.

The Solutions mode > Threat Protection > Content Analysis page displays the current protection status and provides basic options.

Proxy Analysis

The Proxy Analysis area provides two traffic control toggles that enable you to global web protocol and port restrictions to traffic flowing to the WSS.

- **Protocol Restrictions**—By default, all traffic is sent to the WSS and web use and malware policies are applied to applicable traffic. If you select Restrict Traffic to Web Protocols, only TCP traffic on ports HTTPS 80 and (HTTPS (443) is allowed to reach the WSS; all other protocols are blocked (the clients receive exception screens).

- **Port Restrictions**—Selecting Restricting Web Traffic to Standard Ports limits traffic to web server ports (80/443); that is, the internet side of the transaction, not the client side. You cannot select this option unless Restrict Traffic to Web Protocols is selected.

Content Analysis

The Symantec WSS basic malware services block the types of websites that are the source of viruses and other malicious content. The default and unalterable Content Filtering policy prevents access to malicious content websites. Default blocked categories are located in the following sub-groups:

- **Security > Security Concerns**: Spam
- **Security > Security Threats**: Malicious Outbound Data/Botnets, Malicious Sources/Mainets, Phishing, Proxy Avoidance
- **Legal Liability > Liability Concerns**: Child Pornography
No additional configuration is required. The WSS does, however, enable you to designate trusted sources and destinations that are never scanned for malware.

Malware Analysis

For more in-depth malware scanning obtain one of the add-on Malware Analysis licenses.

- The Malware Analysis Standard Service (MASS) prevents first-client infection from unknown malware.

- The Malware Analysis Advance Service (MAAS) adds detonation services that can extend past the real-time sandboxing period, plus email notifications for post-downloaded threats. To add one or more email addresses, navigate to Solutions mode > Threat Protection > Content Analysis and expand the Malware Analysis area.

Enter emails (separated by commas) and click Save.

For full details, see "About Malware Scanning" on page 40.

Malware Exemptions and Policy

You might have a need to exempt some traffic from malware scanning or a specific level of scanning. For example, scanning interferes with your testing on a specific network segment.

- "Exempt a Source From Malware Scan" on page 54

- "Exempt a Destination From Malware Scan" on page 58

Use the Threat Protection Policy Editor to customize your protection strategy.

- "Threat Protection Policy Editor" on page 48
With the Advanced Web Security with Risk Controls and Web Applications add-on license, you can allow or block access to content that has been rated Cautionary Risky, Moderately Risky, or Risky levels. You can also define custom risk score-based policy.

- "Malware Policy From Risk Score" on page 50

Geolocation-Based Policies

If your Web Security Service portal account is provisioned with the Advanced Web Security with Risk Controls and Web Applications add-on license, you can base malware scanning policies from what country the request originates (Add Sources > Geolocation construct) or to what country the request is destined (Add Destinations > Geolocation construct). See "About Geolocation Policies" on page 11.

Web Isolation

Web Isolation is a client-less solution that enables employees to safely browse the internet on any device using any browser. See "About Web Isolation" on page 62.
Threat Protection Policy Editor

By default, the Web Security Service blocks access to known risky content categories (this varies depending on which Default Policy level you or another admin selected during the initial configuration process).

Use the Threat Protection Policy Editor to further customize your protection strategy. If you or another admin previously applicable lists (such as in the Overview > Object Library), the policies already include them. Each blue link in the editor enables you to perform changes to that element. For example, you might—

- Elect to have a stronger file type protection strategy for mobile users.
- Allow specific users or groups access to permanently blocked categories.
- Allow access to uncategorized content.
- Define policies that depend on multiple conditions. For example, the rules triggers if for a specific group that accesses from a specific location (AND construct). You can also create OR constructs.

Tip: If your account has provisioned the Advanced Web Security with Risk Controls and Web Applications add-on license, you can define policy based on Risk Scores. See "Malware Policy From Risk Score" on page 50.

1. In Service mode, select Threat Protection > Policy.

   The Threat Protection Policy Editor contains policy rows grouped by A and B.
   - A—These rules do not depend on content returned from the destination.
   - B—These rules might depend on returned content.

2. Each row labeled with G# has a purpose in its order. Roll over each tool tip icon to understand how the rule interacts with the overall policy.
Each blue link enables you to perform changes to that element. If you or another admin previously applicable lists (such as in the Overview > Object Library), the policies already include them. For example, the above screenshot has a list added to the Risky File Type Source Exemptions in rule G4.

3. To create a rule, click Add Rule. The editor displays the constructs page (Conditions and Verdict).

   - Click Add Sources, Add Destinations, and Content and Limits to add the elements to the rule. You can create AND/OR constructs to make the rule conditional on multiple elements.

   **Tip:** For a more detailed tutorial on how to use this editor. See "About the Content Filtering Rule Editor" on page 18.

   - The Verdict is the action to take on triggered rules: Allow or Block (the Web Security Service displays an exception page on the client system or device).

   **Note:** If your account has the Web Isolation license, the Block verdict has a sub-option to Block unless Isolated. Selecting this means traffic that triggers Web Isolation policy is not blocked by this policy. See "Enable Web Isolation" on page 66.

4. Click Add Rule. The Web Security Service places the rule in the correct order.

5. Click Activate.
Malware Policy From Risk Score

The Symantec Global Intelligence Network (GIN) provides datafeeds that contain content category risk ratings to the Web Security Service. The risk rating ranks from 1 to 10 and has the following labels.

<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2</td>
<td>Content is <strong>Very Likely Safe</strong>. Sites have a proven history of proper behavior.</td>
</tr>
<tr>
<td>3-4</td>
<td>Content is <strong>Likely Safe</strong>. Sites are beginning to establish a history of proper behavior.</td>
</tr>
<tr>
<td>5-6</td>
<td>Content is <strong>Cautious</strong>. Possibilities exist that the sites might not be yet be proven to be safe.</td>
</tr>
<tr>
<td>7-8</td>
<td>Content is <strong>Suspicious</strong>. Evidence exists that the sites are possibly malicious.</td>
</tr>
<tr>
<td>9-10</td>
<td>Content is confirmed as <strong>Malicious</strong>. Solid evidence that the sites are malicious.</td>
</tr>
</tbody>
</table>

By default, the Web Security Service blocks categories such as **Phishing**, but other categories can contain malware sources. For heightened security, many organizations opt to block anything with a risk rating 7 or above. With the Advanced Web Security with Risk Controls and Web Applications add-on license provisioned to your account, you can use the Threat Protection Policy Editor to define more granular risk rating policy.

Consider the following use cases that demonstrate how risk score policy can be of benefit.

- The **Marketing** group might have a more lenient web access policy applied to it because they browse more for research; therefore, you want to set its risk score block level to 6.
- You want any request sent to (or from) specific countries to block any risk score 6 and above.
- Content policy previously blocked the **Uncategorized** category; however, too many false-positives occurred. Now you can block all access to the **Unrated** and other categories that present similar behaviors (for example, **Advertising**) that is risk level 5 and above.
- Block specific file types with a risk rating of 4 and above.
- Your security suite includes the Universal Policy Enforcement (UPE) solution. You have created risk rating policy on your on-premises ProxySG appliance. The Web Security Service accepts that policy when delivered from Symantec Management Center.

Defining risk score policy is the same as described in "Threat Protection Policy Editor" on page 48. After your account is provisioned with the Advanced Web Security with Risk Controls and Web Applications add-on license, the editor displays default rows that contain risk scores.
By default, the Web Security Service provides three Group A rows with Cautionary (6), Moderately Risky (7), and Risky Levels (8-10). By default, these default risk level rules are set to a Block verdict. If your portal account has the Web Isolation add-on license, the default for Cautionary (6) and Moderately Risky (7) is Block Unless Isolated.

You can add other constructs to these rows. The exception is File Types in Contents and Limits because they rely on responses from content servers and thus need to be in Group B.

**Note:** If you or the Admin who performed the Web Security Service account registration process selected High Security as the Default Policy, the Risk Levels are different.

Each row labeled with **G#** has a purpose in its order. Roll over each tool tip icon to understand how the rule interacts with the overall policy.

With the license, the Add Destinations construct now includes a Threat Risk Level element.
The blue-linked default levels are modifiable (name and level values).

You can create a new Risk Level object to apply to specific Sources.

Web Isolation Policy Based on Risk Score

If your Web Security Service account has provisioned the Web Isolation add-on license, you can force content with a specific risk score to be processed in isolation.

Risk Score Reporting

The Web Security Service provides several default reports based on risk scores.

On the Solutions mode > Threat Protection > Reports page, the Security area provides several default reports.

- Trend of Risk Distribution
- Trend of Overall Risk
- Risky Sites Per Country
- Risky Clients Per Country
- Risk Distribution—Pie chart showing percentage of each rating level for a given time frame.
- Riskiest Users—List of users with highest numbers of requests scored over or equal to Risk Score 7. (PDF report not available.)
- Risky Sites Not Blocked—Top sites not blocked with score over or equal to 7

Exempt a Source From Malware Scan

The Web Security Service allows you to exempt web requests from specific sources from malware scanning. Furthermore, you can select the level of scanning for those sources.

Exemptable Sources

You can exempt:

- Specific IP addresses and subnets—Use Case: You might have a list of client systems whose responsibilities exempt their requests from Symantec Web Security Service malware scanning. For example, you have a Security Specialist who requires unabated web access. There are two methods: manually enter an IP address or subnet or define a list in a text file (one entry per line) and import that list.

- Locations—If you do not require granular exemptions, you can exempt an entire location. For example, a micro-branch office connects to the Web Security Service through the Explicit Proxy access method.

- A client IP address or subnet listed as a Trusted Source also causes the Web Security Service to disable Protocol Detection for requests coming from this Trusted Source. Even if SSL Interception is enabled, the service does not intercept any HTTPS (SSL) traffic requested by this source, which might cause unintended policy misses.

Exemption Levels

By default, the Web Security Service exempts the source from the following malware scanning processes.

- **Anti-virus engine scanning**
- **Malware Analysis** (if the account has the MASS or MAAS license)

If the account has the MASS or MAAS license, you can elect to not apply **Malware analysis** or **Malware analysis** and **Anti-virus engine scanning**.

**Procedures**

1. In Solutions Mode, select the **Threat Protection > Content Analysis** link; expand the **Scanning Exemptions** area.

2. The interface provides the following methods to add exempted sources.

   - Click the **Trusted Source IP/Subnets** link—This is the default link/object.
   - Click any other existing link created by you or another Web Security Service Admin.

     Either of these display the Object dialog from which you can add or import trusted (exempt) IP addresses.

   - Click **Add** to create a new object. From this dialog, you can also add new IP addresses and locations plus create combined objects from existing objects. The remainder of this procedure demonstrates this method.

3. (Option 1) Create a combined object from existing objects. If you created custom objects in the Object Library (Overview > **Object Library**), they are available for selection.
a. Click **Add**. The portal displays the Add Exempted Sources dialog.

![Add Exempted Sources dialog](image)

b. Select existing objects.

c. Click **Add** to move them to the **to be added** field.

d. Verify/select the malware scanning levels that are *not* performed against this source.

e. Click **Add**.

4. **(Option 2) Create a new object.**

   a. Click **Add**. The portal displays the Add Exempted Sources dialog.
   
   ![Add Exempted Sources dialog](image)

   b. In the dialog, click **New** and select what to add.
Location or IP/Subnet List—Displays entries from your Object Library or create a new list from selections; can also select entries detected by an already-run report.

Location—Define a new location and Access Method. For example, you want to test and need to create an Explicit Proxy location.

IP/Subnet—Add or import IP addresses.

c. Click Save.

d. Add more objects or click Add.

5. Click Activate.

Change Exemption Scanning Level

For any exempted source, you can change the Malware Scanning Level, which are described in "Exemption Levels" on page 54.
a. Select a source object.

b. Click **Change Exemption Level**.

c. The dialog contains a show selected… link, which displays all of the objects in the current rule. The screenshot above reflects this selections.

d. Select a different level and click **Save**.

e. Click **Activate**.

**Next Step**

- "Exempt Files From Error Handling" on page 61
- Return to "Protect Your Network From Web Threats" on page 45.
Exempt a Destination From Malware Scan

The Web Security Service allows you to exempt web requests from specific sources from malware scanning. Furthermore, you can select the level of scanning for those sources.

Exemptable Destinations

You can exempt:
- Specific IP addresses and subnets—Use Case: Your employees routinely access information stored on an external server that is not otherwise connected to the Internet.
- Domains/URLs—Use Case: Your employees routinely access information from a secure partner site.
- Categories—Use Case: You have a collection of categories that you want scanned only for risky files.
- Web Applications—Use Case: You feel financial applications, such as E*Trade, do not require malware scanning.

Exemption Levels

By default, the Web Security Service exempts the destination from the following malware scanning processes.
- Anti-virus engine scanning
- Malware Analysis (if the account has the MASS or MAAS license)

If the account has the MASS or MAAS license, you can elect to not apply Malware analysis or Malware analysis and Anti-virus engine scanning.

Procedures

1. In Solutions Mode, select the Threat Protection > Content Analysis link; expand the Scanning Exemptions area.
2. Click the Destinations tab.
3. The interface provides the following methods to add exempted sources.
   - Click the Trusted Destination IP/Subnets, Domains/URLs, or Web Applications link—These are default links/objects.
   - Click any other existing link created by you or another Web Security Service Admin.
     Either of these display the Object dialog from which you can add or import trusted (exempt) IP addresses.
   - Click Add to create a new object. From this dialog, you can also add new IP addresses and locations plus create combined objects from existing objects. The remainder of this procedure demonstrates this method.
4. (Option 1) Create a combined object from existing objects. If you created custom objects in the Object Library (Overview > Object Library), they are available for selection.
a. Click **Add**. The portal displays the Add Exempted Destinations dialog.

![Add Exempted Destinations dialog](image)

b. By default, the dialog displays all object types. To narrow the field, select a type from the **All Types** drop-down list.

c. If you know the name of the object, enter it (or any other keyword) in the search field.

d. Select existing objects.

e. Click **Add** to move them to the **added** field.

f. Verify/select the malware scanning levels that are *not* performed against this source.

g. Click **Add**.

5. (Option 2) Create a new object.

   a. Click **Add**. The portal displays the Add Exempted Destinations dialog.

   b. In the dialog, click **New** and select what to add.
- **Category/URL/IP Subnet/Web Application List**—Displays entries from your Object Library or create a new list from selections; can also select entries detected by an already-run report.

- **URL or IP/Subnet**—Add or import URLs or IP addresses.
  
  c. Click **Save**.

  d. Add more objects or click **Add**.

6. Click **Activate**.

**Next Step**

- "Exempt Files From Error Handling" on page 61

- Return to "Protect Your Network From Web Threats" on page 45.
Exempt Files From Error Handling

Some files are rejected by ICAP error detection based on their type. For example, malware scanning routinely rejects password-protected archives. The Web Security Service allows you to exempt specific file types from ICAP error handling and allow them to continue to the client.

**Tip:** Currently, Password Protected Archives are the only supported type. Future service updates will add more types.

1. In **Solutions** mode, select **Threat Protection > Content Analysis**.
2. Scroll down to **Scanning Error Handling** and click **Add Scanning Error Exemption**. The portal displays the Exemption Rule dialog.
3. (Optional) Click **Add Sources** and define that construct.
4. (Optional) Click **Add Destinations** and define that construct.
5. Click **Add Error Type**. Currently, only **Add Password Protected Archives** is available. Click it and click **Save**.

**Example rule:**

7. Click **Add Rule**.

7. Click **Activate**.
About Web Isolation

Web Isolation is a client-less solution that enables employees to safely browse the internet on any device using any browser. The zero footprint negates the need for software installation on the clients. The Symantec Web Isolation feature requires a license. If after reading this section you want to enable this Web Security Service feature, contact your Symantec sales representative.

What is Web Isolation?

IT departments invest large amounts of resources to protect employees and assets from malicious activity. The most common element of cyber-security solutions is detection. Anti-virus/malware, network sandboxes, next-generation firewalls, web application firewalls—all depend on detection. In some cases, such as sandboxes, notification of malicious content arrives to the admin after the user has received the content because of the time required to ascertain the verdict. Detection of threats through IOCs and other signatures is necessary to protect against known threats, but in the arms race to apply new attack/exploits, detection by itself is insufficient.

The Symantec Web Isolation solution addresses this security weakness. Instead of relying on malware detection, Web Isolation protects organizations’ end users from cyber attacks by isolating malware and preventing it from reaching end user browsers. A common use case is to protect employees who browse uncategorized and potentially malicious sites.

Web Isolation:

- Provides a safe visual stream of the original web site in the user’s browser.
- End users browse the site as if the site was running directly in the browser.
- Preserves original browsing experience with full usability and control.
- Only safely rendered information arrives at the user’s browser.
- Web Isolation executes web sessions away from endpoints.

Protect Endpoints from Attack

As stated above, Web Isolation executes web sessions away from endpoints, sending only safely rendering information to users' browsers, thereby preventing malware from reaching your network and devices. Web pages are rendered and isolated as graphics for display on the end user’s browser.

- Isolating websites, emails, and documents so that no malicious content can ever reach the end-point.
- Preventing malware and fraud.
- Protecting against drive-by infection, malvertising, and ransomware.
- Blocking malware Command & Control (C&C), and exfiltration communication.
Topography

1–Client initiates a web request.

2–You define policy rules that contain Who, From Where, To Where, and Verdict criteria. Policy that you define on the proxy asset in the Web Security Service determines that this traffic—to uncategorized content for example—requires isolation.

3–On the Web Security Service datacenter asset, the Threat Isolation Engine (TIE) in the data center asset runs the website within a secure disposable container. Simultaneously, the Web Security Service returns safely rendered information to users' browsers. This occurs over a secure web socket. The employee can still scroll, navigate, and enter keystrokes. However, no possibly malicious content, including browser-based exploits, reaches the client browser.

4–TIE retrieves the requests from the content servers.

5–The client browser is allowed to continued (rendered) site access.

6–If Web Isolation detects malicious content:

- Malicious content is blocked by content scanning service.
- Malicious content is eliminated by Web Isolation because of true type validation or rendering failure.
Website Data

The website data remains in the Web Security Service Web Isolation containerized environment, which is disposed of after the browser session. However, you can view reports that track isolation activity.

About the Two Web Isolation License Types

As previously stated, the Web Isolation feature requires a Symantec add-on license. The license is available in two levels.

- **Selective Isolation**—Allows for about 5% of web traffic per subscribed seat for isolation. The Selective Isolation license must apply to all seats in your Web Security Service contract.
- **Full Web Isolation**—You can extend this license to some or all subscribed seats. Grants 100% isolation per subscribed seat.

Both licenses provide Risk Level-based policy (Threat Level Risk object in the Destinations construct).

Contact your Symantec sales representative.

**Tip:** An expired Web Isolation license results in the Web Security Service ignoring the rules defined in the policy editor.

Geolocation—The Advanced Web Security Add-On

If your Web Security Service account has provisioned the Advanced Web Security with Risk Controls and Web Applications add-on license, you gain isolation based on geolocation Sources. For example, you want the Web Security Service to isolate all traffic when the request originates from specific countries (applies to non-fixed Locations only). See "About Geolocation Policies" on page 11.

About Web Isolation and UPE

If you are using Symantec Management Center to manage Web Security Service policy (the Universal Policy Enforcement solution), you can add policy that directs susceptible traffic to Web Isolation. See "About Web Isolation With UPE" on page 71.

About Web Isolation Operations

**Use Cases**

- By default, Web Isolation policy applies to the To Where policy to the Uncategorized and/or Suspicious categories.
- Document isolation occurs on files that originated in browsing sessions.

**Support**

Minimum compatible browser versions:

- Chrome 56
- Edge 38
- Firefox 54
- Internet Explorer 11
- Safari 11

Supported Operating Systems:
- Windows 7+
- Mac OS Sierra+

Traffic
- Ensure that the Web Security Service root certificate is installed on all clients. For clients with Unified Agent on the endpoints, this is automatically installed and applied to Internet Explorer, Edge and Google Chrome. If your organization uses Firefox or another browser that has its own certificate store, this certificate must to be installed directly into that web browsing application.
- Enable SSL Interception in the Web Security Service portal to enable isolation of SSL traffic.
- The policy enforcement hierarchy is **Block > Isolate > Allow.**
- If web security policy is to block a category, URLs associated with that category are not susceptible to isolation.
- Currently, DLP and CASB functionalities on isolated traffic might be incomplete.
- Currently, Web Isolation is not available for Universal Policy Enforcement (UPE) deployments or on mobile devices.
- Because isolation is serving the site representation over the web socket, policy is not applied to the **content** of the HTML responses.
- Uploads/Downloads—Isolation traffic ignores the following operations.
  - Block file download from a specific URL / category.
  - Block file upload to a specific URL / category.
  - Threat prevention exemption based on destination address.
- If your organization uses Skype for Business (SfB) under the following conditions:
  - You have a private SfB server.
  - SSL Interception is enabled.

Then you must bypass the private URLs for SfB/Lync from SSL interception. If you do not, the app hangs.
Enable Web Isolation

Web Isolation protects organizations’ end users from cyberattacks by isolating malware and preventing it from reaching end user browsers.

Prerequisite—Obtain License

Web Isolation requires one of the add-on licenses.

- **Selective Isolation**—Allows for about 5% of web traffic per subscribed seat for isolation.
- **Full Web Isolation**—You can extend this license to some or all subscribed seats. Grants 100% isolation per subscribed seat.

Prerequisite—Install Root Certificate

- Ensure that the Web Security Service root certificate is installed on all clients. For clients with Unified Agent on the endpoints, this is automatically installed and applied to Internet Explorer, Edge and Google Chrome. If your organization uses Firefox or another browser that has its own certificate store, this certificate must to be installed directly into that web browsing application.

You can download the certificate from the SSL Interception page or the **Solutions** mode > **Threat Protection** > **Web Isolation** page.

Optional Prerequisite—Enable SSL

- To isolate HTTPS traffic, enable SSL Interception (**Service** mode > **Network** > **SSL Interception**).

  Examine Encrypted (HTTPS) Traffic

Optional Prerequisite—Custom Lists

Use the **Overview** > **Object Library** to define list objects—such as user/group lists, categories, destinations—to be used in Threat Isolation policy.

Reference—Egress IP addresses

- If you have firewall rule considerations, refer to **Reference: Egress IP Ranges**.

Procedure

**Tip:** The following procedure demonstrates defining policy that applies Web Isolation. Performing the same steps, you can also define policy that exempts traffic from Threat Isolation.

