Web Security Service

Policy Guide

Version 6.10.4.1/OCT.12.2018

Copyrights

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com

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 as well as the WebPulse™ cloud community of over 75 million users.

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 instantly 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 connot 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 11
- "Filter Content" on page 14
- "Malware Policy" on page 31
- "Web Application Policy" on page 58
- "SSL Policy" on page 78
- "Policy: How Do I?" on page 96
- "Policy Reference" on page 126

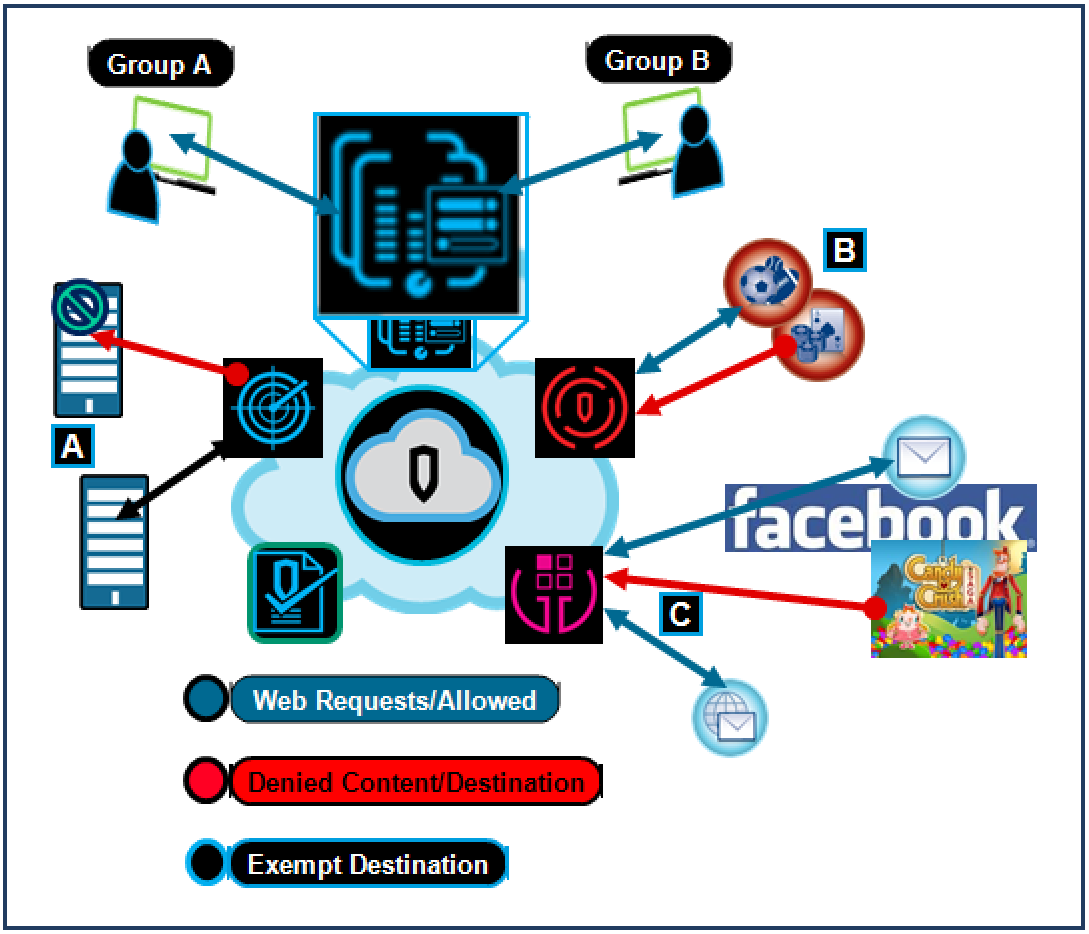
This document contains topics collected from the Web Security Service online documentation. For the complete doc set, see:

Symantec Support Site > WSS Documentation

Table Of Contents

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 Web Security Service 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 (basic policy) or granular rules (advanced policy, Content Filtering only). For example, you can determine what happens to requests based on the role of requester. In the above example, Web Security Service policy is defined to achieve the following:

- A—Allow a network subnet, which requires the highest performance level possible, to bypass Web Security Service 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 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)
- Unified Agent and SEP clients
- Roaming Captive Portal authentication option

Be advised of the following details.

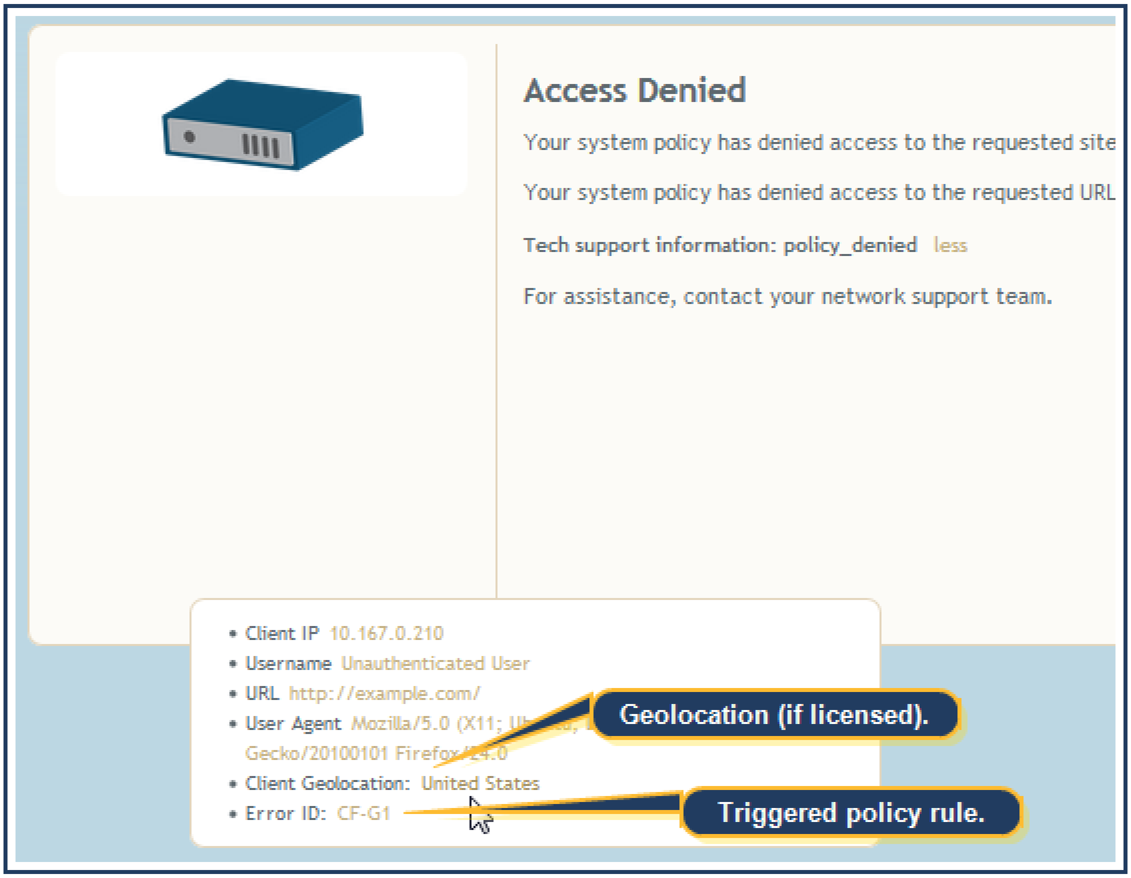
- **Sources**—If the Access Method is Firewall/VPN or Proxy Forwarding, the Web Security Service receives the IP address of the client system; therefore, the service cannot properly determine the geolocation. For these methods, define policy based on the fixed locations (as defined in **Service** mode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



Access Denied

Your system policy has denied access to the requested site

Your system policy has denied access to the requested URL

Tech support information: policy_denied less

For assistance, contact your network support team.

- Client IP 10.167.0.210
- Username Unauthenticated User
- URL http://example.com/
- User Agent Mozilla/5.0 (X11; Ub[illegible] Gecko/20100101 Firefox/24.0
- Client Geolocation: United States
- Error ID: CF-G1

- 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 105.

- 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 23
- "Threat Protection Policy Editor" on page 38
- "Enable Web Isolation" on page 54

Filter Content

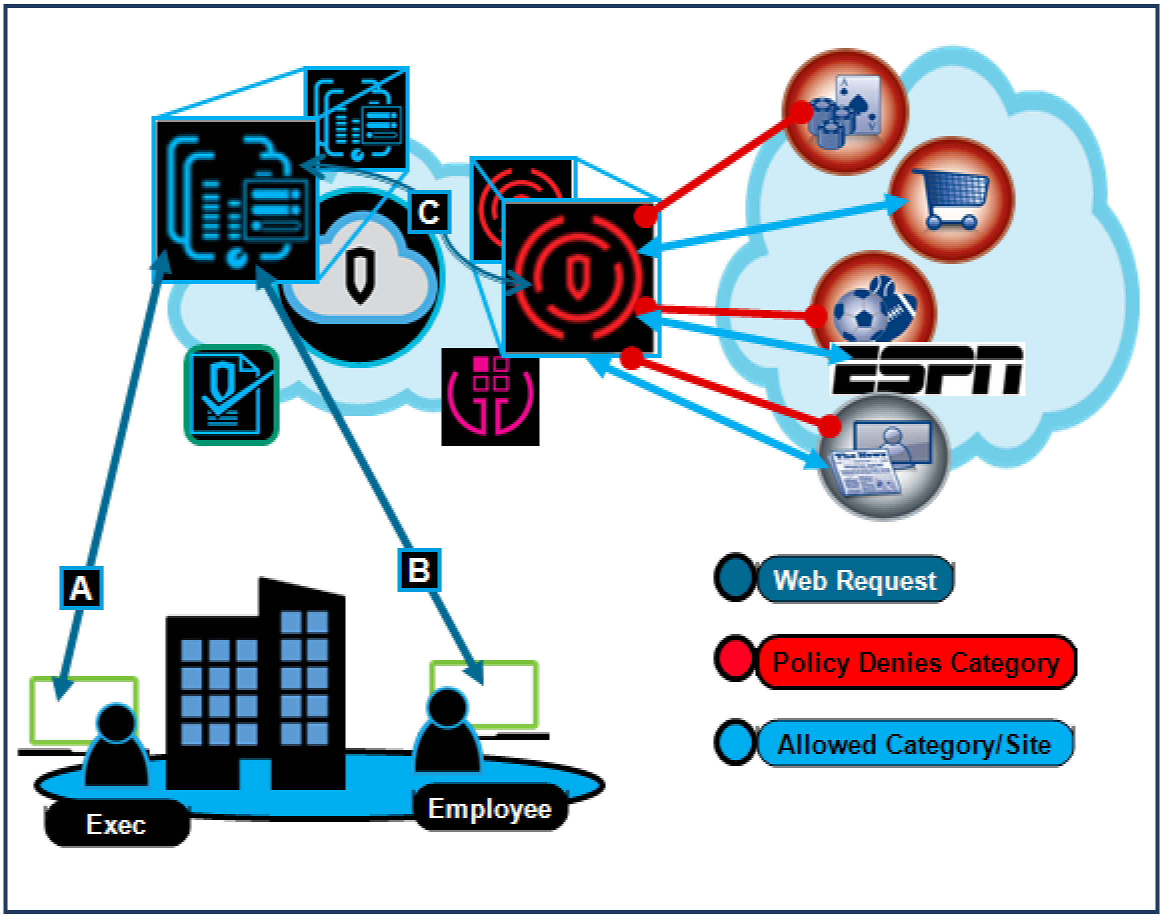
Configure the Web Security Service to apply content filtering policy to web requests and responses.

- "About Content Filtering" on page 15
- "Control User Access to Web Content" on page 17
- "About the Content Filtering Rule Editor" on page 19
- "Create Custom Content Filtering Rules" on page 23
- "Modify the Default Exception Notifications" on page 101
- "Customize the User Notification Template" on page 105

About Content Filtering

The Symantec Web Security Service leverages the Symantec 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 Web Security Service policy checks against this database.

The Web Security Service 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 Web Security Service policy achieves the following:

- **A**—The Exec initiates three web destinations: a **Gambling** site a **Newsgroups/Forums** site.
- **B**—Employees request **Shopping**, **Sports**, and **Newsgroup/Forums** sites.
- **C**—The Web Security Service 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.

Default Policy—By default and unchangeable, the Web Security Service blocks access to known malware sources and some inappropriate content.

- **Liability Concerns**
  - Child pornography
- **Security Concerns**
  - Spam
- **Security Threats**
  - Malicious Outbound Data/Botnets
  - Malicious Sources
  - Phishing
  - Proxy Avoidance

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.

- **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/Questionble/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 Eduction
    - Sexual Expression
    - Software Downloads
    - Violence/Hate/Racism
    - Weapons

Regardless of this selection, you can further modify policy.

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

- "About the Content Filtering Rule Editor" on page 19—Describes the Policy Editor rows and elements.
- "Create Custom Content Filtering Rules" on page 23—Demonstrates how to create policy constructs and rules.
- "About Geolocation Policies" on page 12—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**). See What Can I Do From A Report Dashboard?
- Generate a pre-defined report. Select **Content Filtering > Reports**. Click any link to generate a report. See What Can I Do With Reports?

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 101.
- "Customize the User Notification Template" on page 105.

About the Content Filtering Rule Editor

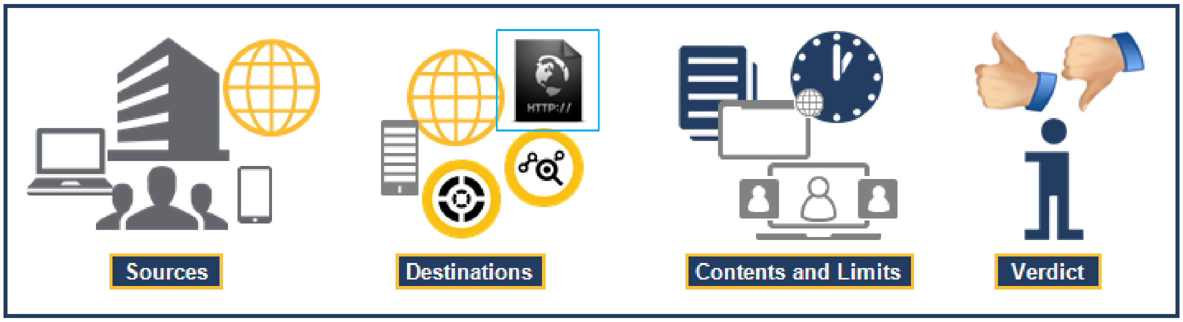
The Symantec Web Security Service **Content Filtering Rules** policy editor allows you to accomplish the following:

- 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, Unified 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 12 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 withing 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 Web Security Service 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

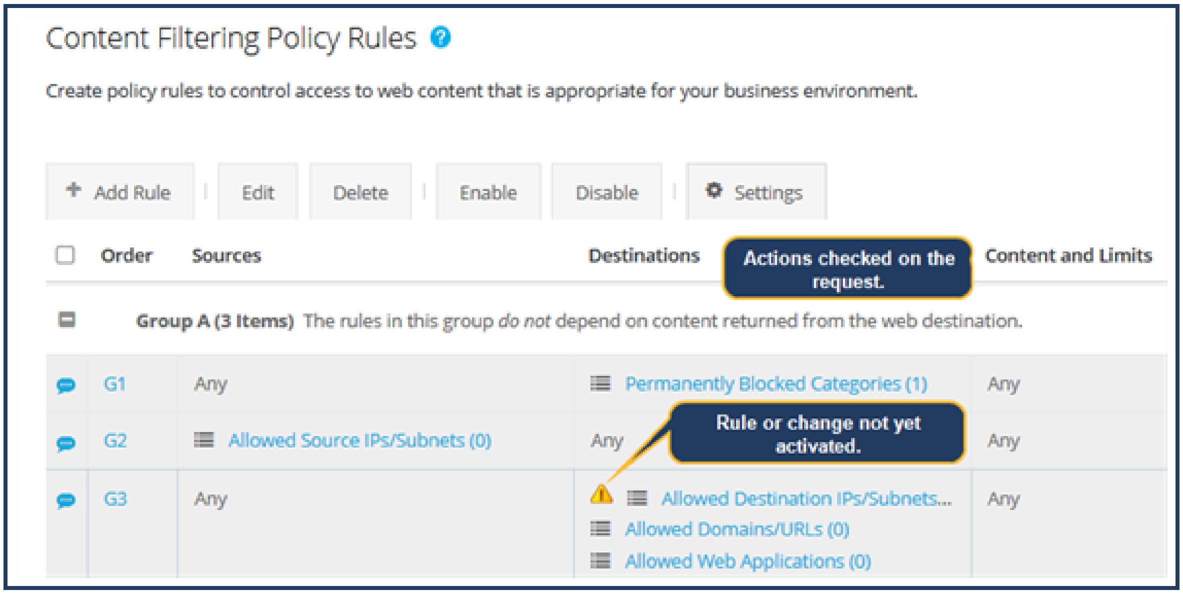
The rules editor contains two distinct areas: **Group A** and **Group B**. As you add and modify rules, the **Content Filtering Rules** policy editor automatically places the rules in the correct group and correct order. Rules might contain conditions for a mix of inbound and outbound traffic; the actions 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 Web Security Service 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.



Content Filtering Policy Rules

Create policy rules to control access to web content that is appropriate for your business environment.

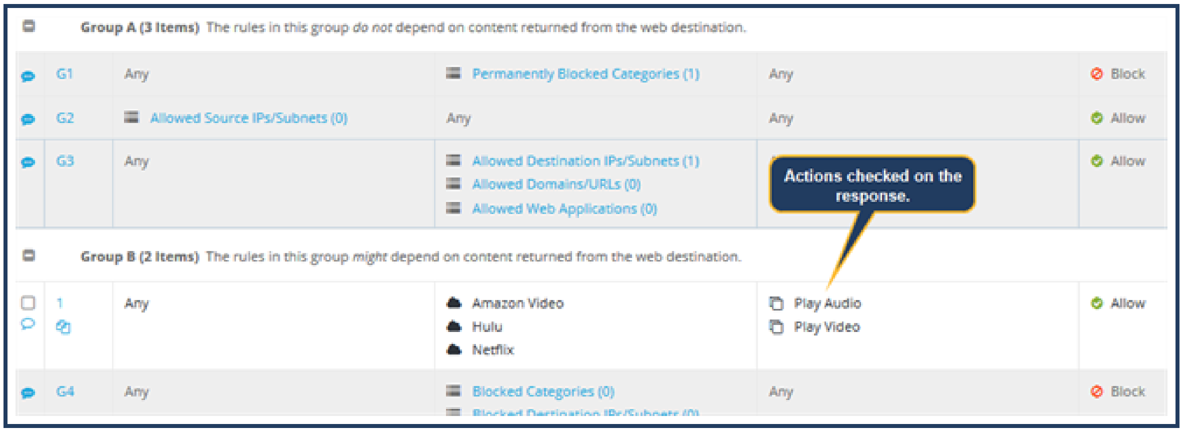
□	Order	Sources	Destinations	Content and Limits
	Group A (3 Items) The rules in this group *do not* depend on content returned from the web destination.			
	G1	Any	Permanently Blocked Categories (1)	Any
	G2	Allowed Source IPs/Subnets (0)	Any	Any
	G3	Any	⚠ Allowed Destination IPs/Subnets... Allowed Domains/URLs (0) Allowed Web Applications (0)	Any

Actions checked on the request.

Rule or change not yet activated.

Group B Rules

If no rule in **Group A** triggers a policy action, the Web Security Service 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.



	Group A (3 Items) The rules in this group *do not* depend on content returned from the web destination.				
	G1	Any	Permanently Blocked Categories (1)	Any	Block
	G2	Allowed Source IPs/Subnets (0)	Any	Any	Allow
	G3	Any	Allowed Destination IPs/Subnets (1) Allowed Domains/URLs (0) Allowed Web Applications (0)		Allow
	Group B (2 Items) The rules in this group *might* depend on content returned from the web destination.				
□	1	Any	Amazon Video Hulu Netflix	Play Audio Play Video	Allow
	G4	Any	Blocked Categories (0) Blocked Destination IPs/Subnets (0)	Any	Block

Actions checked on the response.

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?

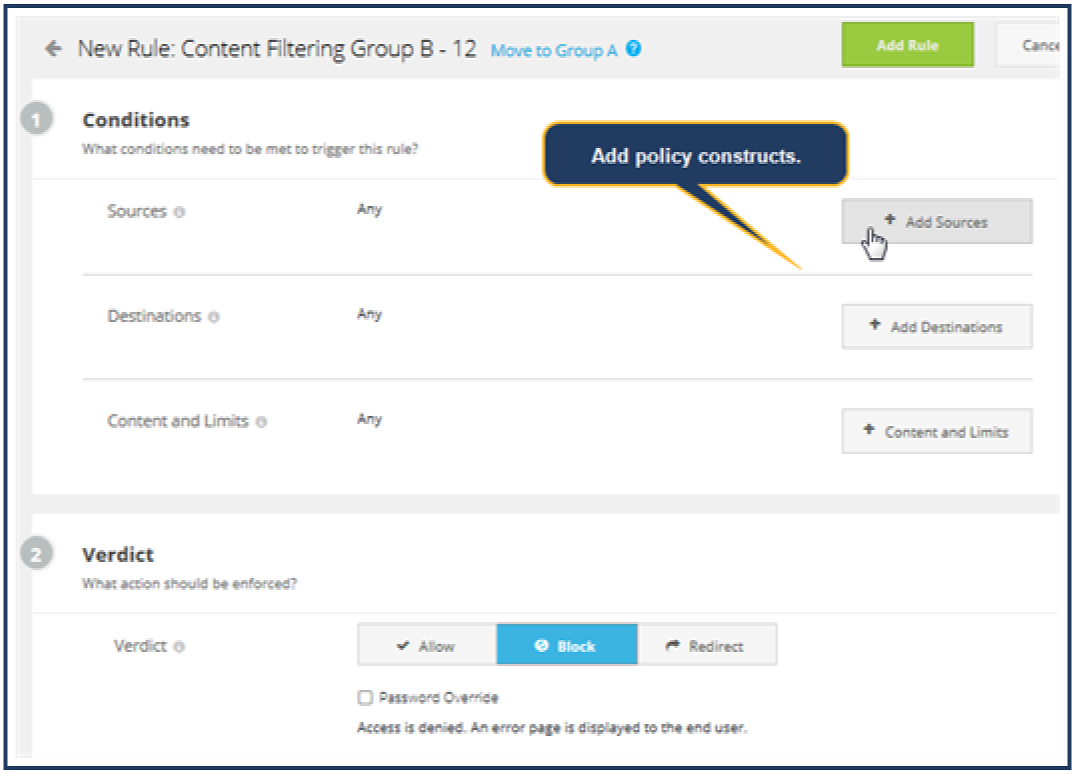
- "Create Custom Content Filtering Rules" on page 23

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**.



New Rule: Content Filtering Group B - 12

1 Conditions

What conditions need to be met to trigger this rule?

Sources: Any

Destinations: Any

Content and Limits: Any

2 Verdict

What action should be enforced?