**Step 1—Enable Web Isolation**

1. Navigate to **Solutions** mode > **Threat Protection** > **Web Isolation**.
2. Select the **Disabled/Enabled** toggle.
Step 2—Define an Isolation Policy Rule

1. Click Add Rule. The editor displays the constructs page (Conditions and Verdict).

2. Click Add Sources.

   For example, you want Web Isolation applied to all Unauthenticated Users and specified Groups.

   **Tip:** You can also create AND conditions, which means the rule triggers when both conditions are met.

   Click Save.

3. Click Add Destinations.
For example, you want to add **Social Networking** categories.

4. The final page, **Verdict**, defines the Threat Isolation action.
   - **Isolate**— The Web Security Service executes the web request in a secure, isolated environment and performs Web Isolation malware scanning.
   - **No Isolation**— The Web Security Service bypasses Web Isolation and serves the response as the full web content.

5. Click **Add Rule**. The Web Security Service adds the Web Isolation policy rule.

6. Click **Activate** to enable the rule.

**Isolation Based on Risk Scores**

If your Web Security Service account has provisioned the Advanced Web Security with Risk Controls and Web Applications add-on license, you can force content with a specific risk score to be processed in isolation.
Monitor Licensed Capacity

As the service begins to process web traffic and perform Threat Isolation, your portal account tracks the activity. You can review the amount of Threat Isolation that has occurred against the capacity deemed by your license.

In the upper-right corner of the Threat Protection > Web Isolation page, click the highlighted percentage element. The portal displays the Isolation License Details dialog.

The above screenshot reflects a newly activated license. As more activity occurs, the Projected Isolation Usage area expands with more data. Roll over graph elements for more data.

Web Isolation Reporting

As traffic begins to undergo Web Isolation, you can review numerous related reports. These reports are on the Solutions mode > Threat Protection > Reports page.
Skype for Business Issue

If your organization uses Skype for Business (SfB) with the following deployment:

- A private SfB server; and
- This SfB server is susceptible to traffic isolation;

Then you must exempt the private SfB/Lync URLs from Threat Isolation policy to prevent the SfB from becoming unresponsive. Add a Do Not Isolate rule as described in Step 2.
About Web Isolation With UPE

Web Isolation is a client-less solution that enables employees to safely browse the internet using any browser.

The Web Security Service supports integration with Symantec Management Center in a solution called Universal Policy Enforcement (UPE). This allows you to author policy locally (with ProxySG appliance/Management Center) and determine which traffic goes to the Web Security Service where the centralized, cloud-based policy implements Web Isolation.

Technical Requirements

Before implementing the policy provided in this topic, ensure the following technical requirements are met.

- You have an existing Universal Policy Enforcement (UPE) implementation; that is, the Visual Policy Manager (VPM) has policy designated for Web Security Service upload. This topic does not contain initial UPE configuration procedures.

- Your Web Security Service has the Web Isolation license (Selective or Full). Without the license, the policy objects are suppressed.

Limitations

- The user and group names in UPE policy must match the user and group names authenticated in the Web Security Service.

Supported Deployments

There are two deployment variations to achieve Web Isolation through UPE.

Deployment Use Case—Existing Web Isolation On-Premises/Service

In this deployment, there is an existing Web Isolation solution that is either an on-premises Symantec Web Isolation platform or a Symantec Web Isolation service account. Policy on the Symantec Secure Web Gateway determines what traffic is susceptible to isolation. You want to use Management Center to push that existing Web Isolation policy to the Web Security Service.
A—Web Isolation on-premises deployment: a Symantec Secure Web Gateway appliance (ProxySG or ASG) interacts with either an on-premises, dedicated Symantec Web Isolation platform or a Web Isolation service.

B—The Web Security Service interacts with a Symantec Web Isolation cloud service (dedicated or shared).

1—The Admin uses the Web Isolation Management UI to determine which traffic is susceptible to isolation based on criteria such as risk score, category, destination. The Management UI generates a Secure Web Gateway policy template. The Admin uses Management Center to push that template to the Web Security Service.

2—An on-site employee issues a web request that triggers Web Isolation.

3—The Threat Isolation Engine (TIE) in the data center asset runs the website within a secure disposable container.

4—The client browser is allowed to continued (rendered) site access while content scanners perform.

5—In the above example, remote clients connect to the Web Security Service. The same traffic is sent to Isolation based on the defined criteria (flow step 1). The Web Isolation service performs the same disposable container and rendered site tasks. You might have also on-premises connections, such as from an IPsec or explicit proxy location.

Note: The Web Security Service can forward to only the Web Isolation cloud service. Forwarding to an on-premises environment is not supported.

Perform This Option?

As mentioned above, the Web Isolation platform has the policy (Content Policy Language—CPL). The Symantec Threat Isolation platform documentation has more details about how to retrieve this.
The chapter is *Integration with a Downstream Proxy*.

**Deployment—Web Security Service Web Isolation Policy**

In this deployment, you do not have any existing proxy forwarding to an isolation product. You want to solely leverage the Web Security Service; however, you are using UPE to manage Web Security Service policy and want to include Web Isolation.

---

**A**—Web Isolation deployment: The Web Security Service interacts with a Symantec Web Isolation cloud service (dedicated or shared).

**B**—Symantec Management Center determines which traffic goes to the Web Security Service.

1—The Admin adds an isolation policy template to a CPL Layer and determines which traffic is susceptible to isolation based on criteria such as risk score, category, destination. The Admin uses Management Center to push that template to the Web Security Service.

2—An on-site employee issues a web request that triggers Web Isolation.

3—The Threat Isolation Engine (TIE) in the data center asset runs the website within a secure disposable container.

4—The client browser is allowed to continued (rendered) site access while content scanners perform.

5—In the above example, remote clients connect to the Web Security Service. The same traffic is sent to Isolation based on the defined criteria (flow step 1). The Web Isolation service performs the same disposable container and rendered site tasks. You might have also on-premises connections, such as from an IPsec or explicit proxy location.
Perform This Option?

- Proceed to "Web Isolation Policy Template" on page 75.
Web Isolation Policy Template

As described in "About Web Isolation With UPE" on page 71, you can use Symantec Management Center add policy that dictates the traffic that the Web Security Service sends to Web Isolation. This solution applies if do not otherwise have a current on-premises Symantec Web Isolation platform. You must implement a policy template.

Technical Requirements

Before implementing the policy provided in this topic, ensure the following technical requirements are met.

- You have an existing Universal Policy Enforcement (UPE) implementation; that is, the Visual Policy Manager (VPM) has policy designated for Web Security Service upload. This topic does not contain initial UPE configuration procedures.
- Your Web Security Service has the Web Isolation license (Selective or Full). Without the license, the policy objects are suppressed.

About the Policy Objects

Two filter objects (conditions) comprise the policy that determines what traffic is susceptible to routing to the Web Security Service for possible Web Isolation. These conditions are called Isolation Match Criteria. Both are required as part of the policy.

- `<Proxy>` layer–Isolation_CondWebIsolationMatchCriteriaWebAccess
- `<Forward>` layer–Isolation_CondWebIsolationMatchCriteriaForwarding

Each layer evaluates each condition to determine if traffic is to be isolated.

UPE and Web Isolation Policy Template

1. Use Management Center to access the VPM.
   - Create a new CPL layer and name it (for example, Web Isolation).
2. Copy the policy template below to a file.
3. Paste the policy into the layer (or in a notepad first to refine, then copy over).
4. Modify the policy to match your testing or solution goals.
5. Save the layer and Install the policy. Distribute to the appropriate Secure Gateway appliances.

Template

You must use the same criteria in each condition (WebAccess and Forwarding). Also, the Isolation_CondWebIsolationMatchCriteriaWebAccess object must use url gestures and the Isolation_CondWebIsolationMatchCriteriaForwarding object must use server_url gestures.

```csharp
;; Begin Template
#if enforcement=wss
define condition Isolation_CondWebIsolationMatchCriteriaWebAccess
;url.threat_risk.level=7..10
;url.category=\"Malicious Outbound Data/Botnets\",\"Suspicious\"
;url.domain=\"malicious.com\"
;authenticated=yes
;client.address=192.168.10.0/24
```
;authenticated=yes url.category="(Malicious Outbound Data/Botnets)"
end

define condition Isolation_CondWebIsolationMatchCriteriaForwarding
;server_url.threat_risk.level=7..10
;server_url.category="(Malicious Outbound Data/Botnets","Suspicious")
;server_url.domain="malicious.com"
;authenticated=yes
;client.address=192.168.10.0/24
;authenticated=yes url.category="(Malicious Outbound Data/Botnets)"
end

; This should be conditioned but is required for Isolation
<SSL-Intercept> condition=Isolation_CondWebIsolationMatchCriteriaWebAccess
ssl.forward_proxy(https)
#endif
;; End Template

The #if enforcement=wss clause ensures this code block is only applicable to Web Security Service deployment. The conditions are tests for routing to the Web Security Service Isolation facility.

Notice that all of the criteria gestures are commented out with a semi-colon ;. You must elect which ones to enable (delete the ;) and edit the line to craft your policy. For example, the template sends the Malicious Outbound Data/Botnets and Suspicious web categories to Web Isolation. You can replace those or add additional per the format.

About SSL Interception of Mobile Traffic (UPE)

The Web Security Service provides a policy wizard that enables you to determine which traffic is susceptible to SSL Interception. You can define SSL policy specifically for traffic generated from mobile devices. If you have enabled SSL Interception globally (without exceptions), Symantec recommends that you disable interception of mobile device traffic to avoid known issues caused by app use of locked/pinned certificates.

Create a pre-defined object:

```plaintext
define condition WSS_AccessViaMobile
#if enforcement=wss
     client.location.access_type=mobile_device
#endif
End
```

Add an SSL layer condition:

```plaintext
<SSL>
Condition=WSS_AccessViaMobile ssl.forward_proxy(no)
</SSL>
```

About Failure Modes

By default, the Web Isolation forwarding policy is Fail Closed. That is, if the forwarding process cannot connect to the Web Isolation service, the request is refused and the client receives an exception notification.

You can elect to set to Fail Open. However, be advised that it will difficult to distinguish whether or not a browser is operating in isolation.

```plaintext
<forward>
forward.fail_open(yes) ; UPE isolation will be fail open
</forward>
```
Web Application Policy

Delete this text and replace it with your own content.

- "About Controlling Web Application Access" on page 78
- "About the CASB Integration" on page 81
- "Integrate With CloudSOC (CASB)" on page 84
- "Set Default Web Application Policy to Allow" on page 89
- "Set Default Web Application Policy to Block" on page 91
- "Define a User-Based Web Applications Policy" on page 93
About Controlling Web Application Access

Web applications are vital to enterprise operations, yet also present challenges. You must balance the availability of various applications required for business with security and your employee web acceptable Use policies. The Symantec Web Security Service provides three methods to control web applications access. A combination of these methods allows you to create a robust, yet targeted policy that both protects your employees while allowing them to perform their business tasks.

Always Block or Always Allow a Web Application

This policy option applies to all employees. The Web Security Service blocks all attempts to access specific web application destinations; or conversely, the service always allows access to specified web application destination.

Allow a Web Application But Block an Action

You can allow everyone access to specific Web Applications, yet prevent actions from within those applications. For example, you allow Facebook access, but want to prevent video uploads to Facebook—an action that consumes valuable network resources.
Define Who Can Access Web Applications

If your enterprise contains multiple users, groups, and roles, you will more than likely elect to define granular web application policy. The Web Security Service allows you to specify who can access a web application, when they can access it, and what happens if they are not allowed access. For example, you have different user groups with different requirements. The Marketing group requires access to Facebook and Twitter; the HR group requires access to Facebook and Linkedin. Other groups are blocked access to those applications.
Web Application Category Reference

For the current list of web applications that the Web Security Service recognizes, see the following article.


Want to configure Web Application policy?

- Proceed to Control Access to Web Applications.
- CASB Audit: "About the CASB Integration" on page 81.
About the CASB Integration

The Web Security Service is an integrated platform for Content Filtering, Threat Protection, DLP, and CASB deep-controls on cloud applications. The Symantec CASB platform, CloudSOC™, provides visibility to over 24,000 cloud applications plus over 60 attributes per application. This enables scalable policy to control Shadow IT and cloud application access.

After completing the one-time WSS-to-CloudSOC integration, you can apply a combined policy enforcement to both platforms based on their respective configurations for all enabled application Gatelets.

CASB Topography

This topography assumes that you have obtained the CASB/CloudSOC product.

1—A WSS admin links the WSS and CloudSOC accounts through a unique Integration ID. After launching CloudSOC from the Web Security Service portal, the Admin enables application Gatelets—for example, Yammer, Google Drive, Box. Within the Gatelets are additional options, such as domains.

2—When Gatelet configurations are saved, the WSS receives a list of applications subject to CASB deep control.
3—Regional employees (on campus or remote) perform requests for web application destinations. The WSS processes the policy; allows or denies the content; and adds entries to the access logs. The WSS uses these access logs for report generation.

4—Over a secure connection, an API connects the WSS to the CloudSOC. The WSS forwards the access logs to the CloudSOC Audit.

5—Admin or WSS user in the Reporting Role accesses the WSS portal; from there, launches the CloudSOC portal, which opens in a separate browser tab. In CloudSOC, users can generate reports.

**Note:** The WSS remains in sync with the Symantec Global Intelligence Network (GIN). Updates to the database occur each day.

About the Traffic Evaluation Order

The following summarizes how the WSS and CloudSOC prioritizes and evaluates traffic according to behavior. When possible, all behaviors are applied; the order addresses conflicts.

This graphic demonstrates the policy and service order when the WSS receives a request. There are two scenarios—A (no CASB Gatelet) and B (redirected CASB Gatelet).

- Denial and blocking based on **policy Allow/Deny rules** configured in the WSS portal or from Universal Policy Enforcement (UPE) uploaded policy rules.
  
  For security and compliance reasons, explicit denials (for Content Filtering or Threat Protection) must be applied.

- **Authentication** verifies the logged-in employee credentials.
SCENARIO A

- **SSL Intercept** except for exemptions configured in the Web Security Service portal.

  Explicit SSL exemptions (for example, traffic to **Healthcare** categories) are assumed to be defined by an organization's legal compliance.

- **Malware scanning** and **Sandboxing** (with Advanced license).

- **DLP** scanning (with license).

- **Web Isolation** (if licensed) forwarding.

SCENARIO B

Applications routed to CloudSOC (CASB Gateway) over ICAP service.

- **Authentication**

  Gatelets only work for WSS connectivity methods where the end user must authenticate. For example, if an endpoint accesses through explicit proxy with no authentication, the CASB Gatelet policy enforcement is ignored.

- **SSL Interception**

  When enabled Gatelet matches, the WSS forwards the traffic to CloudSOC, regardless of the SSL Interception setting.

- **WSS-applied DLP** and **Malware** scanning.

  As CASB Gatelets include Symantec content analysis and integration to Symantec DLP, material can be exempted from WSS processing of those types.

The primary use cases for CASB Gatelets and Isolation are parallel. The Web Isolation service is focused on risky/unfamiliar sites, while CASB Gatelets are by definition for sanctioned applications. The population of sanctioned applications is smaller, thus this remains lower in the order because the account has enabled CASB.

**Current Limitations**

- O365 Gatelet—WSS global O365 SSL exemption is overridden for specific destinations.

- O365 Gatelet—File Sharing Block policy is ignored for the Desktop O365 Apps (OneDrive for Business, Word, Excel, Powerpoint).

  For example, if the file sharing block policy is in place and a user is attempts to share the files (already synced to OneDrive) to another user/group, the files are allowed instead of blocked.

- Google Drive Gatelet—Similar to the Office 365 issue, uploads from Google Drive are allowed despite blocking policy in pace.

- Clients with Unified Agent installed are not able to login to Outlook. The credential dialog repeats.
Integrate With CloudSOC (CASB)

After you obtain the CASB license, you must perform the task to integrate the Web Security Service with the CloudSOC portal.

Technical Requirements

- When you purchase the CASB license, the admin on record receives an e-mail from Symantec that contains the Integration ID. You must have this ID to register. The Integration ID is not the same number as your Web Security Service Subscription ID.
- This procedure describes how to integrate with an existing CloudSOC portal account. If you have not onboarded CloudSOC, do so before continuing with this procedure.

Procedure

1. Add the integration.
   a. In Service mode, navigate to Account Maintenance > Integrations.
   b. Click New Integration; in the dialog, select CASB Audit Service.
   c. On the Integrations page, click to expand the added CASB Integration area.

2. Define the data storage location and data retention limits.

   ![Data retention limits configuration](Configure your data retention limits for CASB)

   a. IMPORTANT—Select the appropriate Data Storage Location for your location. You cannot change this value after setup.
   b. Select how many Months of Data to Track. The current maximum is 3, which means you can view reports that contain data from at the most the three previous months.

3. Enter your company domain and Integration ID.
Configure your data retention limits for CASB

<table>
<thead>
<tr>
<th>Data storage location:</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Months of data to track:</td>
<td>3</td>
</tr>
</tbody>
</table>

Configure your company's domain (e.g. symantec)

<table>
<thead>
<tr>
<th>Company domain:</th>
<th>example.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration ID:</td>
<td>abcdeFGHi1234jkl==</td>
</tr>
</tbody>
</table>

4. Click **Save**.

Access the CASB Audit App

The top of Web Security Service portal has a drop-down arrow next to your Admin name. Select **Cloud App Audit**.

When you click this link, the CloudSOC opens in a new browser tab.
The Dashboard displays high-level data. Click **Store**.

This is where you enable web applications and define domains and policies that are then sent to the Web Security Service portal and made available in policies.
To learn more about implementing web application configurations and monitoring user activities, consult the CloudSOC Help system and other relevant Symantec documentation.

Web Application Policy

As web traffic begins flowing through your network, you now have the ability to define granular block/allow and actions on the tens of thousands of detected web applications.

View CASB-Related Reports

As your Web Security Service account processes traffic, you can view specific reports that provide insight to web application traffic traversing your network.

In Solutions mode, select Overview > Report Center. The following reports contain reports enhanced by the CASB Audit Service.

- Applications by User
- Applications by Client IP
- Blocked Web Applications
- Web Application Actions

Add Reporting Users

Web Security Service Administrators can add other users and designate them as Reporting Users. These users can only view reports; they cannot change configuration settings. When a Reporting User accesses the Elastica Audit Service from the Web Security Service portal, the audit service uses the credentials to create a Reporting User role.

Add new users on the Service mode > Account Maintenance > Admin & Access page.
For more information, search for roles in the Solutions WebGuide.
Set Default Web Application Policy to Allow

The Symantec Web Security Service allows you to ensure that web applications vital to the effectiveness of your workforce are always accessible (assuming that the application itself is functioning properly at the destination). For example, E*Trade applications are required for your business operations.

**Tip:** As stated above, this is the default policy and the Web Security Service performs the check on the connection inbound from the origin content server. You can create additional policy that blocks specific users, groups, and locations access to the web applications that are otherwise allowed by default.

Reference

For the current list of web applications that the Web Security Service recognizes, see the following article.

- Web Application Reference Article

Procedure

This procedure demonstrates how to select specific applications and specify them as always available to any employee (client) that is routing web traffic to the Web Security Service (and is not otherwise blocked by more granular policy).

1. In **Solutions** mode, select **Content Filtering > Policy**.

2. In the **Group A > G3** rule, click the **Allowed Web Applications** link in the **Destinations** column. The portal displays the **Edit Web Application List: Allowed Web Applications** dialog.
a. The initial dialog is read-only. Click **Edit**.

b. Optional—Enter a **Comment** that describes the reason for the policy.

c. Select web applications from one or more high-level categories.

d. Click **Save**.

3. Click **Activate**.
Set Default Web Application Policy to Block

The Symantec Web Security Service allows you to select specific web applications that you feel are detrimental to the effectiveness of your workforce or the security of your network and set the default policy to block. For example, you think access to personal webmail accounts, such as yahoo and gmail, provide a greater security threat. Or you need to block resource intensive or time-wasting applications, such as streamed sports and social network destinations.

**Tip:** As stated above, this is the default policy and the Web Security Service performs the check on the connection inbound from the origin content server. You can create additional policy that allows specific users, groups, and locations access to the Web applications that are blocked for anyone else.

Reference

For the current list of web applications that the Web Security Service recognizes, see the following article.

- [Web Application Reference Article](#)

**Tip:** Obtaining the Symantec CASB license exposes thousands of applications.

Procedure

This procedure demonstrates how to select specific applications and specify them as unavailable to any employee (client) that is routing web traffic to the Web Security Service.

1. In Solutions mode, select Content Filtering > Policy.
2. In the Group B > G4 rule, click the Blocked Web Applications link in the Destinations column. The portal displays the Object Edit: Blocked Web Applications dialog.
a. The initial dialog is read-only. Click **Edit**.

![Edit Web Application List: Blocked Web Applications](image)

b. Optional—Enter a **Comment** that describes the reason for the policy.

c. Select web applications from one or more high-level categories.

d. Click **Save**.

3. Click **Activate**.
Define a User-Based Web Applications Policy

By combining several types of policy, you can create a robust web application policy that both protects your network, ensures acceptable web use policies, and allows employees to complete their job duties based on their roles in the organization. Consider the following use case and example policy.

Use Case

The default Web Security Service settings for all applications is **Allow**. Previously, a Web Security Service admin set the major webmail applications to **Block** and set **E*Trade** to **Allow**. You now want to add a more granular policy based on user groups.

- The FIFA World Cup creates network bandwidth havoc every year; furthermore, reports indicate that Pinterest traffic is trending upward and you want to block access.
- Both Facebook and Twitter can hinder productivity, yet are necessary marketing applications. You want to allow access only to the Marketing group; however, you also want to block security risks (such as downloading files) and block unnecessary features (such as games and chatting) for everyone in those groups.

**Tip:** How a user understands that an application action was blocked is application-dependent. For some actions, nothing happens. This behavior might generate support/IT tickets, so be sure such personnel understand this and can inform employees.

- Human Resources also uses Facebook plus LinkedIn, but you do not want other employees job-networking while working for you.

Example Policy

1. In Solutions Mode, select **Content Filtering > Policy**.

2. Add **FIFA World Cup, Facebook, Twitter, LinkedIn, and Pinterest** to **Blocked Web Applications** to the global block list.

   a. In the **Group B > G4** rule, click the **Blocked Web Applications** link in the **To Where** column. The service displays the Object Edit: Blocked Web Applications dialog.

   b. The initial dialog is read-only. Click **Edit**.
c. Select the **FIFA World Cup** application in the **Sports/Recreation** drop-down (you can search for the term).

d. Select the **Facebook**, **Twitter**, **Linkedin**, and **Pinterest** applications from the **Social Networking** drop-down.

e. Click **Save**.