Verdict: ✓ Allow | Block | Redirect

□ Password Override

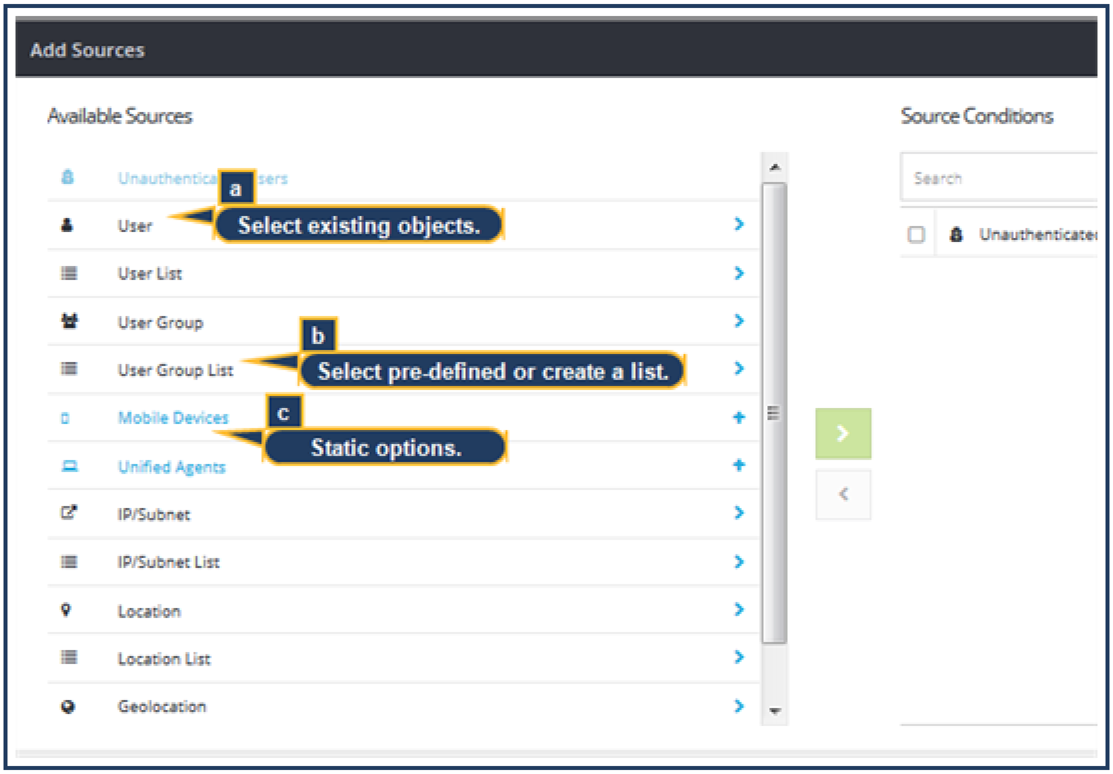
Access is denied. An error page is displayed to the end user.

- 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 Web Security Service 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.

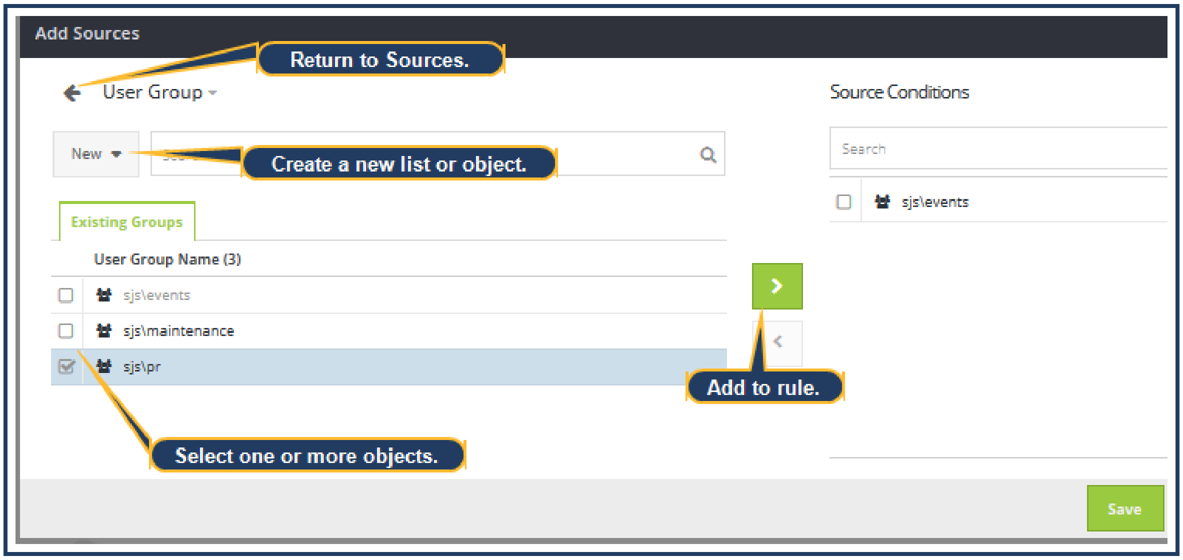
> **Tip:** Geolocation policy requires an add-on license. See "About Geolocation Policies" on page 12 for more details.

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.

   - **Unathenticated 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 the have the SymantecUnified Agent installed. These are connections from beyond the corporate network.

Select any construct to display its options. Show screen...



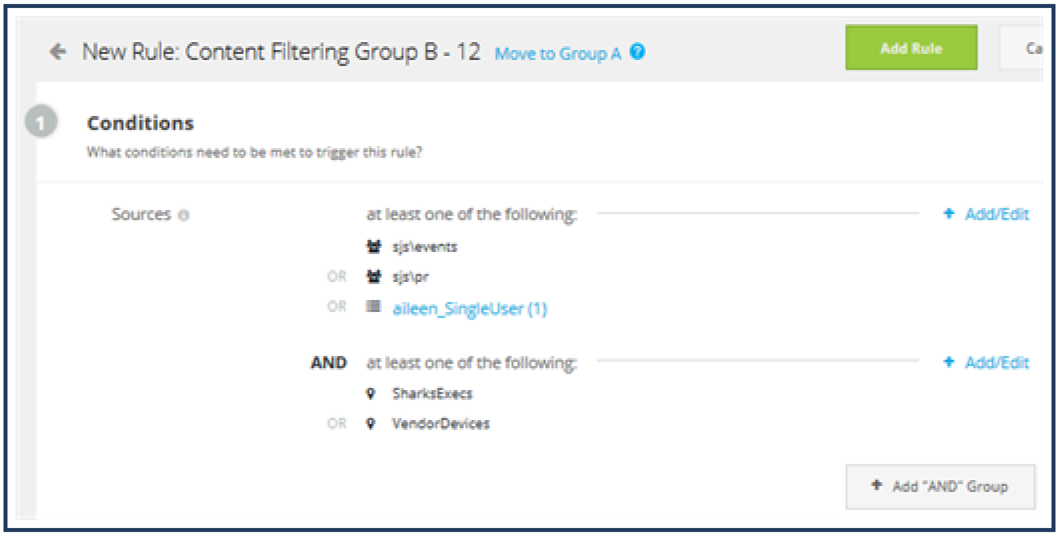
- The editor displays all of the objects that are available for this rule. Select one or more and click the right-arrow to assign them to the rule.
- You can also click **New** and select to create a new list or in applicable constructs a new object.

After completing your selections, perform one of the following.

- If this rule in 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.


New Rule: Content Filtering Group B - 12
Move to Group A
Add Rule
Ca
1
Conditions
What conditions need to be met to trigger this rule?
Add/Edit
Add/Edit
Add "AND" Group

Sources at least one of the following:
sjs\events
OR sjs\pr
OR aileen_SingleUser (1)

AND at least one of the following:
SharksExecs
OR VendorDevices

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

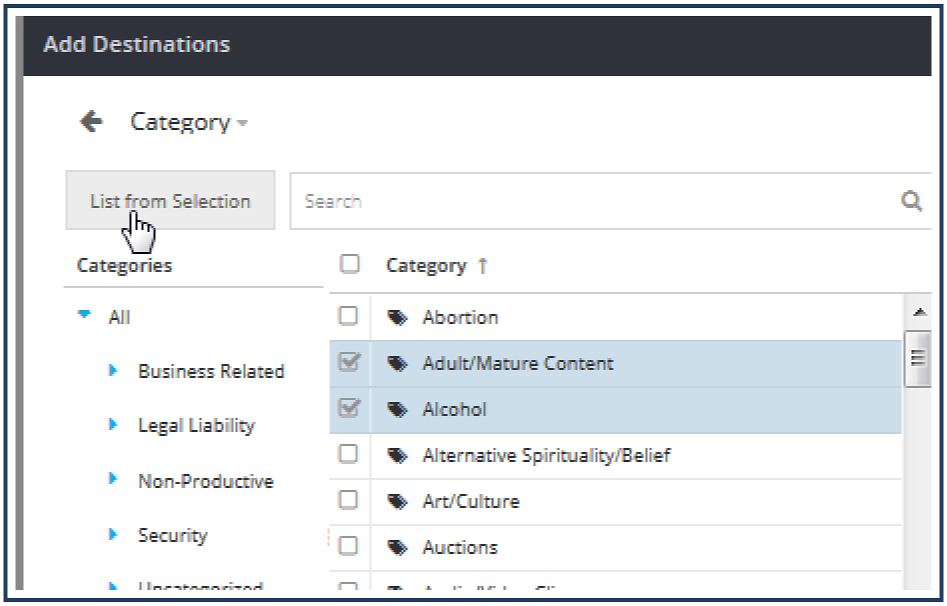
This example demonstrates what you can add to the **Destinations** construct of the rule, plus how to create lists within.

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...



□ Abortion
☑ Adult/Mature Content
☑ Alcohol
□ Alternative Spirituality/Belief
□ Art/Culture
□ Auctions

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.

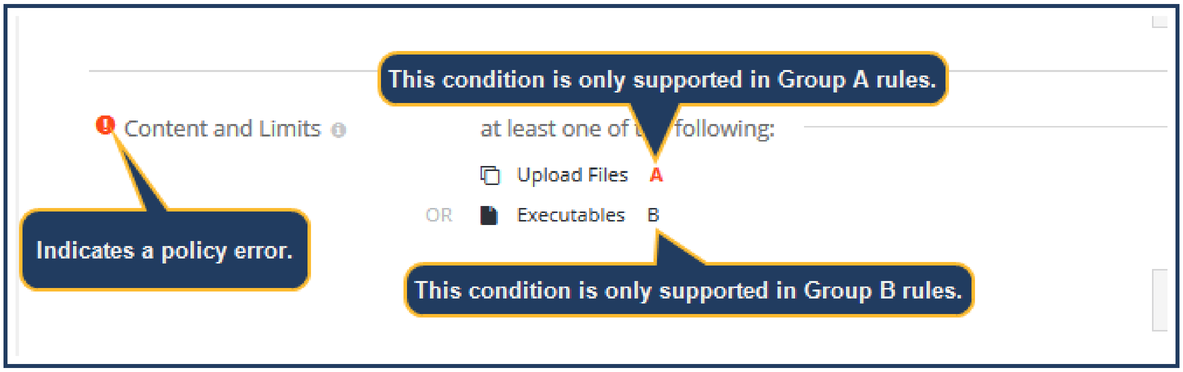
> **Tip:** See "Reference: File Types Detected by Advanced Policy" on page 131.

- **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**.

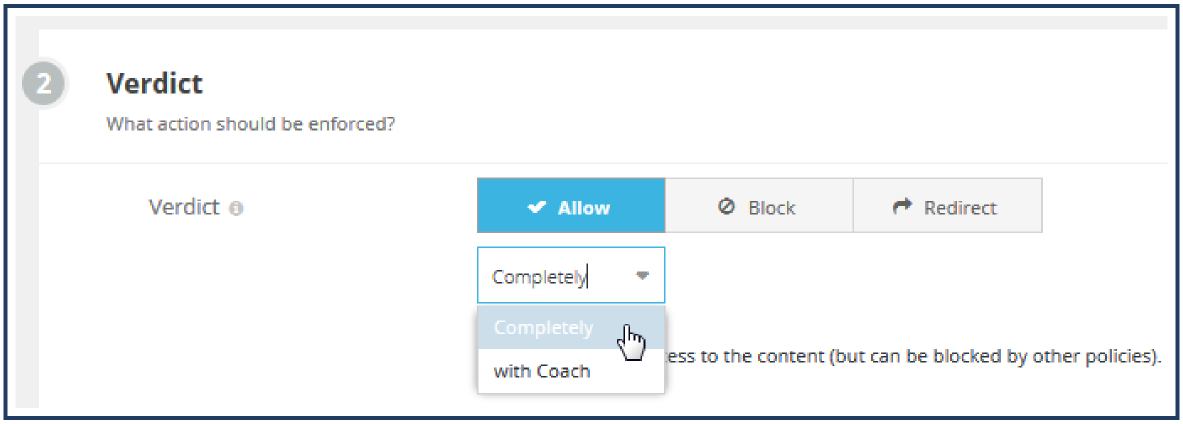

This condition is only supported in Group A rules.
Content and Limits
at least one of the following:
Upload Files A
OR
Executables B
Indicates a policy error.
This condition is only supported in Group B rules.

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

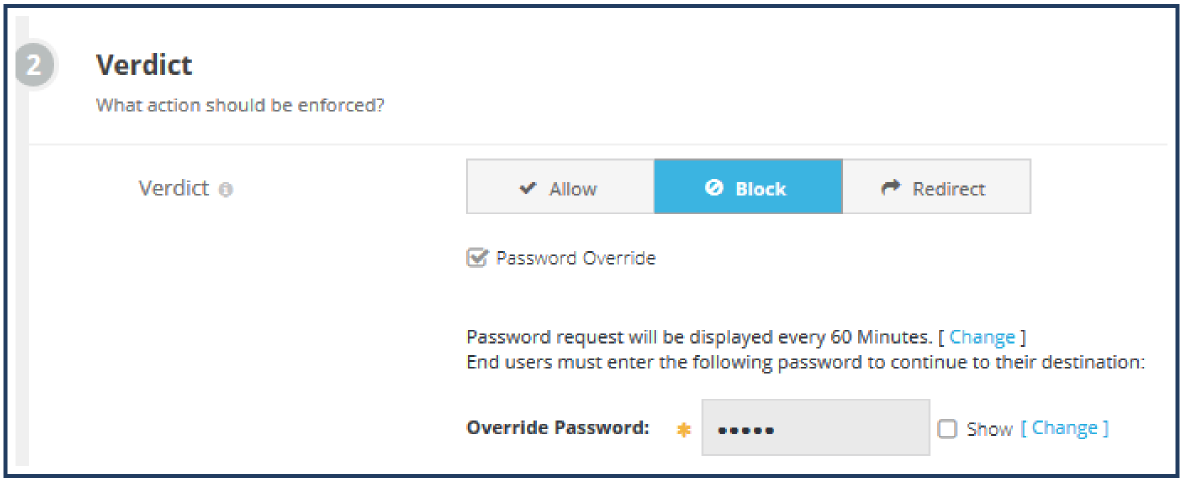
Now that you have created the conditions that trigger the policy rule, the final configuration is to instruct the Web Security Service what action to take. This is called the **Verdict**.

Allow


2
Verdict
What action should be enforced?
Verdict
Allow
Block
Redirect
Completely
Completely
with Coach
ess to the content (but can be blocked by other policies).

- **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



Verdict

What action should be enforced?

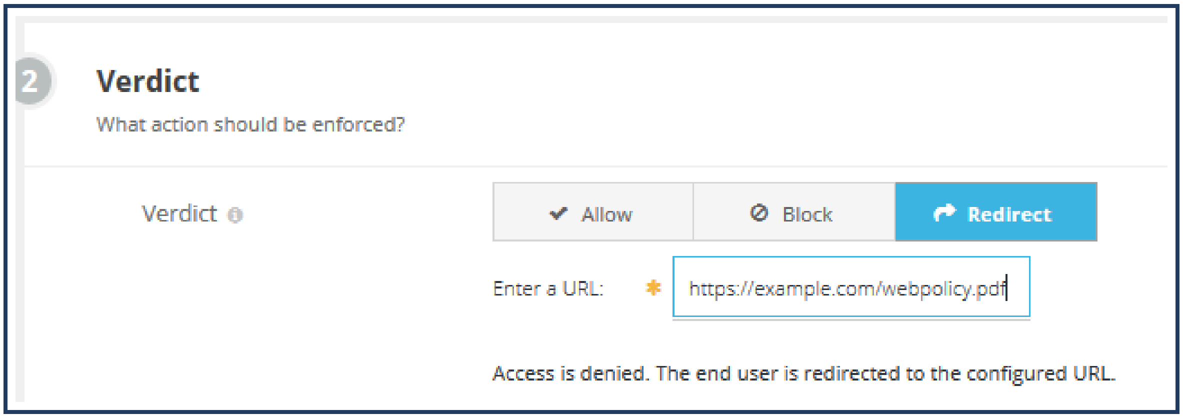
Verdict: Allow | **Block** | Redirect

☑ Password Override

Password request will be displayed every 60 Minutes. [Change]
End users must enter the following password to continue to their destination:

Override Password: * ●●●●● □ Show [Change]

- **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.



Verdict

What action should be enforced?

Verdict: Allow | Block | **Redirect**

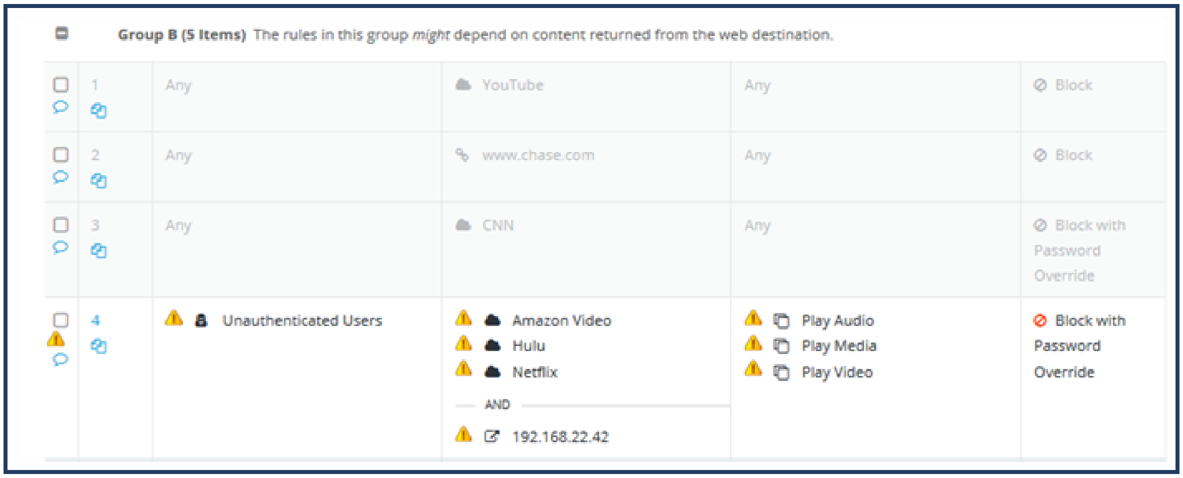
Enter a URL: * https://example.com/webpolicy.pdf

Access is denied. The end user is redirected to the configured URL.

- **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**.

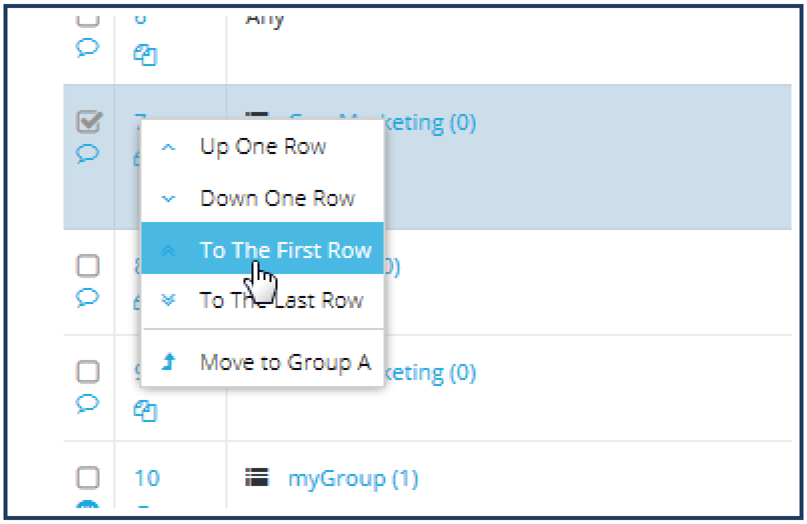


Group B (5 Items) The rules in this group *might* depend on content returned from the web destination.

1	Any	YouTube	Any	Block
2	Any	www.chase.com	Any	Block
3	Any	CNN	Any	Block with Password Override
4	Unauthenticated Users	Amazon Video Hulu Netflix AND 192.168.22.42	Play Audio Play Media Play Video	Block with Password Override

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 96 for use case examples.

Malware Policy

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

Malware Policies

Web Isolation Solution

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.

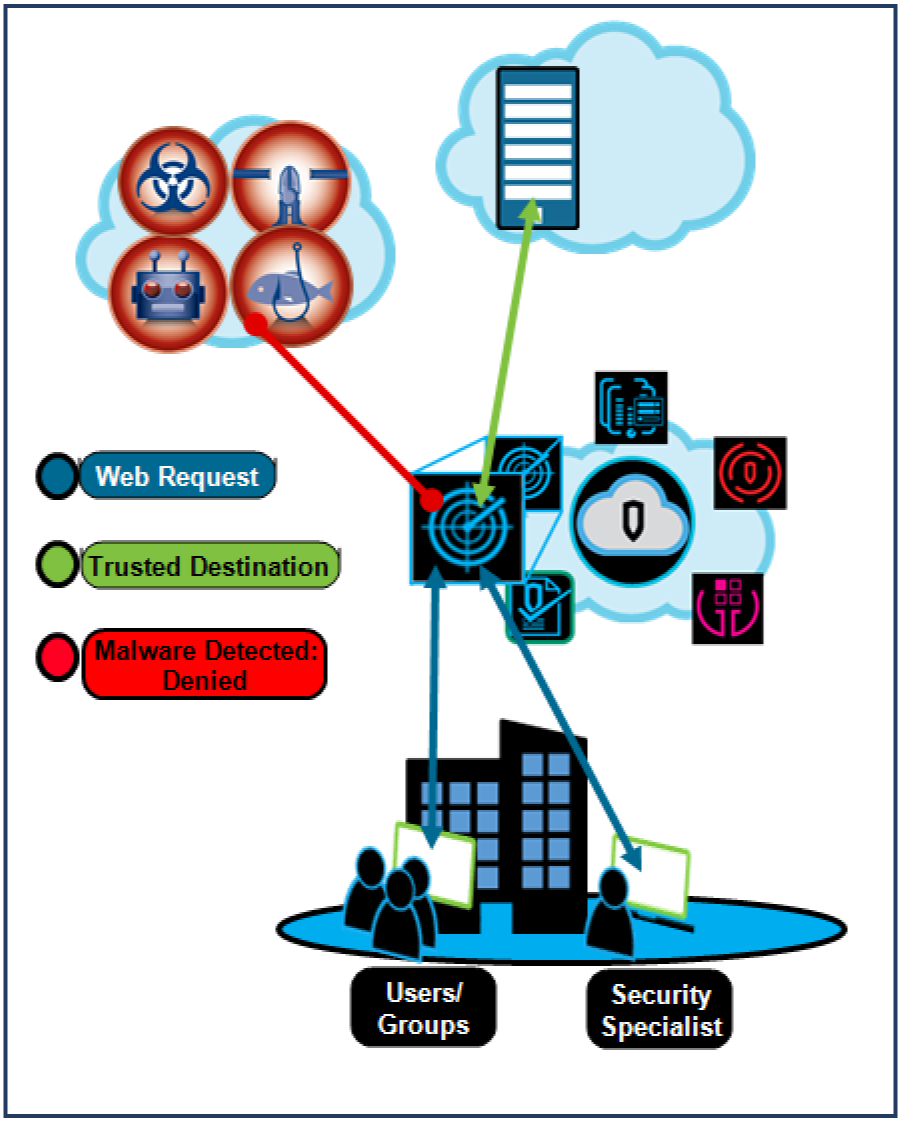
> **Tip:** For a client-less option, see "About Web Isolation" on page 50.

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 first-client infection from unknown malware. It block smalicious content in real-time based on sandboxing resources (Malware Anaylsis + 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.