   The **Blocked Applications (#)** number increments to include the four applications.

f. Yellow triangle icons indicate non-active policies. Click **Activate**. At this point, anyone who attempts to access any of those applications are blocked.

3. Allow Marketing access to Facebook and Twitter.

   a. Click **Add Rule**. The service displays the Create New Rule dialog.

   b. Click **Add Sources**.

   c. Click **User Group**.

   d. Select the group to be granted access—for this example, **CorpMarketing**.
e. Click Save.

f. Click Add Destinations

g. Click Web Application.

h. Search for Facebook and Twitter and add them; click Save.

i. For the Verdict construct, select Allow > Completely. Click Finish, which adds the rule in Group B above the default global block rule. The order is important, as when a component of rule gets matched, subsequent rules are ignored.

4. You now want to prevent Marketing employees from downloading attachments, playing games, and chatting from within Facebook.

   a. Repeat Step 3, creating a rule that applies to the same CorpMarketing group (Sources construct).

   b. Select the same web applications on the Destinations construct.

   c. Click Contents and Limits; click Actions.

   d. Select the actions to block, such as Download Video and Games.
e. Click **Save**.

f. Set the **Verdict** construct to **Block**.

g. Click **Add Rule**; the service displays the new action blocking rule in **Group B**.

h. Click **Activate**.

5. Create another rule for the **CorpHR** group to be allowed **Facebook** and **Linkedin**.

6. Click **Activate**. You now have conditional rules that fully allow access, limit access, or block web applications.

How a user understands that an application action was blocked is application-dependent. For some actions, nothing happens. This behavior might generate support/IT tickets, so be sure your support staff understand this and can inform employees.
SSL Policy

Enable SSL interception and define policy.

- "About Scanning Encrypted Traffic" on page 98
- "Install Encrypted Traffic Certificates" on page 102
  - "Install SSL Root Certificate for Chrome Browsers" on page 104
  - "Install SSL Root Certificate for Mozilla Firefox Browsers" on page 106
  - "Install SSL Root Certificate for Microsoft Internet Explorer Browsers" on page 108
  - "Install SSL Root Certificate for Safari Browsers" on page 109
- "Create SSL Policy" on page 110
- "Troubleshoot Dropped SSL Connections" on page 125
About Scanning Encrypted Traffic

By default the Symantec Web Security Service does not intercept inbound HTTPS traffic from destination web locations and applications. With the default configuration, the WSS applies content filtering policy to the furthest extent possible; however, it cannot apply policies to transactions that require deeper inspection, such as web application controls or malware scanning. Enabling SSL interception allows the WSS to decrypt HTTPS connections, examine the contents, and perform policy checks.

To retain the security of personal private information, Symantec recommends excluding some content filtering categories from termination and inspection. By default, the WSS does not intercept HTTPS traffic categorized as Brokerage/Trading, Financial Services, and Health, because this content usually involves private, sensitive personal account information. Additionally, for mobile devices, the WSS does not intercept traffic from a list of specific applications as these applications are known to break when intercepted on mobile devices.

To view which applications the WSS bypasses, see: https://support.symantec.com/en_US/article.TECH252764.html

**Tip:** If your policy allows uploading and downloading attachments in Gmail, you *must* enable SSL Interception. See "Define a User-Based Web Applications Policy" on page 93.

**Tip:** All Intermediate CAs used for certificate emulate are signed with SHA-2 (SHA256).
Content Filtering Use Case

Some users configure their Facebook accounts for secure connections ([https://www.facebook.com/](https://www.facebook.com/)). With SSL interception enabled, the WSS intercepts the inbound SSL connections and applies a policy check, such as **Block Games**.

Without SSL interception enabled, your acceptable web-use policies might not be fully enforced.
Malware Prevention Use Case

Another benefit of SSL interception is the detection of malware embedded in secure connection. No further configuration is required as the WSS provides malware scanning by default.

Without SSL intercept enabled, your network might still be at risk if the WSS cannot intercept and inspect inbound SSL connections.
Granular SSL Policy

The WSS allows you to selectively intercept HTTPS requests from specific network elements, such as single users, user groups, locations, and access method. Consider the following use cases.

- You know that not all browsers in specific locations or user groups have the root certificate installed and you want to exempt those elements until configuration completes.
- A single user is having SSL connection problems and you want to exempt that user while you investigate.

In the following diagram, SSL interception is enabled in the WSS.

A—An employee located at the corporate **Location** performs an HTTPS request to Facebook.

B—An employee connecting through the **Proxy Forwarding** connectivity method performs an HTTPS request to Facebook.
C—There is no SSL Interception policy based on location or the Proxy Forward Access Method, so the interception occurs; the WSS examines the returned HTTPS connection from Facebook.

D—A remote user with the WSS Agent installed on his client performs an HTTPS request to Facebook.

E—The WSS is configured to exempt all HTTPS traffic from WSS Agent from SSL interception.

Next Step

- If you do not want to enable SSL, Symantec still strongly recommends that you download and install the root certificate to client systems. For more information, proceed to "Install Encrypted Traffic Certificates" below.
- Define granular SSL Policy. "Create SSL Policy" on page 110
- Want to manage your own certificates? See "Deploy a Self Managed Certificate for SSL Interception" on page 116.

Install Encrypted Traffic Certificates

While root certificates are required when SSL Interception is enabled, Symantec strongly recommends installing the Web Security Service root certificates on all client systems independent of the SSL setting. One reason is that a majority of social networking sites use SSL, which means the WSS must perform some SSL interception for policy checks and enforcement. Without the certificates, clients receive Untrusted Issuer warnings, which generates support/IT inquiries and loss of productivity.

About the Root Certificate Recommendation

If you elect to not enable SSL interception, Symantec strongly recommends that you still deploy the WSS root certificate to clients because some SSL interception is required for policy enforcement against web applications.

Tip: All Intermediate CAs used for certificate emulate are signed with SHA-2 (SHA256).

Procedure: Obtain Certificate and Propagate

Step 1—Download the SSL Root Certificate.

If you previously completed this, proceed to Step 2.

If you enable SSL Interception, users receive a security warning dialog each time they attempt to browse an encrypted (HTTPS) website because their browser does not recognize the certificate returned by the WSS. To prevent this security prompt, download the certificate and propagate it to all client browsers.

Ensure that the WSS root certificate is installed on all clients. For clients with WSS Agent on the endpoints, this is automatically installed and applied to Internet Explorer, Edge and Google Chrome. If your organization uses Firefox or another browser that has its own certificate store, this certificate must be installed directly into that web browsing application.

1. In Service mode, select Network > SSL Interception.

2. Next to SSL Root Certificate, click Download.
3. Click **Save File** and save the certificate to an internally accessible location, such as a server that hosts applications provided by IT.

Step 2—Distribute or install the certificate on supported browsers.

Propagate the cert to all supported client browsers. One way to do this is to send out the link to the certificate location and instruct users how to install it. Select the following links for browser-specific installation instructions.

- **Apple Safari**
- **Google Chrome**
- **Microsoft Internet Explorer**
- **Mozilla Firefox**

Related Topics

- "About Scanning Encrypted Traffic" on page 98
- Examine Encrypted (HTTPS) Traffic
- "Deploy a Self Managed Certificate for SSL Interception" on page 116
Install SSL Root Certificate for Chrome Browsers

Perform the following steps for Google Chrome browsers. The procedures assume that you have downloaded the root certificate from your Web Security Service portal account to a network location.

1. In the Chrome browser, navigate to the **Under the Hood** settings page: Wrench icon > Options > Under the Hood (or enter chrome://settings/advanced).

2. Access the import certificate wizard.

   ![Image of Under the Hood settings page](image)

   a. In the **HTTPS/SSL** area, click **Manage Certificates**.
   
   b. Select the **Trusted Root Certification Authorities** tab.
   
   c. Click **Import**.

3. Import the certificate.

   a. On the first wizard screen, click **Next**.
   
   b. Click **Browse** and navigate to the certificate location; select it and click **Next**.
   
   c. Select the **Place all certificates in the following store** option.
d. If not already selected, **Browse** and select **Trusted Root Certification Authorities**; click **Next**.

e. Click **Finish**.

4. If another security warning dialog displays, click **Yes**.

**Next Step**

- Return to "Create SSL Policy" on page 110.
Install SSL Root Certificate for Mozilla Firefox Browsers

Perform the following steps for Mozilla Firefox browsers. The procedures assume that you have downloaded the root certificate from your Web Security Service portal account to a network location.

1. Access the **Import** certificate screen.
   
   a. Select **Advanced**.
   
   b. Select the **Encryption** tab.
   
   c. Click **View Certificates**. The browser displays the Certificate Manager dialog.

   ![Certificate Manager](image)

   a. **Certificate Name**
   
   - portal.bluecoatcloud.com
   - Blue Coat SG210 Series
     - 10.9.50.94
     - 10.9.50.94
     - 10.9.50.94
   - Blue Coat SG600 Series
     - 10.9.17.69
     - 10.9.17.69

   ![Certificate Manager](image)
d. Navigate to where you stored the certificate and click **Open**.

e. Click **Import**. The browser displays the Downloading Certificate dialog.

2. On the Downloading Certificate dialog, select **Trust this CA to identify websites** and click **OK**.

![Download Certificate Dialog]

If this dialog does not display, you must upgrade Firefox to a recent version.

**Next Step**
- Return to "Create SSL Policy" on page 110.
Install SSL Root Certificate for Microsoft Internet Explorer Browsers

Perform the following steps for Microsoft Internet Explorer browsers. The procedures assume that you have downloaded the root certificate from your Web Security Service portal account to a network location.

1. In the browser:
   a. Navigate to where you downloaded the file.
   b. Right-click the file, and select Install Certificate.
   c. You might be prompted for admin credentials and/or a confirmation prompt.

2. On the first wizard screen, click Next.

3. On the Certificate Store screen:
   a. Select the Place all certificates in the following store option.
   b. Click Browse.
   c. Select the Trusted Root Certification Authorities option.
   d. Click OK.

4. Click Next.

5. Click Finish.

6. If another security warning dialog displays, click Yes.

Next Step

- Return to "Create SSL Policy" on page 110.
Install SSL Root Certificate for Safari Browsers

Perform the following steps for Apple Safari browsers. The procedures assume that you have downloaded the root certificate from your WSS portal account to a network location.

For Safari Browsers on OS X

1. From the browser, open the directory in which you downloaded the root cert file.
2. Double-click the certificate.
3. You are prompted to store the certificate in the login keychain or the system keychain. To make the certificate available to all users of this system, select system keychain.
4. In Keychain Access, select the System keychain; then select Cloud Services Root CA certificate.
5. Select File > Get Info and expand the Trust section.
6. Change Secure Sockets Layer (SSL) value to Always Trust.
7. Close the dialogs and enter your password.

For Safari Browsers on a Windows System

1. In the browser:
   a. Navigate to where you downloaded the file.
   b. Right-click the file and select Install Certificate.
   c. You might be prompted for admin credentials and/or a confirmation prompt.
2. On the first wizard screen, click Next.
3. On the Certificate Store screen:
   a. Select the Place all certificates in the following store option.
   b. Click Browse.
   c. Select the Trusted Root Certification Authorities option.
   d. Click OK.
4. Click Next.
5. Click Finish.
6. If another security warning dialog displays, click Yes.

Next Step
- Return to “Create SSL Policy” on page 110.
Create SSL Policy

Create and enable SSL policy to ensure the Symantec Web Security Service correctly intercepts and exempts SSL traffic. Intercepting SSL traffic allows the Web Security Service to decrypt HTTPS connections, examine the contents, and perform policy checks. Exempting SSL traffic allows traffic to remain encrypted.

By default, the WSS does not intercept:

- HTTPS traffic that is categorized as Brokerage/Trading, Financial Services, and Health, because this content usually involves private, sensitive personal account information.
- Applications that are listed in the SSL Bypass List or Mobile App Bypass list because their traffic is known to break due to certificate pinning issues.

**Note:** If traffic is from a mobile device or bypassed (not intercepted), then the WSS does not apply CASB Gatelets or Web Isolation to the traffic. These features are currently not available for mobile traffic, and bypassed traffic cannot be isolated.

For more information on decrypting SSL traffic, see "About Scanning Encrypted Traffic" on page 98.

Technical Requirement

- Download and distribute the WSS root certificate. See "Install Encrypted Traffic Certificates" on page 102.

About the SSL Bypass List

Symantec maintains an initial list of applications in the SSL Bypass List that are known to break when their traffic is intercepted due to certificate pinning. The list is continually being updated; however, traffic for additional applications and domains that are not included in the list might break. For these applications and domains, Symantec recommends using the policy editor to exempt them from SSL interception. For the list of applications in the SSL Bypass List, see: [https://support.symantec.com/en_US/article.TECH252764.html](https://support.symantec.com/en_US/article.TECH252764.html)

**Note:** The sites and applications in the SSL Bypass List are also exempted for mobile devices.

About Mobile SSL Policy

You can apply SSL interception policy for mobile devices using the policy editor. Symantec maintains an initial list of applications in the Mobile SSL Bypass list that are known to break when their traffic is intercepted due to certificate pinning. The list is continually being updated; however, traffic for additional applications and domains that are not included in the list might break. For these applications and domains, Symantec recommends using the policy editor to exempt them from SSL interception. For the list of applications in the Mobile SSL Bypass list, see: [https://support.symantec.com/en_US/article.TECH252764.html](https://support.symantec.com/en_US/article.TECH252764.html)
Note: In the default policy, the sites and applications in the Mobile App Bypass list are only exempted for mobile devices (unless the site or application is also listed in the SSL Bypass List).

About SSL Sources and Destinations

You can write policy to intercept and exempt traffic for:

- **Sources**: Define policy that instructs the Web Security Service to not intercept SSL traffic from these sources. The portal enables you to select from previously defined lists or other elements as defined in your network.

- **Destinations**: Define policy that instructs the Web Security Service to not intercept SSL traffic to these destinations. The portal enables you to select from previously defined lists or other elements as defined in your network.

For more information on the policy editor, see "About the Content Filtering Rule Editor" on page 18.

<table>
<thead>
<tr>
<th>Element Type</th>
<th>Available Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detected authentication elements <em>(User, User Group)</em>—As provided by the authentication method (Auth Connector/SAML).</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: Be advised that user/group data is not always available before SSL Interception occurs.</td>
</tr>
<tr>
<td></td>
<td>IP/Subnet—Select from previously entered IP addresses/subnets that were defined in Solutions mode &gt; Overview &gt; Object Library &gt; Global Objects.</td>
</tr>
<tr>
<td></td>
<td>Locations—Exempt entire locations defined that are defined in Service mode &gt; Network &gt; Locations.</td>
</tr>
<tr>
<td></td>
<td>Deployment Type—Exempt all SSL traffic from a specific Access Method. For example, do not intercept SSL traffic from any client connecting with Roaming Captive Portal or from mobile devices.</td>
</tr>
<tr>
<td></td>
<td>Lists <em>(User, User Group, Location, IP/Subnet)</em>—These are previously defined object lists. To create a list to use specifically for this SSL policy, navigate to Solutions mode &gt; Overview &gt; Object Library &gt; User Defined Objects.</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Category—Exempt web traffic that belongs to specific categories.</td>
</tr>
<tr>
<td></td>
<td>URL and IP/Subnet—Exempt specific URLs or IP addresses. Select from previously entered domains that were defined in Solutions mode &gt; Overview &gt; Object Library &gt; Global Objects.</td>
</tr>
<tr>
<td></td>
<td>Lists <em>(Category List, URL List, IP/Subnet List)</em>—These are previously defined object lists. To create a list to use specifically for this SSL policy, navigate to Solutions mode &gt; Overview &gt; Object Library &gt; User Defined Objects.</td>
</tr>
</tbody>
</table>
Note: Before you enable policy, ensure you have downloaded and distributed the root certificate. See "Install Encrypted Traffic Certificates" on page 102.

About OCSP Validation

The OCSP Validation toggle provides you with the ability to enable or disable OCSP validation checks, so that you can:

- Decide whether sites that fail validation are at risk for being untrustworthy.
- Resolve any errors that are produced when OCSP validation is enabled.

Procedures

To create policy to exempt or intercept SSL traffic:

1. In Service mode, select Network > SSL Interception.
2. Expand the SSL Interception Policy drop-down and click Add Rule.
3. (Optional) Add sources:
   a. Click Add Sources.
   b. From the Available Sources drop-down lists, expand an element to filter the view.
   c. Select one or more sources to create policy for and click the right-pointing arrow to move sources to the Source Conditions list.
d. (Optional) For most categories, you have the option to create a new source. The New drop-down list allows you to create a new object and add it to the policy from this dialog. This might be helpful if you are immediately troubleshooting from a source that is not currently part of a custom list.

![Add Sources](image)

- **User**
- **List from Selection**
- **Username (23)**

- **New**
- **Search**

- **User**

- **Source**
- **Email**
- **Username**
- **Domain**

- **Category**
- **List from Selection**
- **Search**

- **Business Related**
- **Legal Liability**
- **Non-Productive**
- **Security**
- **Uncategorized**

- **Category**
- **List from Selection**
- **Search**

- **Financial S..**
- **For Kids**
- **Gambling**
- **Games**
- **Government..**
- **Health**
- **Humor/Jokes**

- **All Destinations**
- **This condition has no effect. Add items from the left to define this condition.**

- **Save**
- **Cancel**

e. Click **Save**.

4. (Optional) Add destinations:
   a. Click **Add Destinations**.
   b. From the **Available Destinations** drop-down lists, expand an element to filter the view.
   c. Select one or more destinations to create policy for and click the right-pointing arrow to move destinations to the **Destination Conditions** list.
d. (Optional) For most categories, you have the option to create a new source. The **New** drop-down list allows you to create a new object and add it to the policy from this dialog. This might be helpful if you are immediately troubleshooting for a destination that whose traffic is blocked by SSL policy.

![Add Destinations](image1)

e. (Optional) You can create policy that uses Symantec’s list of mobile applications that are known to break when decrypted. To add the list to policy, from the **Available Destinations** screen, click **Mobile App Bypass**.

![Edit Destinations](image2)

f. Click **Save**.

5. Assign a verdict:
   - To intercept traffic for your defined sources and/or destinations, click **Intercept**.
   - To exempt traffic for your defined sources and/or destinations, click **Do Not Intercept**.

6. Click **Add Rule**.
7. After defining interception and exemption policies, enable SSL policy:
   a. Toggle the switch to **SSL Interception Enabled**.

   ![SSL Interception Enabled]

   b. Click **Activate**; the WSS now intercepts SSL traffic per the defined policy.

   **Warning:** Enabling SSL on the WSS might introduce unintended results for some websites. If your clients experience dropped connections, consult the information in “Troubleshoot Dropped SSL Connections” on page 125.

8. (Optional) Configure the service to pass-through specific encrypted destination URLs, IP addresses/subnets. or Categories:
   - Domains/URLs—See Pass Through Encrypted Traffic From Specific Destinations.
   - Content Filter categories—See Pass Through Categories That Contain Encrypted Web Traffic.

   **Tip:** See also Apply Limited Policy to Non-Intercepted SSL Traffic.
Deploy a Self Managed Certificate for SSL Interception

To ensure that all traffic is properly analyzed, you can configure the Web Security Service to intercept and decrypt SSL traffic. By default, the Web Security Service portal supports only a certificate chain managed by Symantec for this task. If your organization prefers to use your own certificate infrastructure, you can license the Self Managed Certificate service to integrate your Web Security Service with a Hardware Security Module (HSM) hosted on Amazon Web Service (AWS).

This solution describes how to integrate an Amazon Cloud HSM service with a Web Security Service account.

**Note:** For each domain in your Web Security Service configuration, you must configure a unique HSM host.

About Integrating HSM

Self Managed Certificate support provides you with the ability to install your own certificate into the WSS portal. With this in place, you can now:

- **Simplify user on-boarding**
  
  When SSL/TLS traffic is intercepted and decrypted by the Web Security Service, the private key stored on the integrated HSM is used. At no point does the private key leave the HSM. As your users’ browsers already trust your root certificate, adding users to WSS takes less time to set up.

- **Control your own certificates**
  
  With this configuration, you retain control of your certificate chain and how it is used.

Prerequisites

Ensure that you have the following:

- An Amazon Web Service (AWS) account hosting a CloudHSM cluster.
- An EC2 instance in the above AWS Account where the AWS CLI has been configured with AWS administrator credentials.
- Python 2.7 (pre-installed in Amazon Linux)
  
  To check Python version run the following command in your EC2 instance: python --version.

- A Python Installable Package (PIP) module version 6.x and above compatible with Python 2.7.
  
  To check your PIP version run the following command in your EC2 instance: pip --version.
  
  If PIP is not installed, execute this command: sudo yum install python2-pip.

- Install the AWS Software Development Kit, Boto3, version 1.7 or later above.
  
  To check what version of Boto3 is installed in your EC2 instance, run this command: pip freeze | grep boto3.
If Boto3 is not installed, run this command in your EC2 instance: `sudo pip install boto3`.

- **WSS SUBSCRIPTION ID.**
  
  This ID is included in your order confirmation email sent by Symantec after subscribing to the Web Security Service.
  
  If you are new to the Web Security Service, wait to receive the confirmation mail before proceeding with steps outlined in this document.

- **CloudHSM Cluster ID**
  
  See the step labeled To Create a Cluster in the CloudHSM documentation, available at [https://docs.aws.amazon.com/cloudhsm/latest/userguide/create-cluster.html](https://docs.aws.amazon.com/cloudhsm/latest/userguide/create-cluster.html).

- **CloudHSM CA Certificate, saved as customerCA.crt**
  
  This file is used in the step Initialize the Cluster in the CloudHSM documentation, available here: [https://docs.aws.amazon.com/cloudhsm/latest/userguideinitialize-cluster.html](https://docs.aws.amazon.com/cloudhsm/latest/userguideinitialize-cluster.html).

- **CloudHSM Crypto Username and Password**
  
  These credentials are created during the step Create Users in the CloudHSM documentation here: [https://docs.aws.amazon.com/cloudhsm/latest/userguide/manage-hsm-users.html](https://docs.aws.amazon.com/cloudhsm/latest/userguide/manage-hsm-users.html).