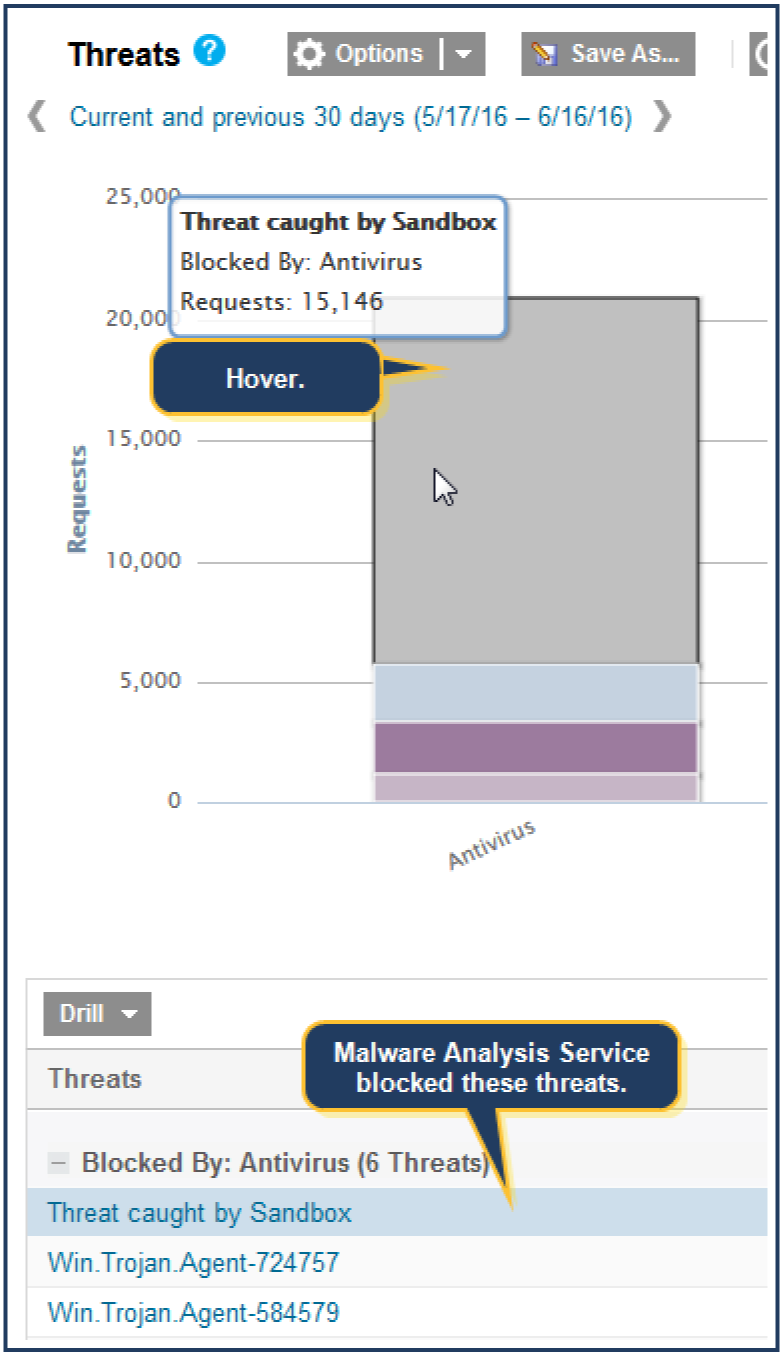
Because detonation can take longer than the real-time sandboxing period, the service delivers the file to the user *after* this time *while* detonation continues in the background. Any post-download detection triggers an administrative alert (email) with the details of the potential client infection (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).


Threats
Options
Save As...
Current and previous 30 days (5/17/16 – 6/16/16)
25,000
20,000
15,000
10,000
5,000
0
Requests
Antivirus
Hover.
Drill
Malware Analysis Service blocked these threats.

Threat caught by Sandbox
Blocked By: Antivirus
Requests: 15,146

Threats

Blocked By: Antivirus (6 Threats)

Threat caught by Sandbox

Win.Trojan.Agent-724757

Win.Trojan.Agent-584579

> **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 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 Web Security Service policy checks against this database.

The Web Security Service 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 32.

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

Content Analysis

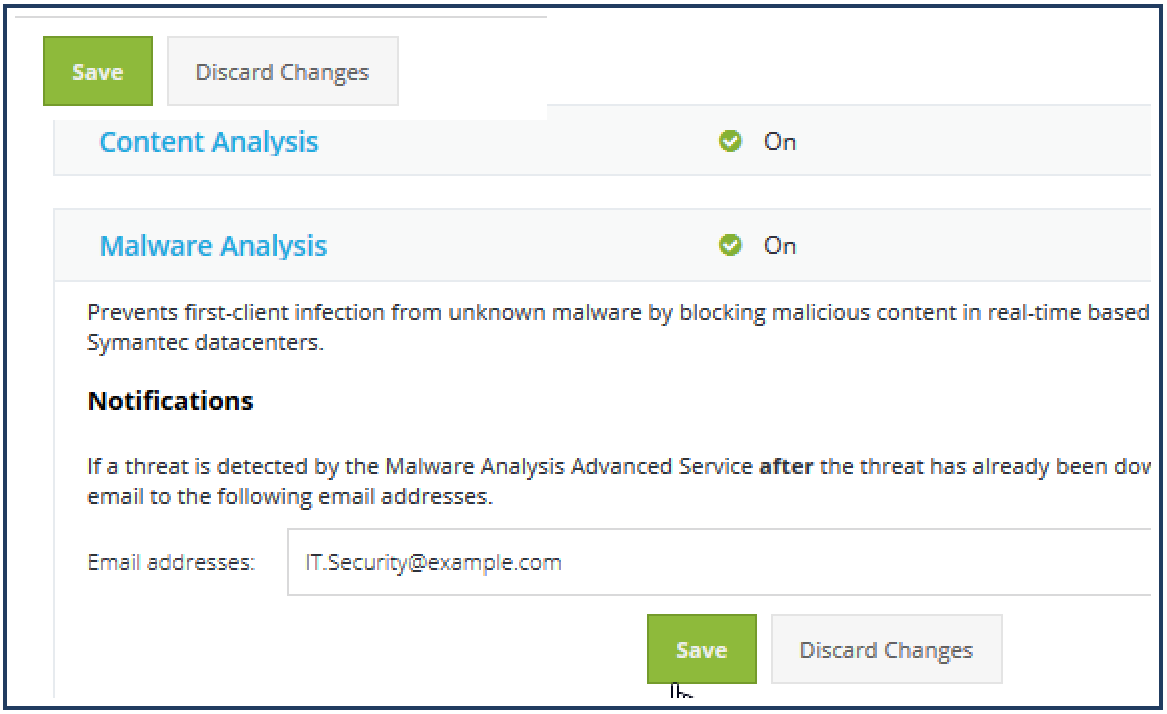
The Symantec Web Security Service basic malware services block the types of websites that are the source of viruses and ptjer malicious content. The default and unalterable Content Filtering policy prevents access to malicious content websites. Default blocked categories are located in the following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

- **Security** > **Security Concerns**: **Spam**
- **Security** > **Security Threats**: **Malicious Outbound Data/Botnets**, **Malicious Sources/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.

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.



Content Analysis ✓ On

Malware Analysis ✓ On

Prevents first-client infection from unknown malware by blocking malicious content in real-time based
Symantec datacenters.

Notifications

If a threat is detected by the Malware Analysis Advanced Service **after** the threat has already been dov
email to the following email addresses.

Email addresses: IT.Security@example.com

Enter emails (separated by commas) and click **Save**.

For full details, see "About Malware Scanning" on page 32.

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 43
- "Exempt a Destination From Malware Scan" on page 47

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

- "Threat Protection Policy Editor" on page 38

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 40

Geolocation-Based Polices

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).

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 50.

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. 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.

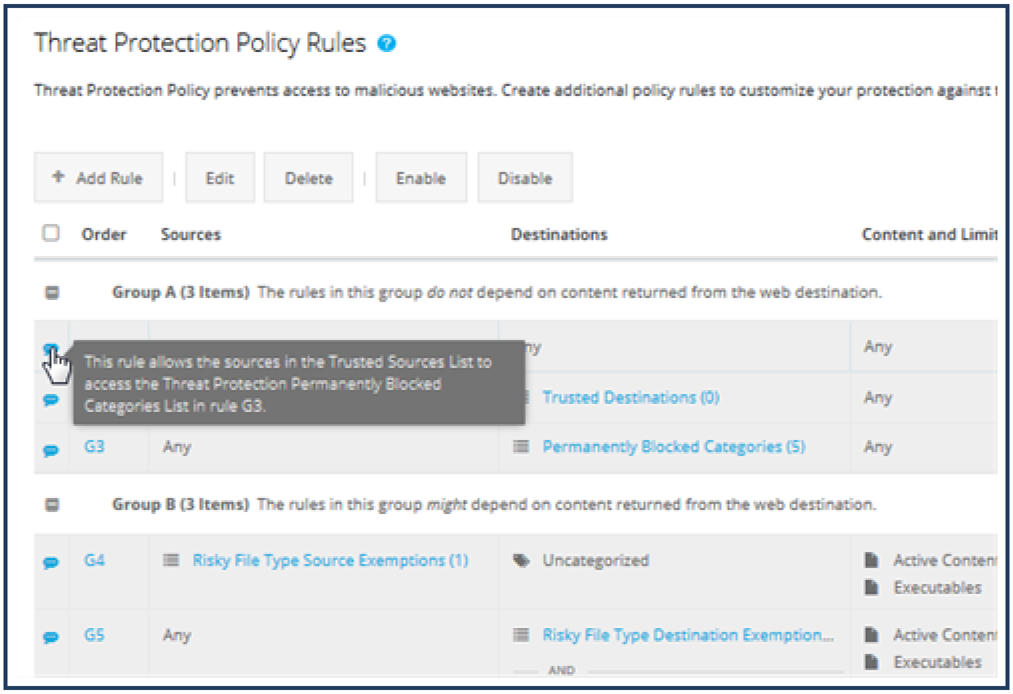
> **Tip:** If your account has provisioned the Advanced Web Security with Risk Controls and Web Applications add-on license, you can define policy based on Risk Scores. See "Malware Policy From Risk Score" on page 40.

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.



Threat Protection Policy Rules

Threat Protection Policy prevents access to malicious websites. Create additional policy rules to customize your protection against t

This rule allows the sources in the Trusted Sources List to access the Threat Protection Permanently Blocked Categories List in rule G3.

□ Order	Sources	Destinations	Content and Limit
Group A (3 Items) The rules in this group *do not* depend on content returned from the web destination.			
		ny	Any
		Trusted Destinations (0)	Any
G3	Any	Permanently Blocked Categories (5)	Any
Group B (3 Items) The rules in this group *might* depend on content returned from the web destination.			
G4	Risky File Type Source Exemptions (1)	Uncategorized	Active Conten Executables
G5	Any	Risky File Type Destination Exemption... AND	Active Conten Executables

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 19.

   - 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 54.

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.