---

**Step 1- Prepare Your CloudHSM Account For WSS Integration**

After you have satisfied the prerequisites, log in to your AWS EC2 instance and complete the following tasks:

1. Copy the file `SelfManagedCertificate.zip` to any directory on your EC2 instance.
   
   This file is included in your Symantec Provisioning Form.

2. Unzip the file with the following command:
   ```
   unzip ./SelfManagedCertificate.zip
   ```
   
   This command extracts the files into a new directory called `SelfManagedCertificate`.

3. Copy the CloudHSM CA Certificate file 'customerCA.crt' identified in Prerequisites to the `SelfManagedCertificate` directory created in step 2.

4. Create an account role to allow the automatic acceptance of the Virtual Private Cloud (VPC) Peering connection from Symantec's AWS account, and extract your CloudHSM Cluster information with the following script. To define these values manually, see appendix A at the end of this procedure.
   ```
   ./smc_init -r <AWS_REGION> -i <CLOUDHSM_CLUSTER_ID> -u <CRYPTO_USERNAME> -p <CRYPTO_USER_PASSWORD> -s <WSS_SUBSCRIPTION_ID> -a <SYMC_AWS_ACCOUNT_ID>
   ```
   
   If the script fails, a log file is automatically created under `SelfManagedCertificate/logs`. Create an S3 bucket with the following path:

Upload the file to this new bucket, and provide access to the Symantec AWS account, per the details in Appendix A.

The above script performs the following tasks:

- Creates a CloudFormation stack called wss-smc-vpc-peer-role.
- Extracts the CloudHSM Cluster information required for peering with the Symantec HSM client.
- Uploads your CloudHSM configuration details to an AWS S3 bucket and provides access to Symantec's AWS account.

### Script Variables

The variables in the above command script are as follows:

- `<AWS_REGION>` — The region of your CloudHSM installation, based on Amazon's definitions here:
  
  https://docs.aws.amazon.com/general/latest/grande.html#cloudhsm_region

- `<CLOUDHSM_CLUSTER_ID>` — The Cluster ID for your CloudHSM account.

- `<CRYPTO_USERNAME>` — The username for the account you created during the prerequisites stage.

- `<CRYPTO_PASSWORD>` — The password for the account you created during the prerequisites stage.

- `<WSS_SUBSCRIPTION_ID>` — The Subscription ID provided to you by Symantec in your Web Security Service order confirmation email. If your subscription ID includes an underscore (_), replace it with a dash (-).

- `<SYMC_AWS_ACCOUNT_ID>` — 239531557249 is the Symantec AWS Account ID.

**Caution:** If you receive an Access Denied error message when executing the script, verify that AWS credentials configured on EC2 instance have adequate privileges to execute these commands. Review the log_{current_date}.log file under .logs sub-directory for additional information.

### Procedure—Verify that the peering association was created successfully.

1. Log into the AWS Web Management console and verify that the CloudFormation stack labeled `wss-smc-vpc-peer-role` was created.
a. Go to the AWS Services page and search for CloudFormation.

![AWS Services page](image)

b. Confirm that wss-smc-vpc-peer-role is listed among your Stacks, with a status of CREATE_COMPLETE, and that the key RoleARN is listed in your Outputs configuration.

![CloudFormation console](image)

2. Send an email to DL-Smc-SMC-OPS@symantec.com with the subject SMC Initialization: WSS Subscription <WSS_SUBSCRIPTION_ID> to inform Cloud Operations that the configuration is complete.

**Note:** This address is to be used for provisioning only. For support concerns, please reach follow the appropriate support contact steps as directed on https://support.symantec.com.

Cloud Operations provisions your Web Security Service cloud account and sends you an email with an S3 URL to use in the next section to complete the association.

**Step 2- Register your CloudHSM/WSS Association**

1. In the AWS Management page, open the CloudFormation Console and click **Create Stack**.

2. When prompted to select a template, select **Specify an Amazon S3 template URL**.
Paste the URL provided by Cloud Operations and click Next.

3. Enter a name for your Stack and click Next.

4. Click Next on the options page; no optional configuration items need to be changed. Click Next.

5. Review the details in the review page, and click Create.

CloudFormation updates the required AWS resources to complete VPC peering.

6. Browse to the CloudFormation console.

The stack status shows CREATE_COMPLETE. This confirms that the appropriate entries have been created in the Security Group and Route Table.

**Step 3- Activate CloudHSM in the WSS Portal**

Verify that the service is active and configured

1. Navigate to Service > Account Maintenance > Integrations. Confirm successful integration by looking for the green check mark with Paired next to AWS CloudHSM.
Step 4- Enable Your Intermediate Certificate for SSL Interception

1. In the Web Security Service portal, go to Service > Network > SSL Interception.

2. Click Add Self Managed Certificate.

   ![Add an SSL Interception Self Managed Certificate](image)

   Select a Private Key stored in your AWS CloudHSM account and enter its corresponding Public key.

   - Private Key Handle: Select...
   - Public Key (PEM):

   Click Save. 

3. Select the option corresponding to the new self managed certificate.

   ![Certificate List](image)

   - Symantec Certificate: 23-01-20, Available
   - Self Managed Certificate: 18-08-19, Expired, 262157
   - Self Managed Certificate: 28-08-19, Available, 262158
   - Self Managed Certificate: 21-03-28, Available

   Click Use for SSL Interception.

4. Click Activate at the top of the portal to commit these changes to your portal account.

5. When ready to use this new configuration to intercept, decrypt, and re-sign SSL connections, click the slider at the top of this page to change the option from Disabled to Enable.

   **Tip:** You can click the download button next to your certificate in the list to download the public key to your local system.
Known Issues

- **Certificate Expiration Behavior**— 60 days prior to a Self Managed Certificate expiring, the SSL configuration page in the portal will display a warning. If the certificate used for interception expires, the service requires intervention. You must perform one of the following.
  - Resolve the issue by installing a certificate with a valid expiration date.
  - Use the Symantec Certificate (see Step 3 above) for interception.
  - Disable SSL interception.

- **AWS Certificate Key Labeling**

  The Amazon Web Service does not enforce any rules to ensure that the keys hosted in your AWS HSM clusters are labeled with unique names. The CloudHSM APIs that Amazon provides to retrieve key information is based on labels; querying for a list of keys results in an array of entries identified by labels. The API prunes duplicate labels from this list. As the Web Security Service relies on this information, Symantec strongly recommends that you use unique labels for each private key.

- **Maximum Certificate Chain Depth**

  Self-Managed Certificate currently only supports a maximum certificate chain depth of three: Root CA > Intermediate Issuer CA > Emulated Server Certificate. If your security infrastructure requires support for additional intermediate CA certificates, Symantec recommends administrators push the intermediate CA certificates to client browsers to ensure the appropriate trust relationship is maintained and full verification of the certificate chain is successful.

- **DLP Scanning Behavior During Failure**

  In the event of a CloudHSM failure or error, DLP will not actively block leaks. When CloudHSM is operational DLP functions as intended.

Manual Cluster Information

To manually gather cluster information, collect the following and upload to S3 bucket (as in Step 4).

**Step 1—CloudHSM Cluster information**

Create file with the name `smc_config` with following contents:

- `awsAccountId=
- `vpcId=
- `cidrRange=
- `routeTableId=
- `securityGroupId=
- `crossAccountRoleArn=
- `partitionName=`
- cryptoUser=
- cryptoUserPwd=
- eniIP=

**Example smc_config file.**

```plaintext
awsAccountId=12345678901
vpcId=vpc-389bd941
cidrRange=10.0.0.0/16
routeTableId=rtb-f50c758d
securityGroupId=sg-0b1dd275
crossAccountRoleArn=arn:aws:iam::12345678901:role/wss-smc-vpc-peer-role-peerRole-1BSWQUNBM7XBI
partitionName=PARTITION_1
cryptoUser=username
cryptoUserPwd=password
eniIP=10.0.2.29
```

**Step 2—Upload the file.**

As described in Prerequisites, upload the **customerCA.crt** file to the following S3 Bucket URL.


- **WSS_SUBSCRIPTION_ID**—The Subscription ID provided to you by Symantec in your WSS order confirmation email. In the event your subscription ID includes an underscore, (_) replace it with a dash (-).
- **AWS_REGION**—AWS region of your CloudHSM. For CloudHSM AWS Regions refer the AWS documentation. [https://docs.aws.amazon.com/general/latest/gr/rande.html#cloudhsm_region](https://docs.aws.amazon.com/general/latest/gr/rande.html#cloudhsm_region).

**Example**

Sydney region is ap-southeast-2.