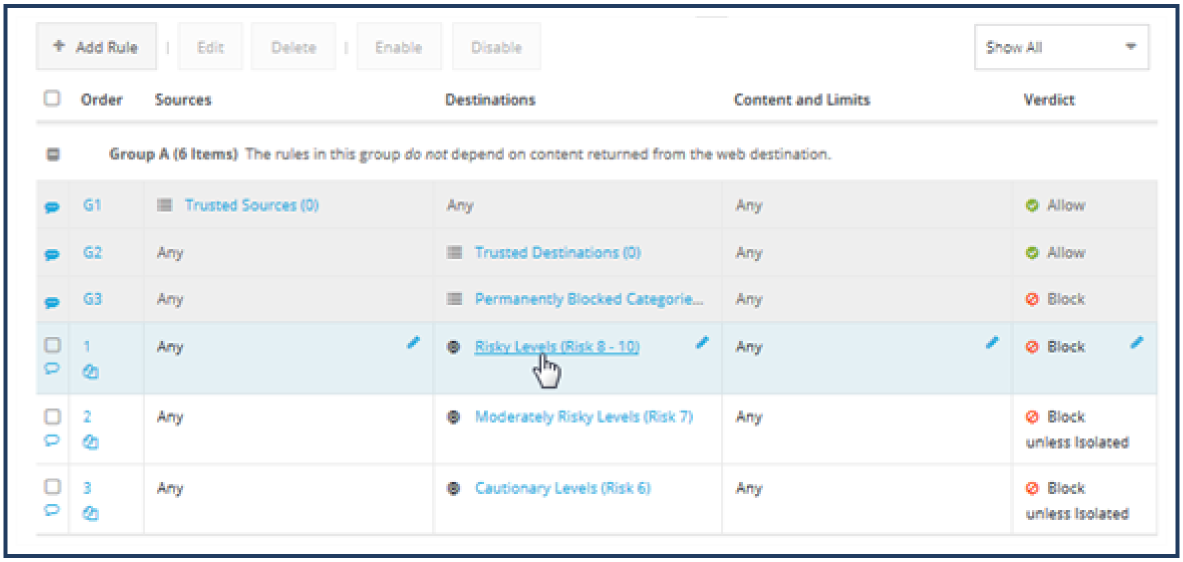
Score	Description
1-2	Content is **Very Likely Safe**. Sites have a proven history of proper behavior.
3-4	Content is **Likely Safe**. Sites are beginning establish a history of proper behavior.
5-6	Content is **Cautious**. Possibilities exist that the sites might not be yet proven to be safe.
7-8	Content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

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 **Unrated** 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 38. 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.



□	Order	Sources	Destinations	Content and Limits	Verdict
		Group A (6 Items) The rules in this group *do not* depend on content returned from the web destination.			
	G1	Trusted Sources (0)	Any	Any	Allow
	G2	Any	Trusted Destinations (0)	Any	Allow
	G3	Any	Permanently Blocked Categorie...	Any	Block
□	1	Any	Risky Levels (Risk 8 - 10)	Any	Block
□	2	Any	Moderately Risky Levels (Risk 7)	Any	Block unless Isolated
□	3	Any	Cautionary Levels (Risk 6)	Any	Block unless Isolated

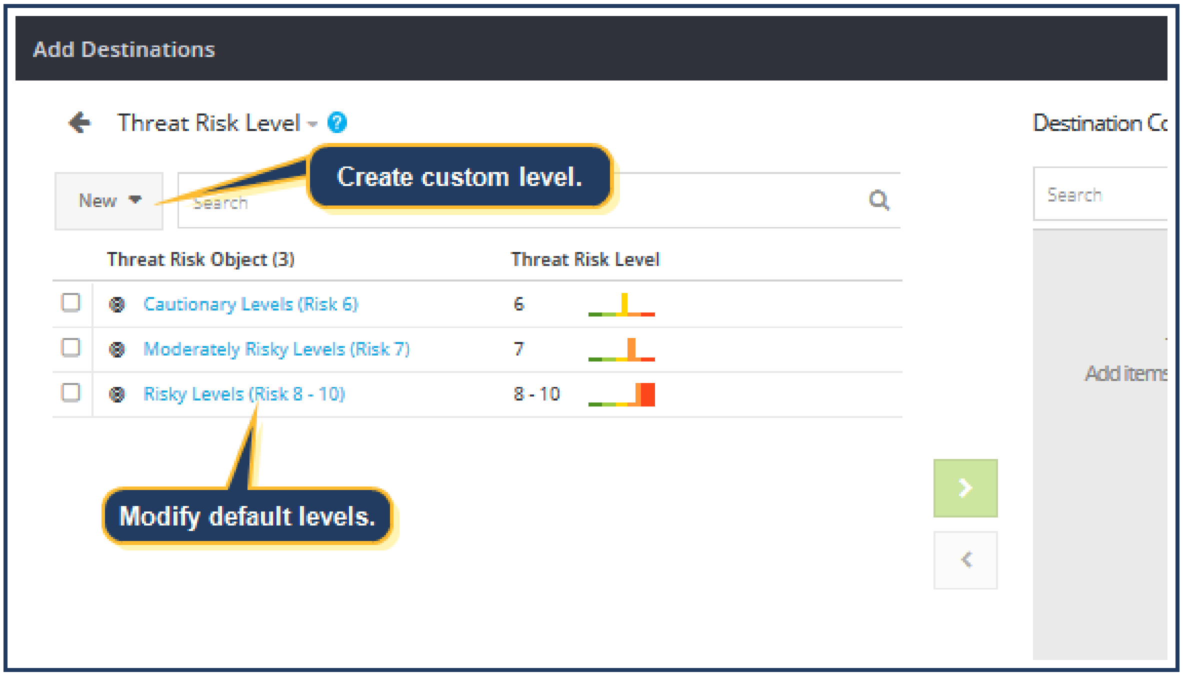
By default, the Web Security Service provides three **Group A** rows with **Cautionary (6)**, **Moderately Risky (7)**, and **Risky Levels (8-10)**. By default, these default risk level rules are set to a **Block** verdict. If your portal account has the Web Isolation add-on license, the default for **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.



Threat Risk Object (3)	Threat Risk Level
Cautionary Levels (Risk 6)	6
Moderately Risky Levels (Risk 7)	7
Risky Levels (Risk 8 - 10)	8 - 10

- 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

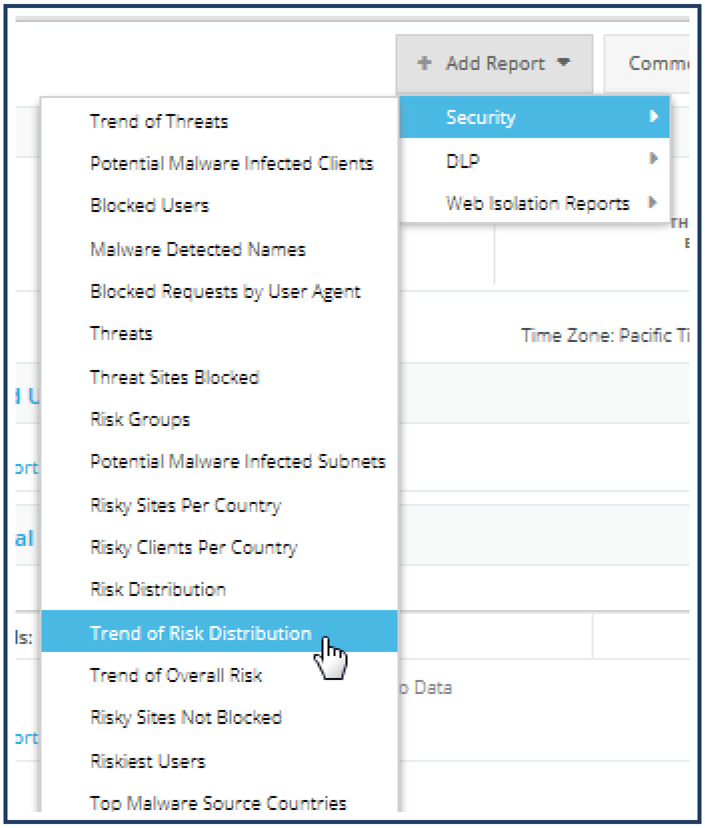
The Web Security Service provides several default reports based on risk scores.

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

On the **Service** mode **> Threat Protection > Dashboard** page, select risk score-based report applets from the **Add Report > Security** menu.



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 SymantecWeb 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 scannning**
- **Malware Analysis** (if the account has the MASS or MAAS license)

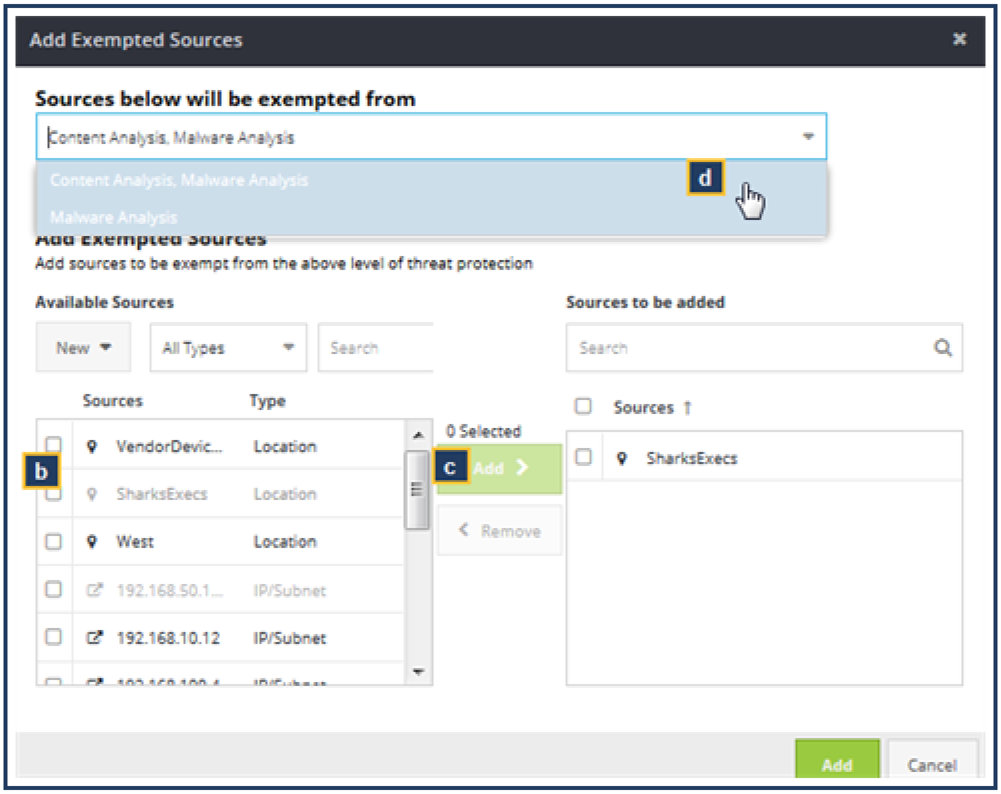
If the account has the MASS or MAAS license, you can elect to not apply **Malware analysis** or **Malware analysis** and **Anti-virus engine scanning**.

Procedure

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

Sources below will be exempted from

Content Analysis, Malware Analysis

- Content Analysis, Malware Analysis
- Malware Analysis

Add Exempted Sources

Add sources to be exempt from the above level of threat protection

Available Sources

Sources	Type
VendorDevic...	Location
SharksExecs	Location
West	Location
192.168.50.1...	IP/Subnet
192.168.10.12	IP/Subnet

0 Selected

Sources to be added

Sources
SharksExecs

b. Select existing objects.

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

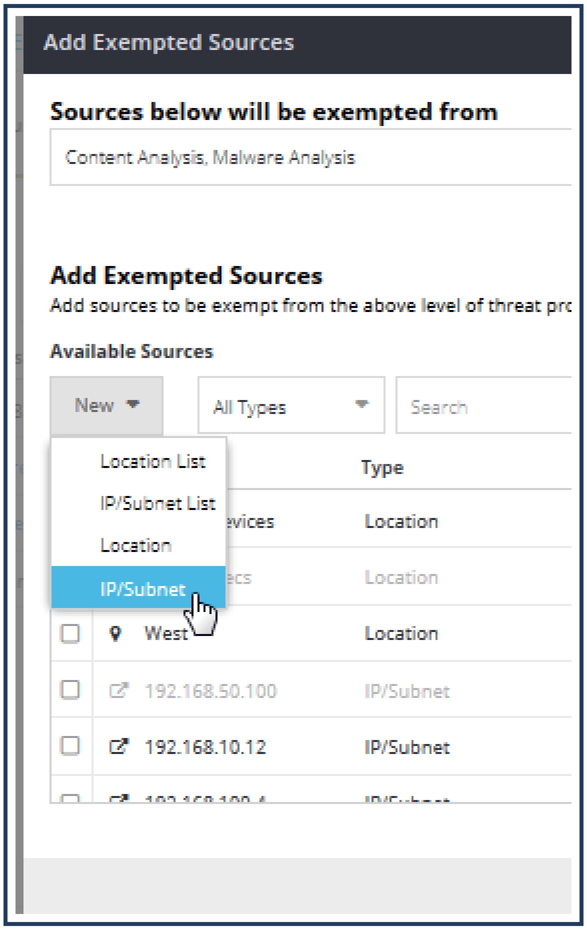
d. Verify/select the malware scanning levels that are *not* performed against this source.

e. Click **Add**.

4. (Option 2) Create a new object.

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

b. In the dialog, click **New** and select what to add.



Add Exempted Sources

Sources below will be exempted from

Content Analysis, Malware Analysis

Add Exempted Sources

Add sources to be exempt from the above level of threat prc

Available Sources

		Type
	evices	Location
	ecs	Location
□	West	Location
□	192.168.50.100	IP/Subnet
□	192.168.10.12	IP/Subnet

- **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.

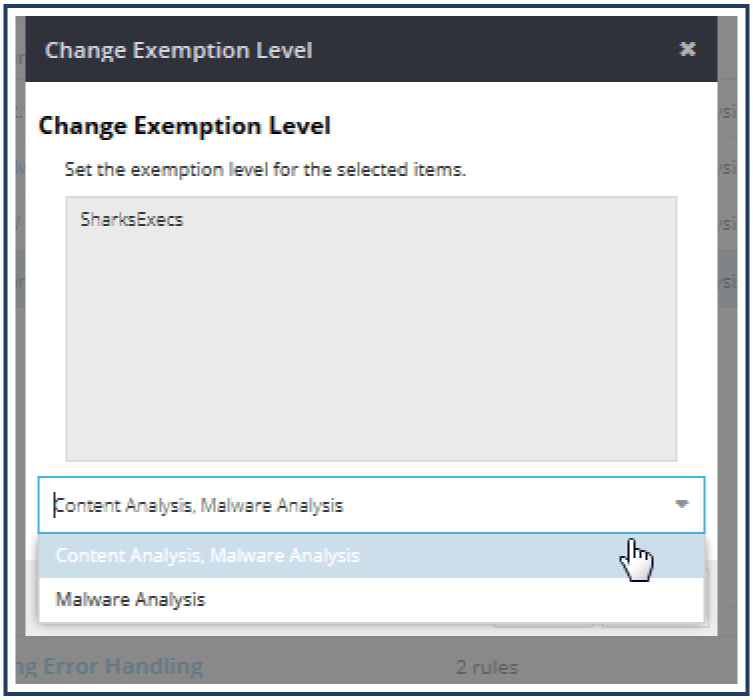
c. Click **Save**.

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 43.



Change Exemption Level

Change Exemption Level

Set the exemption level for the selected items.

SharksExecs

Content Analysis, Malware Analysis

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. Sselect a different level and click **Save**.

e. Click **Activate**.

Next Step

- Exempt Files From Error Handling
- Return to "Protect Your Network From Web Threats" on page 36.

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 scannning**
- **Malware Analysis** (if the account has the MASS or MAAS license)

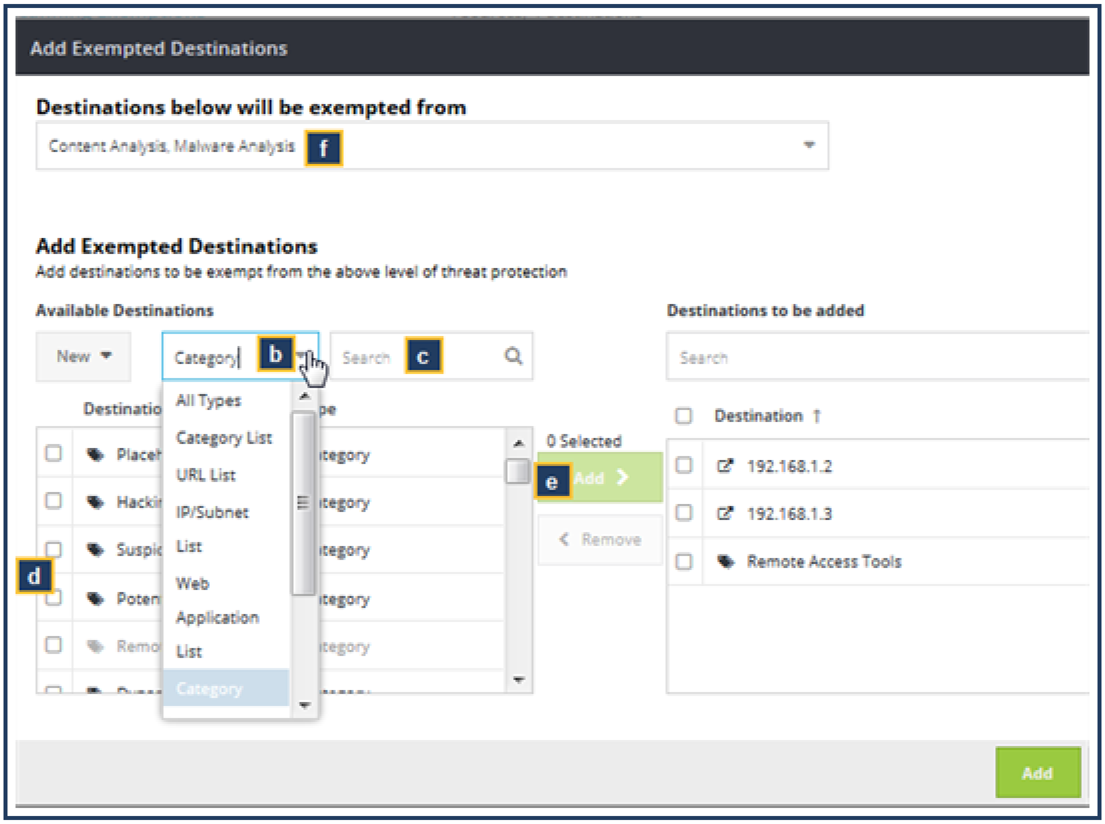
If the account has the MASS or MAAS license, you can elect to not apply **Malware analysis** or **Malware analysis** and **Anti-virus engine scanning**.

Procedure

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

Destinations below will be exempted from

Content Analysis, Malware Analysis

Add Exempted Destinations

Add destinations to be exempt from the above level of threat protection

Available Destinations

Destinations to be added

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.

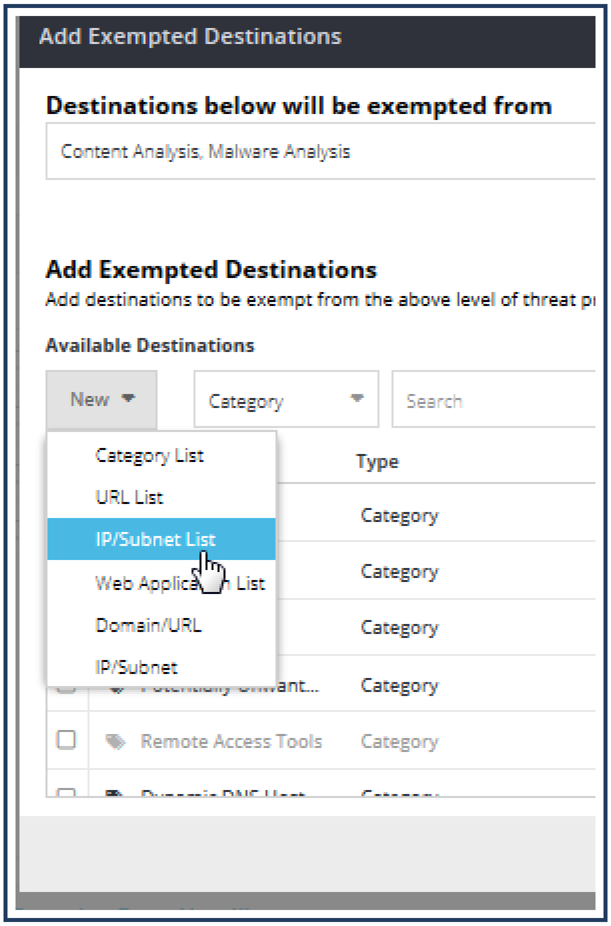
f. Verify/select the malware scanning levels that are *not* performed against this source.

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.



Add Exempted Destinations

Destinations below will be exempted from

Content Analysis, Malware Analysis

Add Exempted Destinations

Add destinations to be exempt from the above level of threat pı

Available Destinations

- **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
- Return to "Protect Your Network From Web Threats" on page 36.

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 cyberattacks 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:

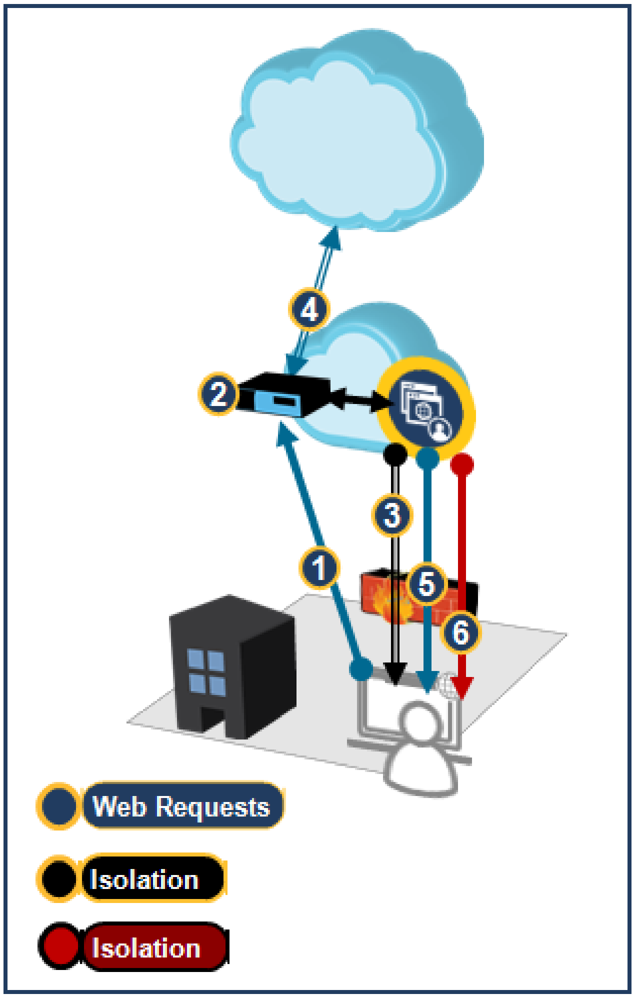
- Provides a safe visual stream of the original web site in the user's browser.
- End users browse the site as if the site was running directly in the browser.
- Preserves original browsing experience with full usability and control.
- Only safely rendered information arrives at the user's browser.
- 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, phishing, 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 Threat 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 12.

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

- You must ensure the service root certificate is installed on all clients.
- 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

Threat 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.

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

Optional Prerequisite—Enable SSL

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

  "Examine Encrypted (HTTPS) Traffic" on page 83

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.