Provide read and write access for this S3 bucket to Symantec's AWS account:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::239531557249:root"
      },
      "Action": [
        "s3:GetBucketAcl",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::wss-smc-tenant-WSS_SUBSCRIPTION_ID"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::239531557249:root"
      },
      "Action": [
        "s3:GetObject",
```
"s3:PutObject",
  "Resource": [
    "arn:aws:s3:::wss-smc-tenant-WSS_SUBSCRIPTION_ID/*"
  ]
}

WSS_SUBSCRIPTION_ID—The Subscription ID provided to you by Symantec in your Web Security Service order confirmation email. In the event that your Subscription ID contains an underscore (_), replace it with a dash (-).
Troubleshoot Dropped SSL Connections

With SSL enabled, the Symantec Web Security Service intercepts the SSL request to perform its security functions. This means that there must be a trust established between the requesting workstation and the service. The workstation allows the service to access the secure site (on the client's behalf) and establish an intermediary trust.

Dropped SSL Connections

Access issues might be caused by either one of the following scenarios.

- In some instances the requested HTTPS site (SSL) might detect that the request has been intercepted and disallow the connection. One way the site determines this is by certificate pinning, which is the process of recognizing the host or service's certificate when an attempted connection occurs. Because a cert already identifies or associates both parties, any attempt to come in between the client and the OCS is immediately recognized and the connection is refused. The workaround is to find out what domains are getting looked at for the certificates and then exclude them from SSL interception.

- Another method sites might use to prevent and protect against attacks is to allow access only from predefined IP addresses. These predefined IP addresses are part of the web sites allowed addresses or ACL (access control list). When an attempted connection occurs from a site that is not allowed by the ACL, the request goes unacknowledged. For the user, the browser seems to not reach the site and times out.

In this scenario and similar, Symantec recommends that you take these sites' IP addresses and set an exception on your firewall that excludes these addresses from going through the IPSec tunnel; for other access methods, add these IP addresses to the SSL Pass Through IPs/Subnets list.
Cloud Firewall Service Policy

Policy for non-standard web ports and application monitoring.

- "About the Cloud Firewall Service" on page 127
- "About the CFS Policy Editor" on page 135
- "CFS Policy Planning and Examples" on page 148
About the Cloud Firewall Service

The rapid move of infrastructure from on-premises to the cloud brings the need to secure all internet-bound traffic, including traffic from non-standard ports. The Cloud Firewall Service (CFS), a multi-tiered licensed component of the Web Security Service, provides next-generation firewall capabilities and extends network security beyond the standard web ports (80/443). The CFS enables you to define firewall policies to control all TCP or UDP traffic based on IP addresses, destination ports, locations and users and groups. Accepted traffic continues to WSS security/policy processing functionality. Furthermore, you can enable Application Monitoring, which allows you to define policies to accept or deny based on specific web applications.

Licensing and Use Cases

The WSS CFS requires one of two available add-on licenses. Selecting the appropriate license depends on your solution goals. The following sections describe the add-on licenses and what use cases they fulfill.
CFS Standard License

Abstract

- I want to enforce Protocol, Source IP, Destination IP/hostname, and Destination Port firewall policies across the entire organization.
- I want to apply firewall policies to roaming endpoints (WSS Agent 6.1+ and mobile devices).
- I require the enforcement and user and group-based CFS policies.

Entities

- Logs all traffic denied by CFS policy. Accepted traffic is not logged.
- User and group-based policies.
- User/Group logging controls integrated with user privacy controls.

Cloud Firewall Use Cases

Forward all traffic to the WSS.

- I want to configure my on-premises firewall to point to the WSS as the default route for all traffic.

Prevent specific traffic types to be used across the organization.

- I want to prevent the use of TCP destination port 22 (SSH).

I have an on-premises security stack and want to reduce complexity by sending each location direct-to-net with a centralized firewall policy enforcement across the organization.

- I want to remove my branch offices' MPLS nodes and direct the network traffic to the WSS and CFS policies.

Endpoints and Reporting.

- I want to enforce an acceptable network use policy on roaming endpoints.
- I want to have reports for all web (HTTP/HTTPS) traffic and blocked non-web traffic.

Prevent specific users and groups from using specific traffic types within the organization.

- I want to prevent any unauthorized users or groups from using SSH; to enforce data and access protections.
- I want to limit the use of FTP/SFTP on standard ports to specific users and groups that require downloading and uploading files.

I have operations already migrated to the cloud. The challenge now is going direct-to-net but allowing only the required network traffic type based on user and group roles.

- I want to ensure that group-based firewall policies are enforced across the organization independently of location or endpoint type.
Endpoints and Reporting.

- I want to enforce an acceptable network user and group-based firewall policies for roaming users.
- I want to have reports for all users and groups with blocked non-web (HTTP/HTTPS) traffic.
CFS Advanced License

Abstract

- I require monitoring and control for applications such as Windows File Sharing; non-web file streaming; Proxy Avoidance; applications running over dynamic non-standard ports.

Note—Standard applications running on well-known ports might not require this type of advanced application monitoring and control.

Entities

- CFS Standard features.
- Application and application category-based policies.
- All traffic and applications from non-standard web ports are logged for information and reporting.

Note: Traffic through standard web ports are logged in the WSS web access logs; not the CFS.

Application Monitoring Use Cases

Prevent specific applications or application types to be used by certain users and groups at the organization.

- I want to prevent any unauthorized users and groups from using SSH even if they are not using standard TCP port 22.
- I want to permit the use of FTP/SFTP for specific users and groups that require downloading and uploading files even if some of the FTP/SFTP servers are not using standard ports.

I have operations already migrated to the cloud. The challenge now is going direct-to-net but allowing only the applications the organization has licensed or purchased.

- I want to ensure sure that the organization’s endpoints are using only the Outlook desktop application for Office 365 and have no communications with other unauthorized mail services.

Extend the on-premises firewall policies to roaming users; enforce differentiated firewall policies per user types and groups and also per application.

- I want to enforce user and group-based firewall policies to the organization’s roaming users but also prevent them from using unauthorized applications, such as BitTorrent.

Correlate the impact of specific applications used by certain users and groups.

- I want detailed reports on users and groups that have permissions for testing new applications.
Supported Connectivity Matrix

<table>
<thead>
<tr>
<th>Supported Connectivity Methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN/IPsec</td>
<td></td>
</tr>
<tr>
<td>WSS Agent 6.1+</td>
<td></td>
</tr>
<tr>
<td>Cloud Connect Defense (CCD)</td>
<td></td>
</tr>
<tr>
<td>Mobile Devices (unknown locations)</td>
<td></td>
</tr>
<tr>
<td>SD Cloud Connector</td>
<td></td>
</tr>
</tbody>
</table>

**Limited Support**
- Explicit Proxy over IPsec
  - Destination IP or port-based firewall policies are not supported because the CFS sees connection to the proxy in the datacenter; not to the destination.

**Not Applicable Connectivity Methods**
- SEP Traffic
- Explicit Proxy
- Proxy Forwarding
  - When CFS is enabled, the CFS ignores traffic from these sources. Policies defined in the other WSS editors apply.

CFS Traffic Overviews

The following diagrams and descriptions provide high-level details of how the CFS is positioned in the WSS traffic flow.
CFS—No Application Monitoring

A—A client sends a request from a location routed through a firewall device.
- An IPsec tunnel is established.
- The CFS receives the initial packets.
- Authentication identifies the user and group affiliation from the associated client IP address.

B—A client sends a request from a client system with WSS Agent, from a mobile device, or from the Cloud Connect Defense (CCD) app on a Windows 10 system.
- An IPsec tunnel is established.
- The CFS receives the initial packets.
- Authentication identifies group affiliation from the logged in employee.

C—The CFS applies its policy to check against the requested network services, protocols, and ports.
- If a Deny verdict occurs, the CFS terminates the request and no packets traverse beyond the CFS to the WSS proxy.
- If an Accept verdict occurs, the CFS passes the request to the WSS proxy, which determines the next decision based on SSL, CASB, Web Isolation, and web use policies). Exception: DNS traffic passes through the WSS proxy asset.
CFS—With Application Monitoring Policy

Requires the CFS Advanced License

An Application Monitoring policy is enabled.

A—A client sends a request from a location routed through a firewall device.

- An IPsec tunnel is established.
- The CFS receives the initial packets.
- Authentication identifies the user and group affiliation from the associated client IP address.

B—A client sends a request from a client system with WSS Agent, from a mobile device, or from the Cloud Connect Defense (CCD) app on a Windows 10 system.

- An IPsec tunnel is established.
- The CFS receives the initial packets.
- Authentication identifies group affiliation from the logged in employee.

C—The CFS Application Monitoring module examines packets to identify the requested firewall application. During this transaction, traffic might be transferred until the application is determined.

- If a Deny verdict occurs, the CFS terminates the request and no packets traverse beyond the CFS to the WSS proxy.
If an **Accept** verdict occurs, the CFS passes the request to the WSS proxy, which determines the next decision based on SSL, CASB, Web Isolation, and web use policies. Exception: UDP and non-DNS traffic passes through the WSS proxy asset.
About the CFS Policy Editor

The Web Security Service Cloud Firewall Service (CFS) replicates firewall capabilities and extends network security beyond the standard web ports (80/443). Through, you can determine what non-web (HTTP/HTTPS) traffic is permitted in your organization. This policy can be ubiquitous across the whole organization or determined by users, groups, and firewall-detected applications.

- This topic describes the components of the policy editor. After you understand this topic, you can review policy use cases and examples in the next section.

Technical Requirements

- WSS Admin Access.
- An access control plan to allow or deny internet outbound traffic based non-web ports, network services, sources, destinations, and locations.
  
  Users, groups, and applications if properly licensed for these elements.
- Authentication—Standard and Advanced license enable user and group-based policies.
  - WSS Agent, CCD, and SEP-Mobile provide identities per connection.
  - Fixed-site IPsec connections require the Auth Connector for domain log in detection.
  - Challenge-based SAML or Captive Portal authentication requires the IP surrogate option.
- An authentication method is implemented if you are applying policies to specific users or groups.

Limitations

- To properly support domain bypasses, the WSS Agent does not send DNS requests to the WSS when CFS is enabled. DNS requests are sent direct.
- The maximum length of a username string is 50 characters. For example, Domain\UserName.

About the CFS Policy Editor

The WSS CFS policy editor allows you to create custom rules that define what traffic from non-standard ports is allowed to proceed to the WSS for further acceptable use and threat protection.

**Note:** The policy editor components vary based on the CFS license tier applied to your account.

To view the policy editor, in **Solutions** mode, select **Cloud Firewall > Policy**. The Policy Rules matrix comprises five or six columns depending on the license tier—an **Order** column and four or five policy constructs—and a series of rows. The following sections describe how to interpret the editor and create new rules.
CFS Policy Construct

Policy Rules columns provide options for four constructs that shape the purpose of the rule.

By Column name—

- **Sources**—
  - Default—Apply to IP addresses/subnets, fixed IPsec Locations, WSS Agents, and Mobile Users.
  - Standard/Advanced Licenses—Add support for to users and groups.

  The default is **Any**.

- **Destinations**—Apply to IP addresses/Subnets and Domains. The default is **Any**.

- **TCP/UDP/Network Services**—
  - Apply the rule to all TCP, UDP, or both traffic.
  - Apply the rule to well-known network service protocols and ports, such as SSH on port 22.
  - Define a custom service. For example, you want to apply against a custom service running through TCP/UDP on unique set of ports.

  The default is **Any**.

- **Verdict**—
  - Accept—The traffic is allowed to proceed through to the WSS.
  - Deny—The CFS drops denied packets.

- **Application Overrides**—
  - Requires the CFS **Advanced License**; this column is not visible without this license.
  - The CFS examines packets to identify the firewall-detected applications and applies the rule **Verdict**. However, you can override a **Deny** verdict. For example, the **Marketing** group is denied all applications except for **Facebook**. For that group, Facebook traffic is allowed, but still susceptible to use policies as defined in the Content Filter policy editor.

**Global Rules**

There are hard-coded rule rows that cannot be deleted. They are designated as **G1**, **G2**, **G3**, and **G4**. Primarily, these rules are in place to enforce pre-defined, default policies. Where applicable for the rule, the columns contain links. Click the link to display
an editor dialog from which you can specify or select policy objects that apply to everyone (unless they are allowed or blocked by other custom policy).

- **G1**—A **Deny** rule that blocks all unsupported IP protocols. This rule cannot be modified.

- **G2**—An **Accept** rule that exempts specified IP addresses and domains from CFS policies.

- **G3**—An **Accept** rule that allows all HTTP/HTTPS traffic that does not match any preceding rules. This ensures the traffic reaches the WSS proxy and policy assets. This rule cannot be modified.

- **G4**—An **Accept** rule that allows all traffic that does not match any of the preceding rules. For this rule, you can click the edit icon and set to **Deny**, which provides the most heightened security.

In the editor, mouse-over the **text bubble** icons and the **G**-numbers in the left column to view these descriptions in text pop-ups.

**Create Custom CFS Rules**

You will more than likely need to create policy rules that accomplish your CFS goals.

On the **Cloud Firewall < Policy** tab, verify that the CFS is **Enabled**.

**Tip:** This setting globally controls the CFS policy enforcement and allows the quick toggling of CFS functions during network troubleshooting.

To launch the rule wizard, navigate to the **Cloud Firewall < Policy** tab and click **Add Rule**.

The Policy Editor enables you to create And/Or constructs. For example, you have a rule where the Sources are either of two users (an Or construct) if the request from a specific location (an And construct).

**The Sources Construct**

This example demonstrates what you can add to the **Sources** construct of the rule.

The policy editor is flexible, allowing you to select objects as well as add new objects within.
- **Add Users/Groups**—This policy applies to specified logged in users and affiliated groups.

- **Add Source IPs**—This policy applies to the client IP addresses seen by the WSS.

- **Add Locations**—
  - This policy applies fixed IPsec locations as previously defined on the **Service mode > Network > Location** tab.
  - Also an option is this policy applies to roaming clients, which can be WSS Agents or mobile devices (from SEP-Mobile or the Android app).

Select any construct to display its options.

The editor displays all of the objects that are available for this rule. Select one or more and click the right-arrow to assign them to the rule.

You can also click **New** and select to create a new list or in applicable constructs a new object.

After completing your selections, click **Save**.

You can also continue to add sources that create an **AND** construct. Consider the following example.
The Admin added three **Source IP** addresses, a fixed **Location**, and two **User Groups**. To trigger the rule, one match from *each* source must occur.

### The Destinations Construct

As with the **Sources** construct, you can create **AND/OR** policies.

Click **Add Destinations**. Select to what internet elements this rule applies.

- **IP/Subnets** and **Domains**—You might have a need to trigger policy when the destination is a specific server, such as a testing server, or a specific domain (URLs are *not* supported).

![Add Destinations](image)

### The Services Construct

The **Services** construct is where you select network traffic protocols and ports.
All TCP/UDP

You want the rule to apply to TCP, UDP, or both types of traffic from the sources and to the destinations you defined.

Well-Known Network Services

The CFS editor presents a list of well-known services and associated ports. For example, FTP and SSH.

Click **Network Service**, then the **Well-Known and Registered Ports** tab.

Custom Services and Port Ranges

If you have a custom service or a service running on non-standard ports, you can define them in the Network Service editor.
1. Click **New**.

2. Define the **Port/Port Range** and select the network **Protocol**.

3. Click **Add** and **Save**.

**The Verdict Construct (CFS Default Behavior and Standard License)**

Now that you have created the conditions that trigger the policy rule, the final configuration is to instruct the CFS whether to **Accept** the traffic into the WSS or **Deny** the traffic. This is called the **Verdict**.

**The Client Experience**

When CFS policy triggers a **Deny** verdict, what the end user sees on the client varies.
If it is a simple Deny, the packets are dropped and the client returns a timed out message.  

If an application control is enabled for the rule, the connection might continue until a block is determined. 

- The user might receive an exception page if the connection is HTTP. Otherwise, it cannot be predicted whether will occur or note; it depends on multiple webpage communication factors.

**The Verdict Construct with Application Monitoring (CFS Advanced License)**

If your account is provisioned with the CFS Advanced license, you have the option to enable Application Monitoring, which examines packets to identify the firewall-detected applications. When enabled, traffic might transfer until the application is determined and a verdict rendered. With reporting, you can monitor application traffic.

Combine monitoring with deny verdict to create a robust, secure policies. Achieve this by adding Application Overrides. For example, your organization uses Microsoft Exchange and you do not want any other email category applications to reach the WSS.

1. Click **Add App Overrides**.
2. Click **Cloud Firewall Application**.
3. Browse categories and applications. In this example, it is easier to create a new List from Selection. Show screen...

a. **Name** the list.

b. Select **Categories**; in this example, **Email**.
c. Use Control + left-click to select or de-select multiple applications; add to the include column.

d. **Save** the new list; **Save** the override list.

**Save and Activate the Policy**

1. When you are satisfied with the rule, click **Save**, which adds it to the CFS rule matrix.

2. Click **Activate**.

The matrix displays all custom rules between the **G2** and **G3** global rules.

**About Reference Rule Limits**

As with other WSS policies editors, you can create and add objects, such as custom User Groups IP address lists. You can create unlimited objects; however, the portal enforces limits when attempting to add them to CFS rules. The limits are expressed as a percentage of maximum CFS limit, which by default is 100.

- Destinations (includes both IP addresses and domains): 80
- Users: 50
- Groups: 50
- Services: 10
- Application overrides: 10

If you attempt to add objects beyond the limit threshold, the portal displays an exception dialog.
CFS Policy Best Practices

- After you update exiting CFS firewall policies, the new policy is applied to future traffic flows. All existing established firewall sessions are enforced by already matched firewall policies. For example, a user belongs to a group that by policy is allowed access to Spotify. That user is moved to group that cannot request Spotify; however, the user is still allowed because the TCP connection is persistent.

- If you define a rule that uses hostname (for example, deny a website domain), be advised that the CFS actually resolves that hostname into an IP address, which it then uses for run-time traffic enforcement. If you are accustomed to other WSS policy editors, such as Content Filtering, you might be inclined to add the domain only. For example, you want to block a site called Example, you typically enter example.com. For CFS policy, however, Symantec recommends defining two destinations: example.com and www.example.com. These two domains open the same page, but might resolve to two different IP addresses.
  - Also be advised that the hostname condition might not be compatible with large sites such as facebook.com. Because of geolocation or other processes, DNS might return different sets of IPs to the client and to the WSS. Only use the hostname condition for sites that you are sure will not return conflicting DNS information for a particular hostname. This might require some testing.

- When designing application-based firewall policies, the accepted application might need to access other applications for dependent services. For example, you want to deny all applications but accept a single application. Using Facebook as an example, Facebook Messenger might depend on services provided by Facebook or Facebook Apps. The dependent application must also be accepted for the original application to be accessed.

- When configuring CFS policies, you can specify destinations as DNS domains or IP/subnets. If the DNS domain uses round-robin DNS or if the DNS domain can be resolved as multiple IP addresses, then the client device and the WSS asset might resolve the DNS domain as different IP addresses. Consequentially, the firewall policy might not be able to block access to the destination using DNS domains.

  In this scenario, Symantec recommends the more effective CFS application monitoring method to block connections. (This functionality requires the CFS Advanced License.)
CFS Reporting

CFS reports are driven by CFS log data (separate from the content access logs).

The **Cloud Firewall > Dashboard** tab displays high-level CFS flow data. A flow is traffic from any port or protocol received by the CFS; this includes traffic that might not reach the WSS content processing because of a Deny verdict in the CFS policy.

The **Cloud Firewall > Reports** tab provides many pre-defined reports designed to present CFS-related data. Given that the CFS feature potentially allows traffic from all ports, port-based reports provide insight. Traffic by Ports, Blocked Traffic by Ports, and Unrecognized Traffic by Ports might be a good place to begin analyzing traffic.
Like other WSS reports, you can drill down, view more details, and apply filters. In a report, the Options dialog (gear icon in upper-right corner) is where you can summarize and filter data.

### Privacy

You can configure the WSS to suppress some or all user identification information from the CFS Log on the devices in the Symantec datacenters.

**Next Selection**

- Proceed to "CFS Policy Planning and Examples" on page 148.
CFS Policy Planning and Examples

The Web Security Service Cloud Firewall Service allows the forwarding of all traffic (web and non-web) to the WSS, which enables user protection through granular firewall rules enforcement. Before proceeding with this topic, understand the contents of the following.

- "About the Cloud Firewall Service" on page 127 describes the solution.
- "About the CFS Policy Editor" on page 135 describes how the editor functions.

Before you begin to define CFS policy, Symantec strongly recommends that you plan out your organization's protection requirements. Within the organization, different teams or groups likely require access to different ports and protocols. This topic provides planning strategies and use case policy examples.

**Note:** The following planning and example information relates mostly to the functionality afforded by the CFS Standard and Advanced licenses. With the default behavior, you can define simple, global protocol and port policies.

Plan CFS Policy Enforcement

As network security administrator, you must design firewall policies to meet the needs of different teams. The first step is to decide who and/or what to protect. Consider defining security profiles.

- Do specific users in the organization (from your Active Directory or SAML IdP) require access to specific ports, protocols, or web applications? For example, a QA engineer requires full access for testing.
- Do groups contain users who share the same security profiles and needs? For example, QA and Dev groups require access to specific ports, but the non-development groups are to be denied.
- Is policy based on requests from specific network subnets required? For example, network subnet 192.168.0.0/16 is dedicated to testing web applications.
- Do fixed locations require policies? For example, a branch location is a test lab that connects to the WSS from a location defined in the portal.
- Determine if the security profiles require Accept or Deny firewall traffic verdicts.
- As with any granular policy, you can have exceptions with each security profile. Refine each by considering differing needs. For example, a super administrator in a group requires even less restrictive policy.

Example Planning Use Case

Example Corp has two locations.
LOCATION ONE—Headquarters, which has multiple network segments to consider.

- GREEN SEGMENT—The corporate network (192.168.0.0/16), which is the employee path to the internet. CFS policy requirements—
  - All users allowed to perform any internet requests except for applications that use peer-to-peer file transfers.
  - Users in the TechMarketing group are allowed to use peer-to-peer applications.

- LIGHT BLUE SEGMENT—A developer network (10.1.0.0/16) used by some developers. CFS policy requirements—
  - Users are denied all internet sites except a public customer support HTTPS website (1.2.3.4) that hosts a customer discussions forum.
  - Users in the DevSupport group can access the customer log download site (1.2.3.5) through SFTP.

- BLUE SEGMENT—A lab network (10.2.0.0/16) used by developers and quality engineers who perform product testing. In addition, this lab has an all traffic testbed (10.3.1.0/24) that requires all protocols allowed to the internet. CFS policy requirements—
  - Users in the Blue Lab network can go to any internet sites through HTTP/HTTPS.
  - For users who have access to the test bed sub-segment there are no protocol restrictions.

- RED SEGMENT—A restricted lab network (10.3.0.0/16) used by developers and quality engineers who perform product testing. CFS policy requirements—
  - Users in the Red Lab network can go to any internet sites.

LOCATION TWO—A remote Data Center that connects through an IPsec Location named in the WSS portal as RDC.

- This location hosts Example Corp’s data analytics engine and connects to a internet cloud service (1.2.3.6) for periodic data download. The specific protocol used is HTTPS.

- There cannot be any other outbound internet traffic from this remote location.
Example Policies

After you catalog your network segment planning, you can use the CFS Policy Editor (Cloud Firewall > Policy) to implement the policies. The following policy examples match the use cases in the previous section.

GREEN SEGMENT

- IF Source = 192.168.0.0/16 AND Group = TechMarketing AND Destination = Any AND Service = ANY THEN Accept
- IF Source = 192.168.0.0/16 AND Destination = Any AND Service = ANY THEN Accept

Enable Application Monitoring; override to Deny P2P application category.

LIGHT BLUE SEGMENT

- IF Source = 10.1.0.0/16 AND Destination = 1.2.3.4 AND Service = TCP/443 THEN Accept
- IF Source = 10.1.0.0/16 AND Group = DevSupport AND Destination = 1.2.3.5 AND Service = SFTP THEN Accept
- IF Source = 10.1.0.0/16 AND Destination = Any AND Service = ANY THEN Deny

BLUE SEGMENT

- IF Source = 10.3.1.0/24 AND Destination = Any AND Service = ANY THEN Accept
- IF Source = 10.3.0.0/16 AND Destination = Any AND Service = TCP/[80,443] THEN Accept
- IF Source = 10.3.0.0/16 AND Destination = Any AND Service = Any THEN Deny
RED SEGMENT

- IF Source = 10.2.0.0/16 AND Destination = Any AND Service = ANY THEN Accept

RDC LOCATION

- IF Location = RDC AND Destination = 1.2.3.6 AND Service = TCP/443 THEN Accept
- IF Location = RDC AND Destination = Any AND Service = Any THEN Deny

Default Deny Policy?

Consider the need to have a default Deny policy for all web traffic not otherwise affected by Accept rules.

Be advised that this rule is quite restrictive (as indicated by the icon/tooltip). But it provides the highest security level as only traffic that satisfy Accept rules is allowed through to the WSS.
Policy: How Do I?

The Symantec Web Security Service provides policy options that, mostly, determine how specific web traffic is processed by the service. Almost all configurations on the portal in Solutions mode translate into policy. This page allows you to navigate to common, specific tasks.

Service

- I want to create custom lists of objects and network elements to use in multiple policies.
- I want to notify users when an exception occurs.
- I want to customize the error page template.

Content

- I want to block specific web application actions.
- I want redirect acceptable web use policy abusers to the company's Employee Handbook.
- I want to enforce safe search engine policy.

User-Related

- I want to assign Reporting Users based on organizational role.
- I want to coach users when they browse to potentially non-productive web content.
- I want to create a policy to block unauthenticated users.
- I want to allow certain people to over rule the blocked content verdict.
- I want to generate instant policy directly from a user or client value in a report.
- I want to create a policy based on usernames that I see in reports.
- I want to restrict when a specific user has access to content.
- I want to define a policy that applies only to my mobile users.
- I want to block specific application actions.
- I want to enforce search engine Safe Search functionality.
Define Object Lists to Use in Custom Policy

The Symantec Web Security Service Content Filtering Rules policy editor enables you to create or select network objects such as usernames, IP addresses, URLs, and categories. A more efficient method is to create objects that contain lists of related values and then select that object when creating policy. The further advantage is that objects are reusable in multiple policy rules.

The Web Security Service provides an Object Library that displays all of the reusable lists—both global and user-defined. It is from here that you also manage the object lists (create and edit existing).

Use Case Procedure

You want to create a list that combines several time-wasting categories into one content filtering list object for use in a coaching policy.

1. In Solutions Mode, select Overview > Object Library.

2. Access the Category Lists dialog.

   a. Select User Defined Objects.

   b. Select any object. For example, add a new Category List.

   c. Click the Add New. The service displays the new Add New Object dialog.

3. Select the categories to include.
a. **Name** the object; make the name obvious so that other Web Security Service users understand what it is.

b. (Optional) Enter a **Comment** that describes the purpose of the object.

c. Select the object elements. This example selects the **Non-Productive > Social Interaction** category groups.

d. Click **Add** to move them to the **In This List** area.

e. Click **Save**.

f. An orange triangle next to the object indicates new objects are in **Pending** state and remain so until you click **Activate**.

4. Still in Solutions Mode, select **Content Filtering > Policy**.

5. Click **Add Rule** and create a rule that coaches access to these categories.

   a. Click **Destinations**.

   b. Click the **Category Lists** item.
c. Select the object that you created in Step 3 and click the right-arrow icon.

d. Click Save.

e. In the Verdict area, Select Allow and with Coach.

f. Click Add Rule.

6. Objects rest in pending state until they are added to policy rules.
After you define rules (that contain these objects) in the Content Filtering policy editor, the object library displays the object and indicates which rule(s) contain the object.

**Geolocation Objects**

If your portal account has the Advanced Web Security with Risk Controls and Web Applications add-on license, you can use **Geolocation** objects (lists of countries). This allows you to create policy based on from what country or to what country a content request occurs. See "About Geolocation Policies" on page 11.
Modify the Default Exception Notifications

By default, the Symantec Web Security Service displays an notification page to users when the transaction triggers an exception event, such as a policy violation page when a user attempts to access a website or web application protocol that WSS policy is configured to block. The content of the page includes the result message, such as Access Denied, along with other details, such as the client IP address and the reason (for example, a blocked content filter category).

The WSS allows you to modify this page, including selecting a color scheme, adding contact information and changing the displayed logo and company name. For example, add your IT group email address so that users can contact IT to dispute a rating or ask a question about the policy.

If your WSS account includes the Advanced Web Security with Risk Controls and Web Applications add-on license, the exception includes the Client Location, or country of origin as determined by the service. For more details, see "About Geolocation Policies" on page 11.

The Error ID indicates which policy rule triggered the exception. CF-XX is a content filter rule. TP-XX is a threat protection rule. The exception displays N/A if it cannot determine the rule. Other operations, such a password override, might cause an N/A.

Tip: You can also modify the template for this page. See "Customize the User Notification Template" on page 161.
Additionally, English, French (European), German, Italian, Japanese, and Spanish (European) language web browsers display these pages in their respective languages.

**Procedure**

This task requires WSS portal Admin Role credentials.

1. In Service mode, select **Notifications**.

   ![Image of error page customization](image1)

   a. Select which additional text options to include on the page. In addition to letter and numbers, only spaces and plus signs (+) are valid characters.

   b. Select the page style and color.

   c. Click **Save**.

2. Enter the **Company Name** field that replaces the current name on notification pages.

   ![Image of company name entry](image2)

3. (Optional) Change the logo (.png file, 190 pixels x 35 pixels) that displays on exception pages. The default is the Symantec company logo; however, if your company obtained the WSS from a third-party service provider, their logo
might display instead. The logo you add here overrides that configuration.

![Upload Error Logo dialog]

- In the **Current Logo** area, click **Change**. The service displays Upload Error Log dialogs.
- **Browse** to the stored image; select it and click **Open**.
- **Click Save** in the Error dialog.

To revert to the default file, **click Change** and select **Reset**.

![Reset option in Error dialog]

4. Click **Save**.
Note: If the WSS has other pending policy changes, a dialog displays to inform you of this. You can accept to activate all pending policy or navigate to the various policy pages and verify that you want those changes (then return here to save the notification changes).

5. Configure Content Filtering Policy.

Troubleshooting Assistance

You can force the 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, including talking to Support Personnel who speak only English.

- Select Show English Translation Only and click Save.
- When assistance is complete, clear the option.
Customize the User Notification Template

As configured on the Error Pages tab (Service mode > Notifications > Error Pages), the Symantec WSS displays notification pages to users when a browsing action triggers an exception, such as a denied content category. The page contains default information, including the exception reason. You can also select to display information, such as contact information and a custom logo. These notification options should prove sufficient for most enterprise requirements. This information comes from a template, which you can also customize.

Use Cases

- You do not want the notification page to contain specific elements, such as the logo or contact email.
- You want to change the background color or add additional text to an area on the page.

Best Practices

- Symantec considers customizing the notification template an advanced feature. As such, only admin-level WSS users are able to modify the template contents.
- Symantec recommends considerable knowledge of HTML and CSS before performing edits beyond simple string replacements.
- Symantec recommends that you perform only small, deliberate changes to the template rather than recreating a completely new template.
- To avoid display issues, keep the template code compatible with any browser vendor used by employees in your enterprise.
- Certain sections of the template are critical for the page to function properly with other policy elements, such as the Password Override feature. Avoid these clearly marked code sections in the template.
- Do not load content from servers that are outside of your control.
  - JavaScript is running in the page under the context of the page that was blocked and might in some cases have access to sensitive user cookies meant to be kept private. For this reason, avoid loading any third-party hosted JavaScript.
  - Requests to other resources (such as images) might have the Referrer HTTP header present from the page that was blocked, revealing what page the user was visiting when the block page was served. For this reason, avoid loading anything from a 3rd party server.
- When possible, directly include content in the template rather than hosting it on the Internet. This decreases load time and guarantees that a resource is reachable.
  - Base64 images can be encoded directly in the HTML.
  - The template can contain CSS stylesheets.
- The WSS displays the exception page for both HTTP and HTTPS connections. If an image (or some other resource) is referenced in your template using the http:// protocol and the template is used for a page loaded over HTTPS, some browsers might display a warning to inform the user that insecure content was loaded within a secure page. The same might apply in the reverse situation where an https:// resource loads on a page over HTTP. For this reason, Symantec advises to either include the content inline as previously mentioned earlier or perform one of the following.
Host your content both over http:// and https:// and

Use a protocol-less URL to reference it; for example http://example.com/aResource becomes //example.com/aResource. This loads the image over whichever protocol used to load the original page.

The Editor

To view the Custom Notification editor, select Service mode > Notifications > Custom Error Pages.

A—The Preview option allows you to view code changes before they are implemented.
B—Click **Show Replacement Variables** to display all of the code elements that the service uses to populate data.

The variables that begin with \$\text{(config.)} \text{options: comprise the elements on the}\) Notifications > Error Pages.\) These are ones that you can elect to remove from the template.

C—If you run into problems with your edits or you want to start over and create a new template, click Reset to Default HTML, which reverts the template to its default state.

D—When you click **Enable** custom error pages, the system might override any custom edits to the Notifications > Error Pages. For example, if you add contact telephone number to the field on that page, but comment out the field in the Custom Error Page template, the service does not display the entered phone number. If you clear the **Enable custom error pages** option, the service returns to the default page and any customizations that exist there.

**Examples**

The following examples illustrate how you can edit the template.

**Add Text**

Supplement the notification with custom text. The following example adds a new line to **Tech support information** drop-down (accessed by clicking **more**).
Click **Preview** to see how the service will display the page.

**Remove an Element**

Enter HTML code to comment out an element. For example, you do not want the notification to include detailed transaction information/link. Locate the element in the template and add the comment out code: `<!-- text -->`. 
IMPORTANT: Some span tag contain the `localize` attribute. Regardless of any customized text, this attribute instructs the WSS to overwrite with a localized version of the text (including English). To display custom text in a span, you must remove the `localize` attribute. However, doing so prevents localization.

This line retains the default value because of the `localize` attribute.

```html
<p id="httpCode">
    <span localize="[techSupport]">Tech support information</span>: $(exception.id)
</p>
```

This line provides the custom text: Tech support information.

```html
<p id="httpCode">
    <span>Tech support information</span>: $(exception.id)
</p>
```

**Customize the Style**

You can enter CSS code to change the appearance of the page. Locate the Symantec styling section.

```html
<!-- This loads default Symantec styling -->
<style type="text/css">
    body {
        background-color: blue !important;
        font-color: white;
    }
    $(bluecoat-template-default.css)
</style>
```

You can also add javascript (above the style section) to add more complex HTML elements.
Provide Browsing Coaching to Users

The Coaching option enables you to display a message to employees when they attempt to browse web content that is not blocked by Content Filtering policy, yet might not represent the best use of employee time. You elect to not block employee access to some leisure sites, such as Facebook, but do want to given an indication that spending too much time on these might draw attention to oneself.

This message informs the employee that their request will be logged and they must acknowledge this before proceeding to the website. Furthermore, the message suggests that the employee contact IT should they want to dispute the verdict. Currently, this message applies to all coach-able requests and is not customizable.

Note: For coaching to properly function, browser settings must allow cookies.

1. In Solutions Mode, select Content Filtering > Policy.

2. Add a rule or Edit an existing rule (click the symbol in the Verdict column). If adding a new rule, click Next until you reach the Verdict page.

   a. Select Allow and select with Coach. The service displays the Coaching Message text. This text is what employees see.
b. (Optional) By default, the Coaching Message displays upon first content request and then not again for 60 minutes. Click the Change link to set a different duration: Midnight or End of Session (browser close/reopen). Click Save.

3. To complete this non-conditional rule, click Finish. You can edit its elements, such as select categories to which coaching applies.
Policy Example—Prevent Unauthenticated User Access to Content

The **Who** element enables you to trigger the policy when a content request comes from a specific user, user type, or group, based on authentication. This example blocks all unauthenticated users (users on the network who did not log in with internal domain credentials—requires the Auth Connector) from accessing a company-sensitive information on a specific destination subnet.

1. In Solutions Mode, select **Content Filtering > Policy**.
   a. Click **Add Rule**. The service displays the Create New Rule wizard.
   b. Click **Add Sources**.
2. Click **Add Unauthenticated Users**.

![Add Sources](image)

3. Click **Save**.

4. This example prevents access to a specific subnet.
   a. Click **Add Destinations**.
   b. Click **IP/Subnets**.
   c. Click **New IPs/Subnets**. The wizard displays the Add IPs/Subnets page.
d. Enter the destination location and click **Add IPs/Subnets**.

e. Click **Save**.

5. For the **Verdict** construct, click **Block**.

6. Click **Add Rule**.

7. The **Advanced Policy Configuration** page displays the new rule, automatically ordering it correctly—after other existing **Block** rules.

8. Click **Activate**.
Allow Individuals Access to Blocked Content

You might find a need to allow certain individuals access to content that is blocked by policy. For example, you have a subnet that contains servers with company proprietary information and that destination is a blocked except for a specific group; however, a contractor not in the group requires access to complete report.

The Verdict construct in the Content Filtering policy editor allows you to set an override password that allows users who receive this password to bypass the blocked verdict.

**Note:** For coaching to properly function, browser settings must allow cookies.

1. In Solutions Mode, select **Content Filtering > Policy**.

2. Add a rule or Edit an existing rule (click the symbol in the Verdict column). If adding a new rule, look for the Verdict construct.

   a. Select **Block** and select **Password Override**.

   b. Click **Change**. The service displays the Edit Global Password Override Settings dialog.

   c. Define the **Override Password**.
d. (Optional) By default, the password prompt displays upon first content request and then not again for **60 minutes**. From the **Duration** drop-down list, select a different duration: **Midnight** (00:00) or **End of Session** (browser close/reopen).

e. Click **Save**.

3. To complete this non-conditional rule, click **Add Rule**. Either delete it or edit its elements, such as select blocked categories that allow for password override.
Create Policy From a Reported User

As you generate and view Web Security Service reports, you might observe suspicious activity from a client or user and want to instantly create a policy directly from the report.

This feature is only supported in reports that represent singular users, clients, and so on. Reports that display trends, for example, do not have this feature. Consider the following two use cases.

Use Case—Infected Client

You are reviewing the Potential Malware Infected Clients report and notice a large amount of suspicious activity from a specific client. You can instantly apply policy to block that client until you investigate and resolve.

1. In Solutions Mode, select Threat Protection > Reports and generate the Potential Malware Infected Clients report.
a. Select graphic element or table row. This is the user or client that requires a policy change.


2. Define the policy.

![New Rule: Content Filtering Group B - 13](image)

The policy editor automatically adds the suspect IP address to the **Sources** construct. Set the **Verdict** to **Block** and click **Add Rule**.

3. The policy creation switches the view to the **Content Filtering > Policy** page. Your new rule is viewable in the order added. If necessary, move it to another spot in the list (click the number link). For example, you want a rule for an individual to be evaluated before a group rule.

![Policy Page](image)

You must click **Activate** to enable the policy.

4. When you resolve this issue and want to restore the client back into production, return to this page, select the rule, and click **Delete** (or you can click Disable to temporarily halt the enforcement of a rule).
Use Case—User Misconduct

When browsing a user report, you notice that a particular user is abusing Web privileges and you want to create a policy that coaches this person.

1. In Solutions Mode, select Content Filtering > Reports and generate the Web Browsing per User and Category report.

   a. Scroll and scan the report to identify which users require coaching.

   b. Select a row that requires coaching.


2. Define the policy.
a. For this example, set the Verdict as **Allow With Coach**.

b. Click **Add Rule**.

3. The policy creation switches the view to the **Content Filtering > Policy** page. Your new policy is viewable in its proper place in the order of policy. **Show screen...**

You must click **Apply** to enforce the policy. Also, to see the current coaching message that is sent to users who trigger the policy, click the **Edit** icon in the **Verdict** column.
Create Policy Based on Reporting Usernames

The Symantec Web Security Service Content Filtering Rules policy editor allows you to create policy based on usernames that currently exist in the reporting database. Rather than using the Auth Connector to synchronize the full user/group list from the enterprise Active Directory (AD), this subset of username information comes from user credentials, such as the Windows login credentials. The following use cases illustrate the usefulness of this ability.

Use Case—Small Business/Unified Agent Only

Your Symantec Web Security Service account serves a small business, all your clients use the Unified Agent, and you do not need an Active Directory deployment. You can create global policies for all of these users and create specific policies for a few of the users.

Use Case—ProxySG Appliance With RADIUS Authentication

You want to use the Proxy Forwarding access method to send some users/groups to the Web Security Service, but do not have an LDAP environment. With Reporting Username Policy, you can write policy based on the forwarded usernames because they are part of the reporting database.

Create A Reporting Username Policy

1. In Solutions Mode, select Content Filtering > Policy.
   a. Click Add Rule. The service displays the Create New Rule page.
   b. Click Add Sources.
   c. Click User.
2. On the first wizard page, Who, click Users From Reporting.
a. Click From Reporting.

b. Select the Usernames for this policy.

3. Click Save and continue defining the rule as required.
Advanced Policy Example—Set Web Access Times

The **When** element triggers the policy when it matches a specified time frame. For this example, **Chat/Instant Messaging** is a globally blocked category. You decide to have a trial for one week that allows users to use instant messaging, but only Monday through Friday during the lunch time: 12:00 to 1:30 PM.

1. In Solutions modes, select **Content Filtering > Policy**.
2. Click **Add Rule**. The service displays the Create New Rule page.
   a. Click **Add Destinations**.
   b. Click **Web Application**.
3. Select the **Chat (IM/SMS)** category (you can also enter **chat** in the search field).
   a. Select the apps to add or the top-of-column option to add all.
   b. Click the **arrow-icon** to add the apps to the construct.
   c. Click **Save**.
4. Create a schedule construct.
   a. Click **Contents and Limits**.
   b. Click **Schedule**.
   c. Select **New > Schedule**.
d. **Name** the element. (Created elements display in lists and are selectable in other policy rules).

e. (Optional) Provide a descriptive **Comment**.

f. **Only between the following times of day**—Select **Enable** and specify the times. The interface uses a 24-hour clock; this example sets the **From** time to **1200** (12:00 PM) and the **To** time to **1330** (1:30 PM).

g. **Only on the following days of the week**—This example specifies to allow only on week days. Select **Enable** and select **Mon, Tue, Wed, Thu, and Fri**.

h. **Only between the following dates (inclusive)**—You can specify No End Date to keep the policy indefinitely. Or set a data range; for example, you want to test the policy on a trial basis and elicit feedback.

i. Click **Create Schedule and Add to 'When'**.

j. Click **Next**.

5. Click **Save**.

6. Click **Add Rule**.

7. The Content Filtering Rules page displays the new rule, automatically ordering it correctly—before the **Block** rules. A user attempting to instant message at any time other than 12:00 to 1:30 matches the global block rule (**Group B**).

8. Click **Activate**.
Policy Example—Define Policy For Mobile Users

If you have employees connecting to the Web Security Service from supported mobile devices, you can define a policy that applies specifically to that access method. For example, you have stringent policy that applies to corporate-owned desktops and laptops, but want to allow some leniency on allowable Content Filtering categories when the users access from a mobile device outside of business hours.

1. In Solutions Mode, select **Content Filtering > Policy**.
   a. Click **Add Rule**. The service displays the Create New Rule wizard.
   b. Click **Add Sources**.

2. Click **Add Mobile Devices**.

3. Click **Next** and continue to define the policy for mobile devices.
Policy Example—Block Application Actions

You have a set of users for which you want to block specific actions, such as uploading or downloading bandwidth-consuming content. For example, you do not want your guest WiFi users clogging the wireless resources.

1. In **Solutions** mode, select **Content Filtering > Policy**.
2. Click **Add Rule**. The service displays the Create New Rule page.
   a. Click **Add Sources**.
   b. This example applies to a previously created **Location**: HQGuestWiFi.
   c. Click **Save**.
3. Click **Contents and Limits**.
4. Click **Actions**; the service displays all of the currently supported content actions. Select network-expensive actions, such as **Upload Pictures** and **Upload Video** and click **Add**.
The default view is all actions for all web applications. To filter the view to display only valid actions for a specific application, select that application from the **Show Actions For** drop-down list (or enter text in the field).

5. Click **Save**.

6. Click **Add Rule**.

7. Click **Activate**.
Force Safe Searches

Safe Search refers to individual browser settings that allow or disallow displaying links to mature/inappropriate site and image results when using the browser’s search function. The Symantec Web Security Service provides the following browser search engine policy controls.

- Allow all search engines.
- Fully enforce Google’s Safe Search mode regardless of the client browser’s configuration. Google is the only search engine that the Web Security Service currently fully enforces. If you enable this option, select the policy action the service takes against requests to other engines.

**Tip:** When Safe Search is enabled, the Web Security Service performs minimal SSL interception, which is required for policy enforcement. This is regardless of the current SSL interception enabled/disabled state (*Network > SSL Interception*). If your employee base reports certificate warnings, deploy the Web Security Service trusted certificate. See "Install Encrypted Traffic Certificates" on page 102 and Examine Encrypted (HTTPS) Traffic.

1. In **Solutions** mode, select **Content Filtering > Search Controls. Show screen**...

![Search Controls screen](image)

2. Select **Enabled**.

3. Select the action for other search engine requests (as described above).
Note: This safe search engine feature is a modification for the October, 2015 Web Security Service update. If you had previously enabled Safe Search and specified actions for specific engines, the Web Security Service defaults to this policy: Enable Safe Search for Google Search and Allow Unsafe Searches.
Policy Reference

The following topics provide reference material relating to Web Security Service policy.

- "Reference: Updated Content Filtering Categories" on page 186
- "Reference: Role-Based Access Fields" on page 191
- "Reference: File Types Detected by Advanced Policy" on page 192
Reference: Updated Content Filtering Categories

This section lists and describes the Symantec Web Security Service Content Filtering categories. The October 2013 Web Security Service release (v6.2) contained a category name refresh and added these categories.

- **Computer/Information Security**
- **Internet Connected Devices**
- **Marijuana**
- **Piracy/Copyright Concerns**

Deprecated in October, 2013:

- **LGBT**–Sites have been moved to the appropriate content categories (such as Political/Social Advocacy, Personal Sites, Sexual Expression).
- **Pay-to-Surf**–Decreased popularity negates the need for a standalone category. Depending on legitimacy, sites go into Scam/Questionable/Illegal or other business categories.

The definitions below are the most current and might differ from previous descriptions even in cases where the category name remained unchanged.

[https://docs.broadcom.com/docs/webfilter-en](https://docs.broadcom.com/docs/webfilter-en)

<table>
<thead>
<tr>
<th>Name</th>
<th>Previous Name (if applicable)</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alcohol</td>
<td>Same</td>
<td>Sites that discuss, encourage, promote, offer, sell, supply, or otherwise advocate the use or creation of alcoholic beverages—including but not limited to beer, wine, and hard liquors. It does not include sites that sell alcohol as a subset of other products such as restaurants or grocery stores.</td>
</tr>
<tr>
<td>Chat (IM)/SMS</td>
<td>Chat/Instant Messaging</td>
<td>Sites that provide chat, text messaging (SMS), or instant messaging capabilities or client downloads.</td>
</tr>
<tr>
<td>Computer/Information Security</td>
<td>(New)</td>
<td>Sites that provide information or tools for securing or safeguarding computers, networks, and other data systems. While these sites provide helpful and legitimate security information to IT professionals, they also pose a degree of risk because information they provide might be used to help gain unauthorized access to systems.</td>
</tr>
<tr>
<td>Controlled Substances</td>
<td>Illegal Drugs</td>
<td>Sites that discuss, encourage, promote, offer, sell, supply or otherwise advocate the use, cultivation, manufacture, or distribution of non-pharmaceutical drugs, intoxicating plants, solvents or chemicals, and their related paraphernalia. Typically, these substances have no accepted medical use and a high potential for abuse. This category does <strong>not</strong> include alcohol, tobacco, or marijuana sites as these have dedicated categories.</td>
</tr>
<tr>
<td>Name</td>
<td>Previous Name (if applicable)</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>E-Card/Invitations</td>
<td>Greeting Cards</td>
<td>Sites that facilitate the sending of electronic greeting cards, invitations, or similar electronic messages typically used to mark an event or special occasion.</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Same</td>
<td>Sites that provide information about or promote popular culture including but not limited to film, film critiques and discussions, film trailers, box office, television, home entertainment, music, comics, graphic novels, literary news, and reviews. This category also includes entertainment-oriented periodicals, interviews, fan clubs, celebrity gossip, and podcasts; and music and film charts.</td>
</tr>
<tr>
<td>File Storage/Sharing</td>
<td>Online Storage</td>
<td>Sites and services that provide online file or note storage, file sharing, synchronization of files between devices and/or network-based data backup and restoration. These services might provide the means to upload, download, paste, organize, post and share documents, files, computer code, text, non-copyright-restricted videos, music and other electronically formatted information in virtual data storage. Does not include Web Applications or Media Sharing.</td>
</tr>
<tr>
<td>Financial Services</td>
<td>Same</td>
<td>Sites that provide or advertise banking services, lending services, insurance services, financial information, or advice on a variety of fiscal topics including loans. Does not include sites that offer market information, brokerage or trading services, which are categorized in the Brokerage/Trading category.</td>
</tr>
<tr>
<td>Hacking</td>
<td>Same</td>
<td>Sites that distribute, promote or provide tools or other information intended to help gain unauthorized or illegal access to computers, computer networks, or computerized communication and control systems. Includes “white-hat” tools used to test the security of existing systems, e.g., penetration testing tools. Also includes sites with instructions for creating or distributing malware or information on performing cyber attacks.</td>
</tr>
<tr>
<td>Health</td>
<td>Health</td>
<td>Sites that provide advice and information on general health such as fitness and well-being, personal health, medical services, over-the-counter and prescription medications, health effects of both legal and illegal drug use, alternative and complementary therapies, medical information about ailments, dentistry, optometry, and general psychiatry. Also includes self-help and support organizations dedicated to a disease or health condition.</td>
</tr>
<tr>
<td>Internet Connected Devices</td>
<td>(New)</td>
<td>Sites that allow management and monitoring of or network access to physical devices connected to the Internet. Such devices include but are not limited to network infrastructure such as routers and switches, network-enabled industrial equipment, security cameras, home automation equipment, and other Web-enabled devices. Also includes security camera feeds, which are dually categorized as TV/Video Streams.</td>
</tr>
<tr>
<td>Name</td>
<td>Previous Name (if applicable)</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malicious Sources/Malnets</td>
<td>Malicious Sources</td>
<td>Sites that host or distribute malware or whose purpose for existence is as part of a malicious network (malnet) or the malware ecosystem. Malware is defined as software that takes control of a computer, modifies computer settings, or collects or reports personal information without the permission of the end user. It also includes software that misrepresents itself by tricking users to download or install it or to enter personal information. This includes sites or software that perform drive-by downloads; browser hijackers; dialers; any program that modifies your browser homepage, bookmarks, or security settings; and keyloggers. It also includes any software that bundles malware (as defined above) as part of its offering. Information collected or reported is “personal” if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as malware if the user is reasonably notified that the software will perform these actions (for example, it alerts that it will send personal information, be installed, or that it will log keystrokes).</td>
</tr>
<tr>
<td>Marijuana</td>
<td>(New)</td>
<td>Sites that discuss, encourage, promote, offer, sell, supply or otherwise advocate the use, cultivation, manufacture or distribution of marijuana and its myriad aliases, whether for recreational or medicinal purposes. Includes sites with content regarding marijuana-related paraphernalia.</td>
</tr>
<tr>
<td>Mixed Content/Potentially Adult</td>
<td>Open/Mixed Content</td>
<td>Sites with generally non-offensive content but that also have potentially objectionable content such as adult or pornographic material that is not organized so that it can be classified separately. Sites that explicitly exclude offensive, adult, and pornographic content are not included in this category.</td>
</tr>
<tr>
<td>Non-Viewable/Infrastructure</td>
<td>Non-Viewable</td>
<td>Servers that provide Internet infrastructure services and information used by applications but not necessarily viewable by web browsers. Includes security services such as security patch downloads, anti-virus database updates, content filtering systems, shared authentication services, and certificate management services such as OCSP and CRL services. Traffic and content in this category is neither malicious nor objectionable in nature and may be required for applications or network traffic to function properly.</td>
</tr>
<tr>
<td>Office/Business Applications</td>
<td>Web Applications</td>
<td>Sites with interactive, Web-based office, productivity, collaboration, and business applications including business enablement services. Excludes email, chat/IM, or other sites that have a specific content category.</td>
</tr>
<tr>
<td>Personal Sites</td>
<td>Blogs/Personal Pages</td>
<td>Sites consisting primarily of user-generated content that serves as a vehicle for self-promotion on which a variety of personal experiences or interests are shared. These sites do not represent businesses, institutions or governmental entities although they might mention or be sponsored by such bodies. Content on these sites tends to be dynamic in nature. Content topic and tone may vary from benign to extreme or vacillate between the two as determined by the author. Reader comments might also contain mixed content.</td>
</tr>
<tr>
<td>Name</td>
<td>Previous Name (if applicable)</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Piracy/Copyright Concerns</td>
<td>(New)</td>
<td>Sites that provide information or technology for cracking or pirating software or other protected intellectual property, and sites that distribute such media.</td>
</tr>
<tr>
<td>Political/Social Advocacy</td>
<td>Political/Activist Groups</td>
<td>Sites sponsored by groups or individuals that provide information on political parties, special interest groups, organizations, factions or individuals that promote change or reform in public policy, public opinion, social practice, social justice, or related economic activities. Includes sites that advance political or social agendas, lobby for political or social change, facilitate civic engagement, and advocate personal or collective action in its multiple forms including but not limited to petitioning, boycotts, and demonstrations.</td>
</tr>
<tr>
<td>Scam/Questionable/Illegal</td>
<td>Same</td>
<td>Sites that advocate or give advice on performing acts that are illegal or of questionable legality such as service theft, evading law enforcement, fraud, burglary techniques, and plagiarism. Also includes sites that promote scams such as work-from-home, pay-to-surf, and Ponzi schemes and sites that provide or sell legally questionable educational materials such as term papers.</td>
</tr>
<tr>
<td>Sexual Expression</td>
<td>Alternative Sexuality/Lifestyles</td>
<td>Sites that provide information about, promote, or cater to sexual expression and sexual identity in all its forms including the full range of sexual practices, interests, orientations, and fetishes. Does not include sex education which is categorized in the Sex Education category or content that is sexually gratuitous in nature, which is categorized in the Pornography or Extreme categories.</td>
</tr>
<tr>
<td>Software Downloads</td>
<td>Same</td>
<td>Sites wholly dedicated to the download of software for any type of computer or computing device whether for payment or at no charge. Does not include sites or pages that offer a software download as a subset of their overall content.</td>
</tr>
<tr>
<td>Technology/Internet</td>
<td>Computers/Internet</td>
<td>Sites that sponsor or provide information, news, reviews, opinions and coverage of computing, computing devices and technology, consumer electronics, and general technology. Also includes sites of technology-related organizations and companies.</td>
</tr>
<tr>
<td>Tobacco</td>
<td>Same</td>
<td>Sites that discuss, encourage, promote, offer, sell, supply, or otherwise advocate the use or creation of tobacco or tobacco-related products including but not limited to traditional or electronic cigarettes, pipes, cigars, chewing tobacco, hookahs, or nicotine delivery systems. Does not include sites that sell tobacco as a subset of other products such as grocery stores.</td>
</tr>
<tr>
<td>Uncategorized</td>
<td>Unrated</td>
<td></td>
</tr>
<tr>
<td>Web Ads/Analytics</td>
<td>Web Ads</td>
<td>Sites that provide online advertisements, banners, or the means to identify and market to existing or potential customers based on their browsing or online purchasing habits including but not limited to Web analytics sites such as visitor tracking and ranking sites. Includes social plugins and analytics that allow site visitors to share, vote for, or signal their appreciation of a site or its content (e.g., Facebook “Like” or Google “+1” plugins).</td>
</tr>
<tr>
<td>Name</td>
<td>Previous Name (if applicable)</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web Hosting</td>
<td>Same</td>
<td>Sites of organizations that provide top-level domain pages, as well as web communities, blog hosting sites, and other hosting services.</td>
</tr>
</tbody>
</table>
Reference: Role-Based Access Fields

- **Client IP**—The IP address of the system that initiated the web request.
- **Status**—Status code returned from server.
- **Protocol**—The content protocol type; for example, HTTP, FTP.
- **Site**—The name of the requested website.
- **User**—The user name (if the access method supported authentication).
- **Content Type**—Type of content returned; for example: text/html, text/plain, application/xml, application/x-javascript.
- **User Agent**—The client application that performed the request; for example, the browser type and version.
- **Verdict**—Policy block or allow.
- **Malware**—The name of the detected malware/virus.
- **Category**—The content filtering category.
- **Port**—The port number used to broadcast the request.
- **Search Term**—Text strings entered into browser search engines.
- **Web Application**—The name of the application used to generate the request; for example, Sales Force, Facebook.
- **Web Application Action**—
- **Location**—Location name of the originating traffic as configured in the Web Security Service.
- **Risk Group**—This content might belong a risk group.
- **Subnet**—The subnet to which the requesting IP address belongs.
Reference: File Types Detected by Advanced Policy

The Symantec Web Security Service Advanced Policy Configuration wizard (Solutions Mode > Content Filtering > Policy > Add Rule wizard > Contents and Limits construct) allows you to select File Type categories to block or allow. The following lists provide the recognized file extensions for each category.

Active Content

- Applet—Java applets
- Embed—plugins
- object—ActiveX controls
- script—JavaScripts, VPScript, and more

Archives and Compressed Files

- Q?—files compressed by the SQ program.
- 7z—7-Zip compressed file.
- ace—ACE compressed file
- ALZ—Alzip compressed file
- AT3—Sony's UMD Data compression
- bke—BackupEarth.com Data compression
- ARC
- ARJ—ARJ compressed file
- BA—Scifer Archive (.ba), Scifer External Archive Type
- big—Special file compression format used by Electronic Arts for compressing the data for many of EA's games
- BIK, bi—Bink Video file. A video compression system developed by RAD Game Tools
- BKF, bkf—Microsoft backup created by NTBACKUP.EXE
- bzip2, bz2"
- bmp—Paint
- c4—JEDMICS image files, a DOD system
- cab—Microsoft Cabinet
- cals—JEDMICS image files, a DOD system
- cpt, sea—Compact Pro (Macintosh)
- DAA—Closed-format, Windows-only compressed disk image
- deb—Debian Linux install package
- DMG—An Apple compressed/encrypted format
- EEA—An encrypted CAB, ostensibly for protecting e-mail attachments
- egg—Alzip Egg Edition compressed file
- EGT—(.egt) EGT Universal Document also used to create compressed cabinet files replaces .ecab
- ECAB—(.ECAB, .ezip) EGT Compressed Folder used in advanced systems to compress entire system folders, replaced by EGT Universal Document
- ESS—(.ess) EGT SmartSense File, detects files compressed using the EGT compression system.
- GHO—(.gho, .ghs); Norton Ghost
- gzip—(.gz); Compressed file
- IPG—(.ipg) Format in which Apple Inc. packages their iPod games. can be extracted through Winrar
- jar—ZIP file with manifest for use with Java applications.
- LBR—Library file
- LQR—LBR Library file compressed by the SQ program.
- LHA—Lempel, Ziv, Huffman
- Lza—Lempel, Ziv, Huffman
- lzo
- lzma
- lzx
- MPQ—Used by Blizzard games
- bin—MacBinary
- PAK—Enhanced type of .ARC archive
- par—par archives
- par2—par archives
- pk3—Quake 3 archive (.pk3) (See note on Doom³)
- pk4—Doom³ archive (.pk4) (Opens similarly to a zip archive.)
- RAR—Rar Archive (.rar), for multiple file archive (rar to .r01-.r99 to s01 and so on)
- SEN—Scifer Archive (.sen), Scifer Internal Archive Type
- sit—Stufflt (Macintosh)
- sitx—Stufflt (Macintosh)
- tgz—gzipped tar file
- tar
- tar.gz—gzipped tar file
- gz—gzipped tar file
- TB—Tabbery Virtual Desktop Tab file
- TIB—Acronis True Image backup
- uha—Ultra High Archive Compression
- VIV—Archive format used to compress data for several video games, including Need For Speed: High Stakes.
- VOL—Unknown archive
- VSA—Altiris Virtual Software Archive
- Z—Unix compress file
- zoo
- zip

Audio and Music Files

**Lossless Audio**
- AIFF—Audio Interchange File Format
- AU
- CDDA
- IFF-8SVX
- IFF-16SV
- RAW—Raw samples without any header or sync
- WAV—Microsoft Wave
- FLAC—Free lossless codec of the Ogg project
- LA—Lossless Audio (.la)
- PAC—LPAC (.pac)
- M4A—Apple Lossless (M4A)
- APE—Monkey’s Audio (APE)
- RKA—RKAU (.rka)
- SHN—Shorten (SHN)
- TTA—Free lossless audio codec (True Audio)
- WV—WavPack (.wv)
- WMA—Windows Media Audio 9 Lossless (WMA)

### Lossy Audio
- AMR—For GSM and UMTS based mobile phones
- MP2—MPEG Layer 2
- MP3—MPEG Layer 3
- Speex—Ogg project, specialized for voice, low bitrates
- GSM—GSM Full Rate, originally developed for use in mobile phones
- WMA—Windows Media Audio (.WMA)
- AAC—(.m4a, .mp4, .m4p, .aac); Advanced Audio Coding (usually in an MPEG-4 container)
- MPC—Musepack
- VQF—Yamaha TwinVQ
- RA—Real Audio
- RM—Real Audio
- OTS—Audio File (similar to MP3, with more data stored in the file and slightly better compression; designed for use with OtsLabs' OtsAV)
- SWA—Macromedia Shockwave Audio (Same compression as MP3 with additional header information specific to Macromedia Director)
- VOX—Dialogic ADPCM Low Sample Rate Digitized Voice (VOX)
- VOC—Creative Labs Soundblaster Creative Voice 8-bit & 16-bit (VOC)
- DWD—DiamondWare Digitized (DWD)
- SMP—Turtlebeach SampleVision (SMP)

### Other Music Formats
- AUP—Audacity project file
- BAND—GarageBand music
- CUST—DeliPlayer custom sound file format
- MID”—Standard MIDI file; most often just notes and controls but occasionally also sample dumps
- MUS—Finale Notation file, see also Finale (software)
- SIB—Sibelius Notation file, see also Sibelius (computer program)
- LY—LilyPond Notation file, see also GNU LilyPond
- GYM—Sega Genesis YM2612 log
- VGM—Stands for Video Game Music, log for several different chips
- PSF—Portable Sound Format
- NSF—NES Sound Format, bytecode program to play NES music
- MOD—Soundtracker and Protracker sample and melody modules
- PTB—Power Tab Editor tab
- S3M—Scream Tracker 3 module, with a few more effects and a dedicated volume column
- XM—Fast Tracker module, adding instrument envelopes
- IT—Impulse Tracker module, adding compressed samples, note-release actions, and more effects including a resonant filter
- MT2—MadTracker 2 module. It could be resumed as being XM and IT combined with more features like track effects and automation.)
- MNG—BGM for the Creatures game series, starting from Creatures 2; a free editor and player is available
- PSF—PlayStation Sound Format.
- RMJ—RealJukebox Media used for RealPlayer.
- SPC—Super Nintendo Entertainment System sound file format.
- NIFF—Notation Interchange File Format
- MusicXML
- TXM—Track ax media.
- YM—Atari ST/Amstrad CPC YM2149 sound chip format
- JAM—Jam music format
- ASF—Advanced Systems Format
- MP1—For use with UltraPlayer

**Playlist Formats**
- ASX—Advanced Stream Redirector (.asx)
- M3U
- PLS
- RAM—Real Audio Metafile For Real Audio files only.
- XSPF—XML Shareable Playlist Format
- ZPL—Zune Playlist format

**Audio Editing and Music Production Formats**
- AUP—Audacity project file
- BAND—GarageBand project file
- CEL—Adobe Audition loop file (Cool Edit Loop)
- CPR—Steinberg Cubase project file
- NPR—Steinberg Nuendo project file
- CWP—Cakewalk Sonar project file
- DRM—Steinberg Cubase drum file
- OMF—Cross-application format Open Media Framework application-exchange bundled format
- SES—Adobe Audition multitrack session file
- SNG—MIDI sequence file (MidiSoft, Korg, etc.) or n-Track Studio project file
- STF—StudioFactory project file. It contains all necessary patches, samples, tracks and settings to play the file.
- SYN—SynFactory project file. It contains all necessary patches, samples, tracks and settings to play the file.
- SND—Akai MPC sound file

**Computer-Aided Design (CAD)**

- 3dmlw—3DMLW (3D Markup Language for Web) files
- 3dxml—Dassault Systemes graphic representation
- ACP—VA Software VA" ; Virtual Architecture CAD file
- AR—Ashlar-Vellum Argon" ; 3D Modeling
- ART—ArtCAM model
- ASC—BRL-CAD Geometry File (old ascii format)
- ASM—Solidedge Assembly, Pro/ENGINEER Assembly
- BIN, BIM—Data Design System DDS-CAD
- CCC—CopyCAD Curves
- CCM—CopyCAD Model
- CCS—CopyCAD Session
- CAD—CadStd
- CATDrawing—CATIA V5 Drawing document
- CATPart—CATIA V5 Part document
- CATProduct—CATIA V5 Assembly document
- CATProcess—CATIA V5 Manufacturing document
- cgr—CATIA V5 graphic representation file
- CO—Ashlar-Vellum Cobalt; parametric drafting and 3D modeling
- DRW—Caddie Early version of Caddie drawing; Prior to Caddie changing to DWG
- DWG—AutoCAD and Open Design Alliance applications
- DFT—Solidedge Draft
- DGN—MicroStation design file
- DGK—Delcam Geometry
- DMT—Delcam Machining Triangles
- DXF—ASCII Drawing Interchange file format; AutoCAD
- DWB—VariCAD drawing file
- DWF—AutoDesk’s Web Design Format; AutoCAD & Revit can publish to this format; similar in concept to PDF files; AutoDesk Design Review is the reader
- EMB—Wilcom; Wilcom ES Designer Embroidery CAD file
- ESW—Agtek format
- EXCELLON, or Excellon file
- FM—FeatureCAM Part File
- FMZ—FormZ Project file
- G—BRL-CAD Geometry File
- GERBER or Gerber file
- GRB—T-FLEX CAD File
- GTC—GRAITEC Advance file format
- IAM—Autodesk Inventor Assembly file
- ICD—IronCAD 2D CAD file
- IDW—Autodesk Inventor Drawing file
- IFC—BuildingSMART for sharing AEC and FM data
- IGES—Initial Graphics Exchange Specification
- Intergraph's Intergraph Standard File Formats
- IPN—Autodesk Inventor Presentation file
- IPT—Autodesk Inventor Part file
- model—CATIA V4 part document
- PAR—Solidedge Part
- PRT—NX (recently known as Unigraphics), Pro/ENGINEER Part, CADKEY Part
- PLN—ArchiCad project
PSM—Solidedge Sheet
PSMODEL—PowerSHAPE Model
PWI—PowerNSPECT File
PYT—Pythagoras File
SKP—SketchUp Model
RLF—ArtCAM Relief
RVT—AutoDesk Revit project files
RFA—AutoDesk Revit family files
SLDASM—SolidWorks Assembly drawing
SLDDRW—SolidWorks 2D drawing
SLDPRT—SolidWorks 3D part model
STEP—Standard for the Exchange of Product model data
STL—Stereo Lithographic data format (see STL (file format)) used by various CAD systems and stereo lithographic printing machines.
TCT—TurboCAD drawing template
TCW—TurboCAD for Windows 2D and 3D drawing
VC6—Ashlar-Vellum Graphite; 2D and 3D drafting
VLM—Ashlar-Vellum Vellum, Vellum 2D, Vellum Draft, Vellum 3D, DrawingBoard
VS—Ashlar-Vellum Vellum Solids
WRL—Similar to STL, but includes color. Used by various CAD systems and 3D printing rapid prototyping machines. Also used for VRML models on the Web.
XE—Ashlar-Vellum Xenon; for Associative 3D Modeling
brd—EAGLE Layout Editor Board File; Eagle is Commercial EDA software for designing PCBs (printed circuit boards).
OASIS—Open Artwork System Interchange Standard
VHD—A VHDL source file
MS10—NI Multisim file

Databases

ACCDB—Microsoft Database (Microsoft Office Access 2007)
ADT—Sybase Advantage Database Server (ADS)
APR—Lotus Approach data entry & reports
- BOX—Lotus Notes Post Office mail routing database
- CHML—Krasbit Technologies Encrypted database file for 1 click integration between contact management software and the Chameleon(tm) line of imaging workflow solutions
- DAF—Digital Anchor data file
- DAT—DOS Basic
- DB—Paradox
- DBF—db/database II,III,IV and V, Clipper, Harbour/xHarbour, Fox/FoxPro, Oracle
- EGT—EGT Universal Document, used to compress sql databases to smaller files, might contain original EGT database style.
- ESS—EGT SmartSense is a database of files and its compression style. Specific to EGT SmartSense
- EAP—Enterprise Architect Project
- FDB—Firebird Databases
- FDB—Navision database file
- FP, FP3, FP5, FP7—FileMaker Pro
- FRM—MySQL table definition
- GDB—Borland InterBase Databases
- KEXI—Kexi database file (SQLite-based)
- KEXIC—Shortcut to a database connection for a Kexi databases on a server
- LDB—Temporary database file, only existing when database is open
- MDB, mdb, ldb—Microsoft Database (Access)
- ADP—Microsoft Access project (used for accessing databases on a server)
- MDE—Compiled Microsoft Database (Access)
- MDF—Microsoft SQL Server Database
- MYD—MySQL MyISAM table data
- MYI—MySQL MyISAM table index
- NCF—Lotus Notes configuration file
- NSF—Lotus Notes database
- NTF—Lotus Notes database design template
- ODB—OpenOffice.org Base
- ORA—Oracle tablespace files sometimes get this extension (also used for configuration files)
- PDB—Palm OS Database
- PDI—Portable Database Image
- PDX—Corel Paradox database management
- PRC—Palm OS resource database
- SQL—Bundled SQL queries
- REL—Sage Retrieve 4GL data file
- RIN—Sage Retrieve 4GL index file
- SDB—StarOffice's StarBase
- UDL—Universal Data Link
- WDB—Microsoft Works Database

**Desktop Publishing**

- DTP—Greenstreet Publisher, GST PressWorks
- INDD—Adobe InDesign
- MCF—FotoInsight Designer
- PMD—Adobe PageMaker
- PUB—Microsoft Publisher
- FM—Adobe FrameMaker

**Disc Images**

- ISO—The generic file format for most optical media, including CD-ROM, DVD-ROM, Blu-ray Disc, HD DVD and UMD
- NRG—The proprietary optical media archive format used by Nero applications
- IMG—For archiving MS-DOS formatted floppy disks.
- ADF—Amiga Disk Format, for archiving Amiga floppy disks
- ADZ—The GZip-compressed version of ADF
- DMS—Disk Masher System, a disk-archiving system native to the Amiga
- DSK—For archiving floppy disks from a number of other platforms, including the ZX Spectrum and Amstrad CPC
- D64—An archive of a Commodore 64 floppy disk
- SDI—System Deployment Image, used for archiving and providing “virtual disk” functionality
- MDS—DAEMON tools native disc image file format used for making images from optical CD-ROM, DVD-ROM, HD DVD or Blu-ray Disc. It comes together with MDF file and can be mounted with DAEMON Tools or Alcohol 120% software.
MDX—New DAEMON Tools file format that allows to get one MDX disc image file instead of two (MDF and MDS)

DMG—Macintosh disk image files

Executables

The Web Security Service detection of executables involves more than just detecting file extensions; it involves the following methods.

- HTTP File Extensions
- Magic Bytes
- HTTP Response Headers
- Content Dispositions

### HTTP File Extensions

<table>
<thead>
<tr>
<th>8BF</th>
<th>APP</th>
<th>BPL</th>
<th>class</th>
<th>COFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>com</td>
<td>DCU</td>
<td>DOL</td>
<td>EAR</td>
<td>EGT</td>
</tr>
<tr>
<td>ELF</td>
<td>jar</td>
<td>XPI</td>
<td>Mach-O</td>
<td>nlm</td>
</tr>
<tr>
<td>s1es</td>
<td>VAP</td>
<td>WAR</td>
<td>XBE</td>
<td>XCOFF</td>
</tr>
<tr>
<td>VBX</td>
<td>ocx</td>
<td>TLB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### HTTP Response Headers

- `application/octet-stream` (might cause false-positives)
- `application/x-msdownload`
- `application/x-msdos-program`
- `(application|image)/(x- | x-ms | x-win- |)(metafile | wmf)

### Content Dispositions

<table>
<thead>
<tr>
<th>ani</th>
<th>bat</th>
<th>chm</th>
<th>cmd</th>
<th>com</th>
</tr>
</thead>
<tbody>
<tr>
<td>cur</td>
<td>dll</td>
<td>exe</td>
<td>hta</td>
<td>hlp</td>
</tr>
<tr>
<td>msi</td>
<td>pif</td>
<td>reg</td>
<td>scr</td>
<td>vb</td>
</tr>
<tr>
<td>vbs</td>
<td>wmf</td>
<td>wsc</td>
<td>wsf</td>
<td>wsh</td>
</tr>
</tbody>
</table>

### Fonts

- **ABF**—Adobe Binary Screen Font
- **AFM**—Adobe Font Metrics
- **BDF**—Bitmap Distribution Format
- **BMF**—ByteMap Font Format
- **FNT**—Bitmapped Font; Graphical Environment Manager
- **FON**—Bitmapped Font; Microsoft Windows
Gaming

List of common file formats of data for video games on systems that support filesystems, most commonly PC games.

HALO Engine

- MAP—A Level, User Interface, or Sounds
- TAG—An Object
- SAV—A saved game
- LEV—A HALO ZERO Level

TrackMania United/Nations Forever Engine

- CHALLENGE.GBX—(Edited) Challenge files.
- CONSTRUCTIONCAMPAIGN.GBX—Construction campaignes files.
- CONTROLEFFECTMASTER.GBX—Menu parts.
- CONTROLSTYLE.GBX—Menu parts.
- FIDCACHE.GBX—Saved game.
- GBX—Other TrackMania items.
- REPLAY.GBX—Replays of races.

DOOM Engine

- DEH—DeHackEd files to mutate the game executable (not officially part of the DOOM engine)
- DSG—Saved game
LMP—A lump is an entry in a DOOM wad.
LMP—Saved demo recording
MUS—Music file (usually contained within a WAD file)
WAD—Data storage (contains music, maps, and textures)

Quake Engine
BSP—(For Binary space partitioning) compiled map format
MAP—Raw map format used by editors like GtkRadiant or QuArK
MDL—Model for an item used in the game
MD2—Model for an item used in the game
MD3—Model for an item used in the game
MD5—Model for an item used in the game
GLM—Model for an item used in the game
PAK—Data storage
PK2—Data storage
PK3—Used by the Quake II, Quake III Arena and Quake 4 game engines, respectively, to store game data, textures etc. They are .zip files.
PK4—Used by the Quake II, Quake III Arena and Quake 4 game engines, respectively, to store game data, textures etc. They are .zip files.
dat—General data contained within the .PK3/PK4 files
roq—Video format

Unreal Engine
U—Unreal script format
UAX—Animations format for Unreal Engine 2
UMX—Map format for Unreal Tournament
UMX—Music format for Unreal Engine 1
UNR—Map format for Unreal
UPK—Package format for cooked content in Unreal Engine 3
USX—Sound format for Unreal Engine 1 and Unreal Engine 2
UT2—Map format for Unreal Tournament 2003 and Unreal Tournament 2004
UT3—Map format for Unreal Tournament 3
- UTX—Music format for Unreal Engine 1 and Unreal Engine 2
- UXX—Cache format. These are files that client downloaded from server (which can be converted to regular formats)

**Duke Nukem 3D Engine**
- DMO—Save game
- GRP—Data storage
- MAP—Map (usually constructed with BUILD.EXE)

**Diablo Engine**
- SV—Save Game
- ITM—Item File

**Other Formats**
- B—Grand Theft Auto saved game files
- BO—Levels on Poing!PC
- DBPF—The Sims 2, DBPF, Package
- GC—Format used by the Steam content management system for file archives.
- IMG—Format used by Renderware-based Grand Theft Auto games for data storage
- MAP—Format used by Halo: Combat Evolved for archive compression, Doom³, and various other games
- OEC—Format used by OE-Cake for scene data storage.
- POD—Format used by Terminal Reality
- REP—Used by Blizzard Entertainment for scenario replays in StarCraft.
- SC4Lot—SimCity (All game plugins use this format, commonly with different file extensions)
- SC4Model—SimCity (All game plugins use this format, commonly with different file extensions)
- SMZIP—Auto extractor for Stepmania songs, themes and announcer packs.

**Geographic Information System**
- APR—ESRI ArcView 3.3 and earlier project file
- DEM—USGS DEM file format
- E00—ARC/INFO interchange file format
- GeoTIFF—Geographically located raster data
- GPX—XML-based interchange format
- MXD—ESRI ArcGIS project file, 8.0 and higher
- SHP—ESRI shapefile
- TAB—MapInfo Table file format
- DTED—Digital Terrain Elevation Data
- KML—Keyhole Markup Language, XML-based

Graphic Images/Pictures

Color Palettes
- ACT—Adobe Color Table. Contains a raw color palette and consists of 256 24-bit RGB colour values.
- PAL—Microsoft palette file

Raster Graphics
- ASE—Adobe Swatch
- ART—America Online proprietary format
- BMP—Microsoft Windows Bitmap formatted image
- BLP—Blizzard Entertainment proprietary texture format
- CIT—Intergraph is a monochrome bitmap format
- CPT—Corel PHOTO-PAINT image
- CUT—Dr. Halo image file
- DDS—DirectX texture file
- DIB—Device-Independent Bitmap graphic
- DjVu—DjVu for scanned documents
- EGT—EGT Universal Document, used in EGT SmartSense to compress *.png to yet a smaller file
- Exif—Exchangeable image file format (Exif) is a specification for the image file format used by digital cameras
- GIF—CompuServe’s Graphics Interchange Format
- GPL—GIMP Palette, using a textual representation of color names and RGB values
- ICNS—file format use for icons in Mac OS X. Contains bitmap images at multiple resolutions and bitdepths with alpha channel.
- ICO—A file format used for icons in Microsoft Windows. Contains small bitmap images at multiple resolutions and sizes.
- .lbm—(,.iff, .ilbm, .lbm)" ; ILBM
- .ilbm—(,.iff, .ilbm, .lbm)" ; ILBM
- JNG—A single-frame MNG using JPEG compression and possibly an alpha channel.
- JPEG—JFIF (.jpg or .jpeg); a lossy image format widely used to display photographic images.
- JPG—JFIF (.jpg or .jpeg)*; a lossy image format widely used to display photographic images.
- JP2—JPEG2000
- LBM—Deluxe Paint image file
- MAX—ScanSoft PaperPort document
- MIFF—ImageMagick's native file format
- MNG—Multiple Network Graphics, the animated version of PNG
- MSP—A file format used by old versions of Microsoft Paint. Replaced with BMP in Microsoft Windows 3.0
- NITF—A U.S. Government standard commonly used in Intelligence systems
- OTA—A specification designed by Nokia for black and white images for mobile phones
- PBM—Portable bitmap
- PC1—Low resolution, compressed Degas picture file
- PC2—Medium resolution, compressed Degas picture file
- PC3—High resolution, compressed Degas picture file
- PCF—Pixel Coordination Format
- PCX—A lossless format used by ZSoft's PC Paint, popular at one time on DOS systems.
- PDN—Paint.NET image file
- PGM—Portable graymap
- PI1—Low resolution, uncompressed Degas picture file
- PI2—Medium resolution, uncompressed Degas picture file. Also Portrait Innovations encrypted image format.
- PI3—High resolution, uncompressed Degas picture file
- PICT—Apple Macintosh PICT image
- PCT—Apple Macintosh PICT image
- PNG—Portable Network Graphic (lossless, recommended for display and edition of graphic images)
- PNM—Portable anymap graphic bitmap image
- PPM—Portable Pixmap (Pixel Map) image
- PSB—Adobe Photoshop Big image file (for large files)
- PDD—Adobe Photoshop Drawing
- PSD—Adobe Photoshop Drawing
- PSP—Paint Shop Pro image
- PX—Pixel image editor image file
- PXR—Pixar Image Computer image file
- QFX—QuickLink Fax image
- RAW—General term for minimally processed image data (acquired by a digital camera)
- RLE—A run-length encoded image
- SCT—Scitex Continuous Tone image file
- SGI, RGB, INT. BW—Silicon Graphics Image
- tga—Truevision TGA (Targa) image
- targa—Truevision TGA (Targa) image
- icb—Truevision TGA (Targa) image
- vda—Truevision TGA (Targa) image
- vst—Truevision TGA (Targa) image
- pix—Truevision TGA (Targa) image
- TIFF—Tagged Image File Format (usually lossless, but many variants exist, including lossy ones)
- tif—ISO 12234-2; tends to be used as a basis for other formats rather than in its own right.
- XBM—X Window System Bitmap
- XCF—GIMP image (from Gimp’s origin at the eXperimental Computing Facility of the University of California)
- XPM—X Window System Pixmap

Vector graphics
- AWG—Ability Draw
- AI—Adobe Illustrator Document
- EPS—Encapsulated Postscript
- CDR—CorelDRAW vector image
- CMX—CorelDRAW vector image
- DXF—ASCII Drawing Interchange file Format, used in AutoCAD and other CAD-programs
- E2D—2-dimensional vector graphics used by the editor which is included in JFire
- EGT—EGT Universal Document, EGT Vector Draw images are used to draw vector to a website
- SVG—Scalable Vector Graphics, employs XML
- STL—Stereo Lithographic data format (see STL (file format)) used by various CAD systems and stereo lithographic printing machines. See the Computer Aided Design section above.
- wrl—Virtual Reality Modeling Language, for the creation of 3D viewable web images.
- X3D
- V2D—Voucher design used by the voucher management included in JFire
- WMF—Windows Meta File
- EMF—Enhanced (Windows) MetaFile, an extension to WMF
- ART—Xara; Drawing (superseded by XAR)
- XAR—Xara; Drawing

3D graphics
- 3DMF—QuickDraw 3D Metafile (.3mf)
- 3DS—Legacy 3D Studio Model (.3ds)
- AC—AC3D Model (.ac)
- AN8—Anim8or Model (.an8)
- AOI—Art of Illusion Model (.aoi)
- B3D—Blitz3D Model (.b3d)
- BLEND—Blender (.blend)
- BLOCK—Blender encrypted blend files (.block)
- C4D—Cinema 4D (.c4d)
- Cal3D—Cal3D (.cal3d)
- CCP4—X-ray crystallography voxels (electron density)
- CFL—Compressed File Library (.cfl)
- COB—Caligari Object (.cob)
- CORE3D—Coreona 3D Coreona 3D Virtual File(.core3d)
- CTM—OpenCTM (.ctm)
- DAE—COLLADA (.dae)
- DFF—RenderWare binary stream, commonly used by Grand Theft Auto III-era games as well as other RenderWare titles
- DTS—Torque Game Engine (.dts)
- EGG—Panda3D Engine
- FACT—Electric Image (.fac)
- FBX—Autodesk FBX (.fbx)
- G—BRL-CAD geometry (.g)
- GLM—Ghoul Mesh (.glm)
- LWO—Lightwave Object (.lwo)
- LWS—Lightwave Scene (.lws)
- LXO—Luxology Modo (software) file (.lxo)
- MA—Autodesk Maya ASCII File (.ma)
- MAX—Autodesk 3D Studio Max file (.max)
- MB—Autodesk Maya Binary File (.mb)
- MD2—Quake 2 model format (.md2)
- MD3—Quake 3 model format (.md3)
- MDX—Blizzard Entertainment’s own model format (.mdx)
- MESH—New York University (.m)
- MESH—Meshwork Model (.mesh)
- MM3D—Misfit Model 3d (.mm3d)
- MRC—Voxels in cryo-electron microscopy
- NIF—Gamebryo NetImmerse File (.nif)
- OBJ—OBJ (.obj)
- OFF—OFF Object file format (.off)
- PRC—Adobe PRC (embedded in PDF files)
- POV—POV-Ray Document (.pov)
- RWX—RenderWare Object (.rwx)
- SIA—Nevercenter Silo Object (.sia)
- SIB—Nevercenter Silo Object (.sib)
- SKP—Google Sketchup file (.skp)
- SLDASM—SolidWorks Assembly Document (.sldasm)
- SLDprt—SolidWorks Part Document (.sldprt)
- SMD—Valve’s format (.smd)
- U3D—Universal 3D file format (.u3d)
- WINGS—Wings3D (.wings)
- X—DirectX 3D Model (.x)
- X3D—Extensible 3D (.x3d)
- Z3D—Zmodeler (.z3d)
Miscellaneous

Other

- **AXD**—Cookie extensions found in temporary internet folder
- **AXX**—Encrypted file, created with Axcrypt
- **BAK**—Backup file
- **BDF**—Binary Data Format; raw data from recovered blocks of unallocated space on a hard drive
- **CREDX**—CredX Dat File
- **DUPX**—DupeCheck database management tool project file
- **GA3**—Graphical Analysis 3
- **GED**—GEDCOM, (GEnealogical Data COMmunication) file format for exchanging genealogical data between different genealogy software.
- **HLP**—Windows help file
- **IGC**—Flight tracks downloaded from GPS devices in the FAI’s prescribed format
- **INI**—Ini file used by many applications to store configuration
- **INF**—Similar file format to INI; used to install device drivers under Windows, inter alia.
- **KMC**—Tests made with KatzReview’s MegaCrammer
- **LNK**—Binary format file, stores shortcuts under MS Windows 95 and later
- **LSM**—LSMaker script file (program using layered .jpg to create special effects; specifically designed to render lightsabers from the Star Wars universe) (.lsm)
- **PIF**—Used for running MS-DOS programs under Windows
- **POR**—Portable SPSS files, readable by PSPP
- **PXZ**—Compressed file to exchange media elements with PSALMO
- **RISE**—File containing RISE generated information model evolution
- **TOPC**—TopicCrunch SEO Project file holding keywords, domain and search engine settings (ASCII);
- **TOS**—Character file from The Only Sheet
- **TMP**—Temporary file
- **URL**—INI format file, used by Internet Explorer to save Favorites
- **ZED**—My Heritage Family Tree
Cursors
- ANI—Animated Cursor
- CUR—Cursor Files

Financial Records
- TAX—TurboTax File
- YNAB—YNAB File
- MYO—MYOB Limited (Windows) File
- MYOB—MYOB Limited (Mac) File

Office Docs

Documents
- ABW—AbiWord document
- ACL—MS Word AutoCorrect List
- AFP—Advanced Function Presentation
- ANS—ANSI text with Layout
- ASC—ASCII text with Layout
- AWW—Ability Write
- CSV—ASCII text encoded as Comma Separated Values, used in most spreadsheets such as Microsoft Excel or by most database management systems
- CWK—ClarisWorks / AppleWorks document
- DOC—Microsoft Word document
- DOCX—Office Open XML Text document or Microsoft Office Word 2007 for Windows/2008 for Mac
- DOT—Microsoft Word document template
- DOTX—Office Open XML Text document template
- EGT—EGT Universal Document
- FTM—Fielded Text Meta
- FTX—Fielded Text (Declared)
- HTML—HyperText Markup Language (.html, .htm)
- HWP—Haansoft(Hancom) Hangul Word Processor document
- HWPM—Haansoft(Hancom) Hangul Word Processor Markup Language document
- LWP—Lotus Word Pro
- **MCW**—Microsoft Word for Macintosh (versions 4.0; 5.1)
- **NB**—Mathematica Notebook
- **NBP**—Mathematica Player Notebook
- **ODM**—OpenDocument Master document
- **ODT**—OpenDocument Text document
- **OTT**—OpenDocument Text document template
- **PAGES**—Apple Pages document
- **PAP**—Papyrus word processor document
- **PDAX**—Portable Document Archive (PDA) document index file
- **PDF**—Portable Document Format
- Radix-64
- **RTF**—Rich Text document
- **SDW**—StarWriter text document, used in earlier versions of StarOffice
- **STW**—StarOffice/OpenOffice.org/NeoOffice text document template
- **SXW**—StarOffice/OpenOffice.org/NeoOffice text document
- **TeX**—Typesetting system
- **Texinfo**—GNU Project
- **Troff**
- **TXT**—ASCII or Unicode plaintext
- **UOF**—Uniform Office Format
- **UOML**—UniqueObject Markup Language (UOML) is a XML-based markup language; uniqueobject.com
- **WPD**—WordPerfect document
- **WPS**—Microsoft Works document
- **WPT**—Microsoft Works document template
- **WRD**—WordIt! Document
- **WRF**—ThinkFree Write
- **WRI**—Microsoft Write document
- **XHTML, xht**—eXtensible Hyper-Text Markup Language
- **XML**—eXtensible Markup Language

**Mathematical Markup Language (MML)**
- **MathML**—Mathematical Markup Language (.mml)
Page Description Language

- DVI
- EGT—Universal Document can be used to store css type styles (*.egt)
- PLD
- PCL
- PDF—Portable Document Format
- ps—PostScript
- SNP—Microsoft Access Report Snapshot
- XPS
- XSL-FO—Formatting Objects
- CSS
- XSLT—XML Style Sheet (.xslt, .xsl)
- XSL—XML Style Sheet (.xslt, .xsl)
- TPL—Web template (.tpl)

Personal Information Manager

- MSG—Microsoft Outlook task manager
- ORG—Lotus Organizer PIM package
- PST—Microsoft Outlook e-mail communication
- SC2—Microsoft Schedule+ calendar

Presentation

- KEY—Apple Keynote Presentation
- NB—Mathematica Slideshow
- NBP—Mathematica Player slideshow
- ODP—OpenDocument Presentation
- OTP—OpenDocument Presentation template
- POT—Microsoft PowerPoint template
- PPS—Microsoft PowerPoint Show
- PPT—Microsoft PowerPoint Presentation
- PPTX—Office Open XML Presentation
- PRZ—Lotus Freelance Graphics
- SDD—StarOffice’s StarImpress
- SHF—ThinkFree Show
- SHOW—Haansoft(Hancom) Presentation software document
- SHW—Corel Presentations slide show creation
- SSPSS—SongShow Plus Slide Show
- STI—OpenOffice.org 1.url.extension=Presentation template
- SXI—OpenOffice.org 1.url.extension=Presentation
- WATCH—Dataton Watchout Presentation

Project Management Software
- MPP—Microsoft Project

Formats of files used in software for bibliographic information (citation) management.
- bib—BibTeX
- enl—EndNote
- ris—Research Information Systems RIS (file format)

Spreadsheet
- 123—Lotus 1-2-3
- AWS—Ability Spreadsheet
- CLF—ThinkFree Calc
- CELL—Haansoft(Hancom) SpreadSheet software document
- CSV—Comma-Separated Values
- numbers—An Apple Numbers Spreadsheet file
- gnumeric—Gnumeric spreadsheet, a gziped XML file
- ODS—OpenDocument spreadsheet
- OTS—OpenDocument spreadsheet template
- QPW—Quattro Pro spreadsheet
- SDC—StarOffice/OpenOffice.org StarCalc Spreadsheet
- SLK—SYLK (SYmbolic LinK)
- STC—StarOffice/OpenOffice.org
- SXC—StarOffice/OpenOffice.org 1.url.extension=Spreadsheet
- TAB—Tab-Delimited Columns; also TSV (Tab-Separated Values)
- TXT—Tab-Delimited Columns
- VC—Visicalc
WK1—Lotus 1-2-3 up to version 2.01
WK3—Lotus 1-2-3 version 3.0
WK4—Lotus 1-2-3 version 4.0
WKS—Lotus 1-2-3
WKS—Microsoft Works
WQ1—Quattro Pro DOS version
XLK—Microsoft Excel worksheet backup
XLS—Microsoft Excel worksheet sheet (97-2003)
XLSB—Microsoft Excel binary workbook
XLSM—Microsoft Excel Macro-enabled workbook
XLSX—Office Open XML worksheet sheet
XLR—Microsoft Works version 6.0
XLT—Microsoft Excel worksheet template
XLTM—Microsoft Excel Macro-enabled worksheet template
XLW—Microsoft Excel worksheet workspace (version 4.0)

Tabulated data
- tab
- CSV—Comma-Separated Values
- db—Databank format; accessible by many economet

Scripts
- AHK—AutoHotkey script file
- APPLESSCRIPT—See SCPT.
- AS—Adobe Flash ActionScript File
- AU3—AutoIt version 3
- BAT—Batch file
- BAS—QBASIC & QuickBASIC
- CMD—Batch file
- EGG—Chicken
- EGT—EGT Asterisk Application Source File, EGT Universal Document
- HTA—HTML Application
- IBI—Icarus script
- ICI—ICI
- ITCL—Itcl
- JS—JavaScript and JScript
- JSFL—Adobe JavaScript language
- LUA—Lua
- M—Mathematica package file
- MRC—mIRC Script
- NCF—NetWare Command File (scripting for Novell's NetWare OS)
- NUT—Squirrel
- PHP—PHP
- PHP?—PHP (? = version number)
- PL—Perl
- PM—Perl module
- PS1—Windows PowerShell shell script
- PS1XML—Windows PowerShell format and type definitions
- PSC1—Windows PowerShell console file
- PSD1—Windows PowerShell data file
- PSM1—Windows PowerShell module file
- PY—Python
- PYC—Python
- PYO—Python
- R—R scripts
- RB—Ruby
- RDP—RDP connection
- SCPT—Applescript
- SCPTD—See SCPT.
- SDL—State Description Language
- SH—Shell script
- TCL—Tcl
Source Code

Object Code, Executable Files, Shared and Dynamically-Linked Libraries

- **8BF**—Files are plugins for some photo editing programs including Adobe Photoshop, Paint Shop Pro, GIMP and Helicon Filter.
- **APP**—Apple application program executable file
- **BPL**—A Win32 PE file created with Borland Delphi or C++Builder containing a package.
- **Class**—Files; used in Java
- **COFF**—(No suffix for executable image, .o for object file) UNIX Common Object File Format, now often superseded by ELF
- **COM**—Files; commands used in DOS
- **DCU**—Files; Delphi compiled unit
- **DOL**—The file format used by the Gamecube and Wii, short for Dolphin the codename of the Gamecube.
- **EAR**—Files; archives of Java enterprise applications
- **EGT**—A basic Universal Document and also Launches the EGT SmartSense executable file.
- **ELF**—(No suffix for executable image, .o for object files, .so for shared object files); Used in many modern Unix and Unix-like systems, including Solaris, other System V Release 4 derivatives, Linux, and BSD
- **JAR**—Files; archives of Java class files
- **XPI**—A PKZIP archive that can be run by Mozilla Web browsers to install software. (.xpi)
- **Mach-O**—(No suffix for executable image, .o for object files, .dylib and .bundle for shared object files); Mach-based systems, notably native format of Mac OS X
- **nlm**—NetWare Loadable Module (.NLM); the native 32-bit binaries compiled for Novell's NetWare Operating System (versions 3 and newer)
- **s1es**—Executable used for S1ES learning system.
- **vap**—Value Added Process (.VAP); the native 16-bit binaries compiled for Novell's NetWare Operating System (version 2, NetWare 286, Advanced NetWare, etc.)
- **WAR**—Files; archives of Java Web applications
- **XBE**—Xbox executable
- **XCOFF**—(No suffix for executable image, .o for object files, .a for shared object files); Extended COFF, used in AIX

Object Extensions

- **VBX**—Visual Basic Extensions
- **OCX**—Object Control Extensions
Source Code for Computer Programs

- TLB—Windows Type Library

1. ADA—Ada (body) source
2. ADB—Ada (body) source
3. ADS—Ada (specification) source
4. ASM, S—Assembly Language source
5. BAS—BASIC, Visual Basic module
6. BB—Blitz3D
7. BMX—BlitzMax
8. C—C source
9. CLS—Visual Basic class
10. COB, CBL—Cobol source
11. CPP, CC, CXX, C—C++ source
12. CS—C# source
13. CSPROJ—C# project (Visual Studio .NET)
14. D—D source
15. DBA—DarkBASIC source
16. DBPro—DarkBASIC Professional project
17. E—Eiffel source
18. EFS—EGT Forever Source File
19. EGT—EGT Asterisk Source File, could be J, C#, VB.net, EF 2.0 (EGT Forever)
20. EL—Emacs Lisp source
21. FOR—Fortran source
22. FTN—Fortran source
23. F—Fortran source
24. F77—Fortran source
25. F90—Fortran source
26. FRM—Visual Basic form
27. FRX—Visual Basic form stash file (binary form file)
28. GED—Game Maker Extension Editable file as of version 7.0
- GM6—Game Maker Editable file as of version 6.x
- GMD—Game Maker Editable file up to version 5.x
- GMK—Game Maker Editable file as of version 7.0
- GML—Game Maker Language script file
- H—C/C++ header file
- HPP—C++ header file
- HXX—C++ header file
- HS—Haskell source
- INC—Turbo Pascal included source
- JAVA—Java source
- L—Lex source
- LISP—Common Lisp source
- M—Objective-C source
- M—MATLAB
- M—Mathematica
- M4—m4 source
- ML—Standard ML / Objective CAML source
- N—Nemerle source
- PAS—Pascal source (DPR for projects)
- P—Parser source
- PIV—Pivot stickfigure animator
- PL—Perl
- PRG—db, clipper, Microsoft FoxPro, harbour and Xbase
- PY—Python programming language source
- RESX—Resource file for .NET applications
- RC, RC2—Resource script files to generate resources for .NET applications
- SCI, SCE—Scilab
- SCM—Scheme source
- SKB, SKC—Sage Retrieve 4GL Common Area (Main and Amended backup)
- SKD—Sage Retrieve 4GL Database
- SKF, SKG—Sage Retrieve 4GL File Layouts (Main and Amended backup)
- SKI—Sage Retrieve 4GL Instructions
- SKK—Sage Retrieve 4GL Report Generator
- SKM—Sage Retrieve 4GL Menu
- SKO—Sage Retrieve 4GL Program
- SKP—Sage Retrieve 4GL Print Layouts (Main and Amended backup)
- SKS—Sage Retrieve 4GL Screen Layouts (Main and Amended backup)
- SKQ—Sage Retrieve 4GL Print Layouts (Main and Amended backup)
- SKT—Sage Retrieve 4GL Screen Layouts (Main and Amended backup)
- SKZ—Sage Retrieve 4GL Security File
- SLN—Visual Studio solution
- SPIN—Spin source (for Parallax Propeller microcontrollers)
- STK—Stickfigure file for Pivot stickfigure animator
- VAP—Visual Studio Analyzer project
- VB—Visual Basic.NET source
- VIP—Visual Basic project
- VBP—Visual Basic project
- VBG—Visual Studio compatible project group
- VBPROJ—Visual Basic.NET project
- VCPROJ—Visual C++ project
- VDPROJ—Visual Studio deployment project
- Y—YACC source

Video Files

Video File Formats

- AAF—Mostly intended to hold edit decisions and rendering information, but can also contain compressed media essence)
- 3GP—The most common video format for cell phones
- GIF—Animated GIF (simple animation)
- ASF—Container (enables any form of compression to be used; MPEG-4 is common; video in ASF-containers is also called Windows Media Video (WMV))
- AVCHD—Advanced Video Codec High Definition
- AVI—Container (a shell, which enables any form of compression to be used)
- CAM—An MSN webcam log file
- DAT—Video standard data file (automatically created when we attempted to burn as video file on the CD)
- DSH
- FLV—Flash video (encoded to run in a flash animation)
- M1V—Video
- M2V
- FLA—Macromedia Flash (for producing)
- FLR—Text file that contains scripts extracted from SWF by a free ActionScript decompiler named FLARE
- SOL—Adobe Flash shared object ("Flash cookie")
- M4V—File format for videos for iPods and PlayStation Portables developed by Apple
- mkv—Matroska is a container format, which enables any video format such as MPEG-4 ASP or AVC to be used along with other content such as subtitles and detailed meta information
- WRAP—MediaForge (*.wrap)
- MNG—Mainly simple animation containing PNG and JPEG objects, often somewhat more complex than animated GIF
- mov—Container which enables any form of compression to be used; Sorenson codec is the most common; QTCH is the filetype for cached video and audio streams
- MPEG—.mpeg, .mpg, .mpe
- MPG—.mpeg, .mpg, .mpe
- MPE—.mpeg, .mpg, .mpe
- MP4—Multimedia container (most often used for Sony’s PlayStation Portable and Apple’s iPod)
- MXF—Material Exchange Format (standardized wrapper format for audio/visual material developed by SMPTE)
- ROQ—Used by Quake 3
- NSV—Nullsoft Streaming Video (media container designed for streaming video content over the Internet)
- Ogg—Container, multimedia
- RM—RealMedia
- SVI—Samsung video format for portable players
- SMI—SAMI Caption file (HTML like subtitle for movie files)
- SWF—Macromedia Flash (for viewing)
- WMV—Windows Media Video (See ASF)
Video Editing & Production formats

- FCP—Final Cut Pro project file
- MSWMM—Windows Movie Maker project file
- PPJ—Adobe Premiere Pro video editing file
- IMOVIEPROJ—iMovie project file
- VEG, VEG-BAK—Sony Vegas project file
- SUF—Sony camera configuration file (setup.suf) produced by XDCAM-EX camcorders

Virtual Machines

Microsoft Virtual PC/Virtual Server

- VFD—Virtual Floppy Disk (.vfd)
- VHD—Virtual Hard Disk (.vhd)
- VUD—Virtual Undo Disk (.vud)
- VMC—Virtual Machine Configuration (.vmc)
- VSV—Virtual Machine Saved State (.vsv)

EMC VMware ESX/GSX/Workstation/Player

- LOG—Virtual Machine Logfile (.log)
- VMDK—Virtual Machine Disk (.vmdk, .dsk)
- NVRAM—Virtual Machine BIOS (.nvram)
- VMEM—Virtual Machine paging file (.vmem)
- VMSD—Virtual Machine snapshot metadata (.vmsd)
- VMSN—Virtual Machine snapshot (.vmsn)
- VMSS—Virtual Machine suspended state (.vmss, .std)
- STD—Virtual Machine suspended state (.vmss, .std)
- VMTM—Virtual Machine team data (.vmtm)
- VMX—Virtual Machine configuration (.vmx, .cfg)
- VMXF—Virtual Machine team configuration (.vmxf)

Virtualbox

- VDI—VirtualBox Virtual Disk Image (.vdi)
Parallels Workstation

- HDD—Virtual Machine hard disk (.hdd)
- PVS—Virtual Machine preferences/configuration (.pvs)
- SAV—Virtual Machine saved state (.sav)