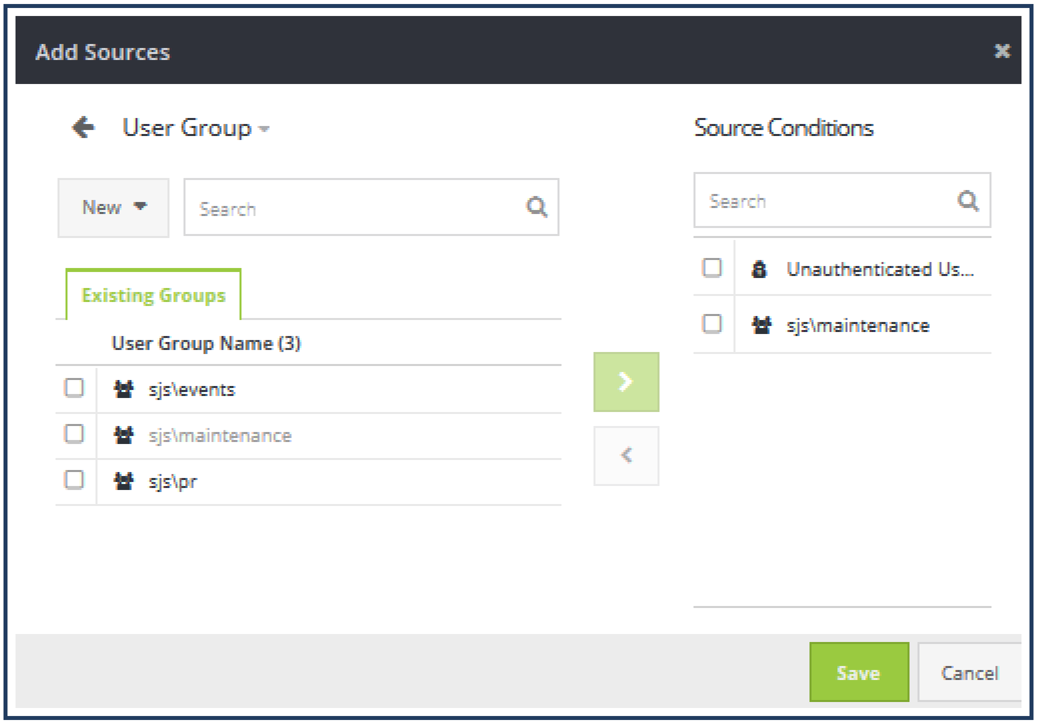
> **Tip:** The following procedure demonstrates defining policy that applies Web Isolation. Performing the same steps, you can also define policy that exempts traffic from Threat Isolation.

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**.

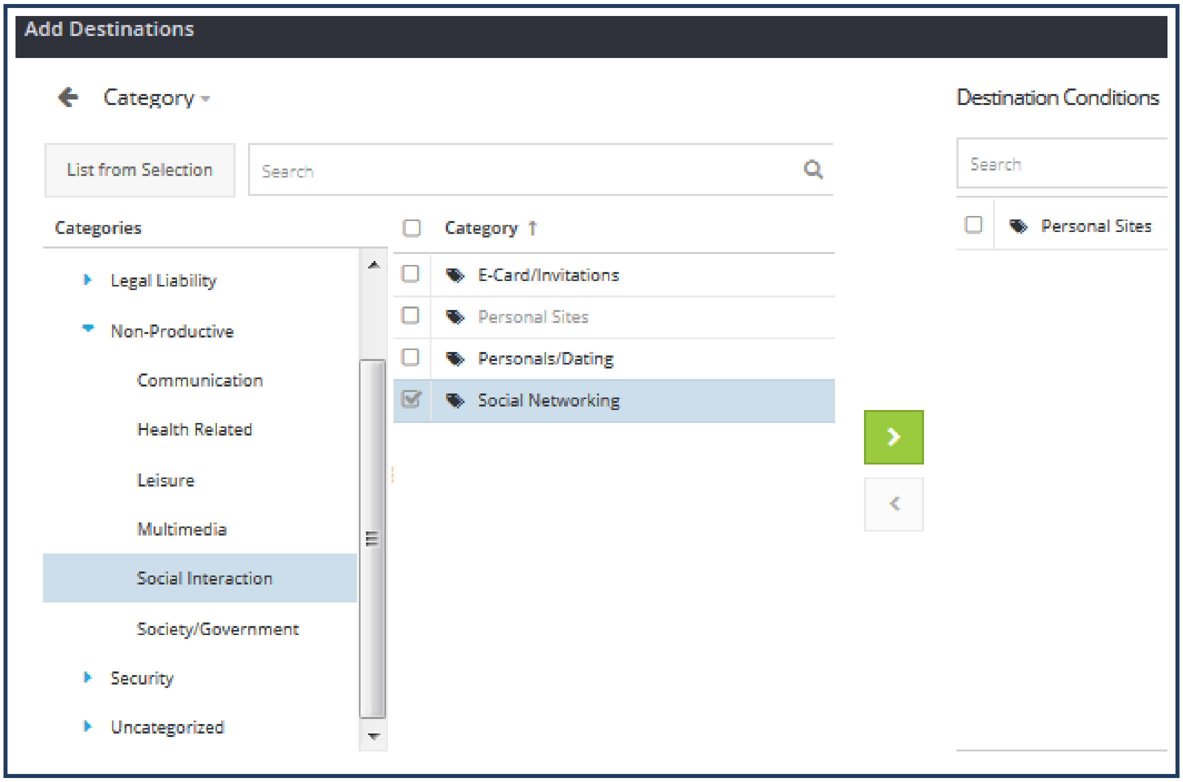


For example, you want Web Isolation applied to all **Unauthenticated Users** and specified **Groups**.

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

Click **Save**.

3. Click **Add Destinations**.

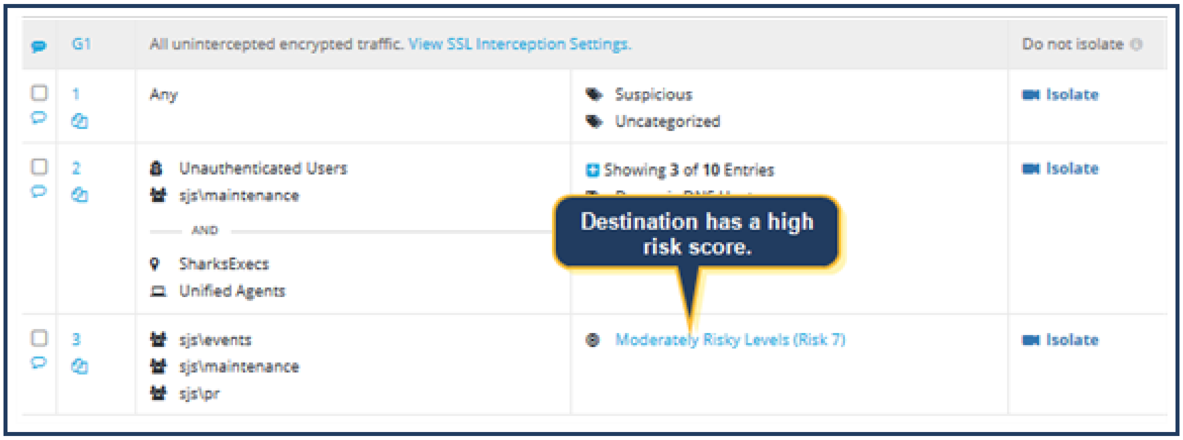


For example, you want to add **Social Networking** categories.

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.



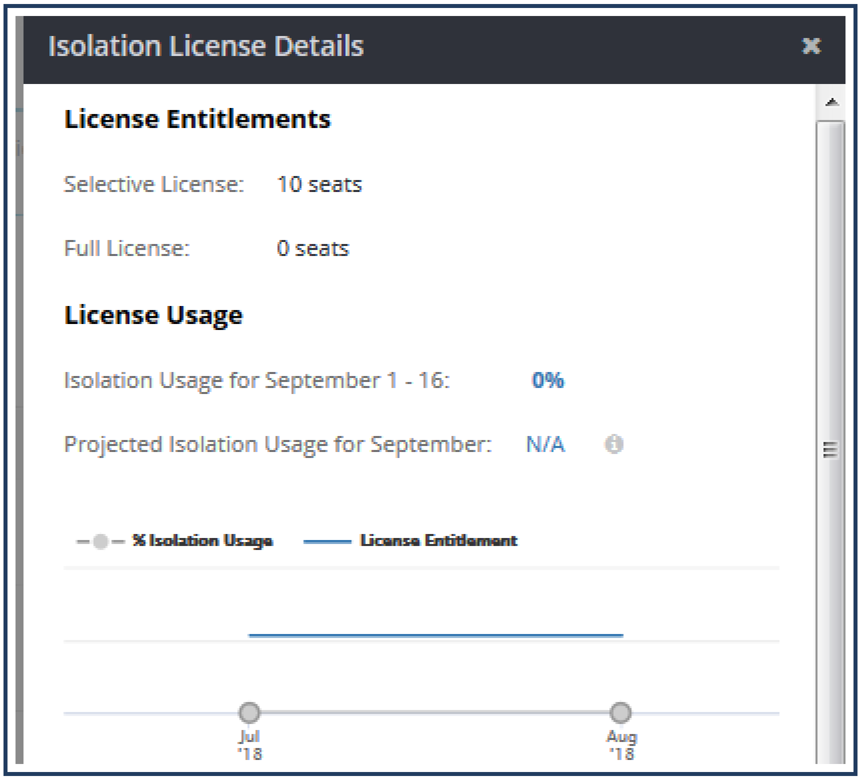
	G1	All unintercepted encrypted traffic. View SSL Interception Settings.		Do not isolate
□	1	Any	Suspicious Uncategorized	Isolate
□	2	Unauthenticated Users sjs\maintenance AND SharksExecs Unified Agents	Showing 3 of 10 Entries	Isolate
□	3	sjs\events sjs\maintenance sjs\pr	Moderately Risky Levels (Risk 7)	Isolate

Destination has a high risk score.

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.



Isolation License Details

License Entitlements

Selective License: 10 seats

Full License: 0 seats

License Usage

Isolation Usage for September 1 - 16: 0%

Projected Isolation Usage for September: N/A

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, the 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**.

Web Application Policy

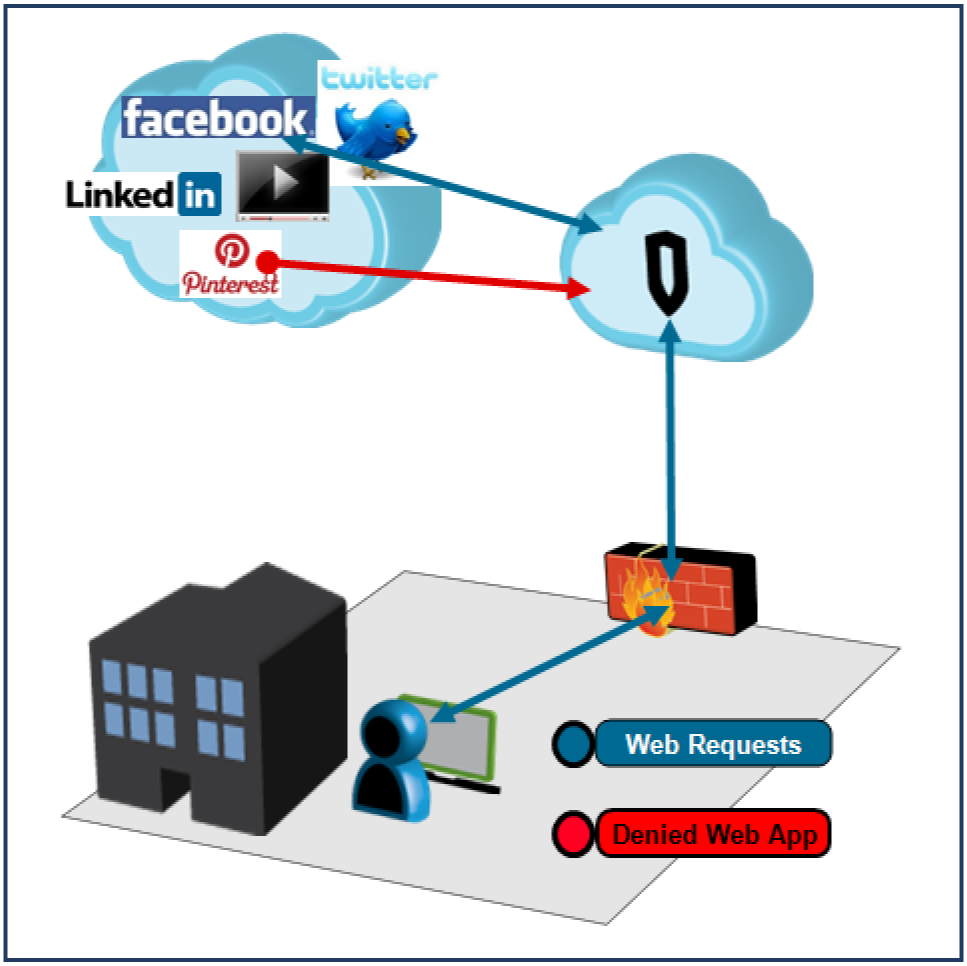
Delete this text and replace it with your own content.

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.

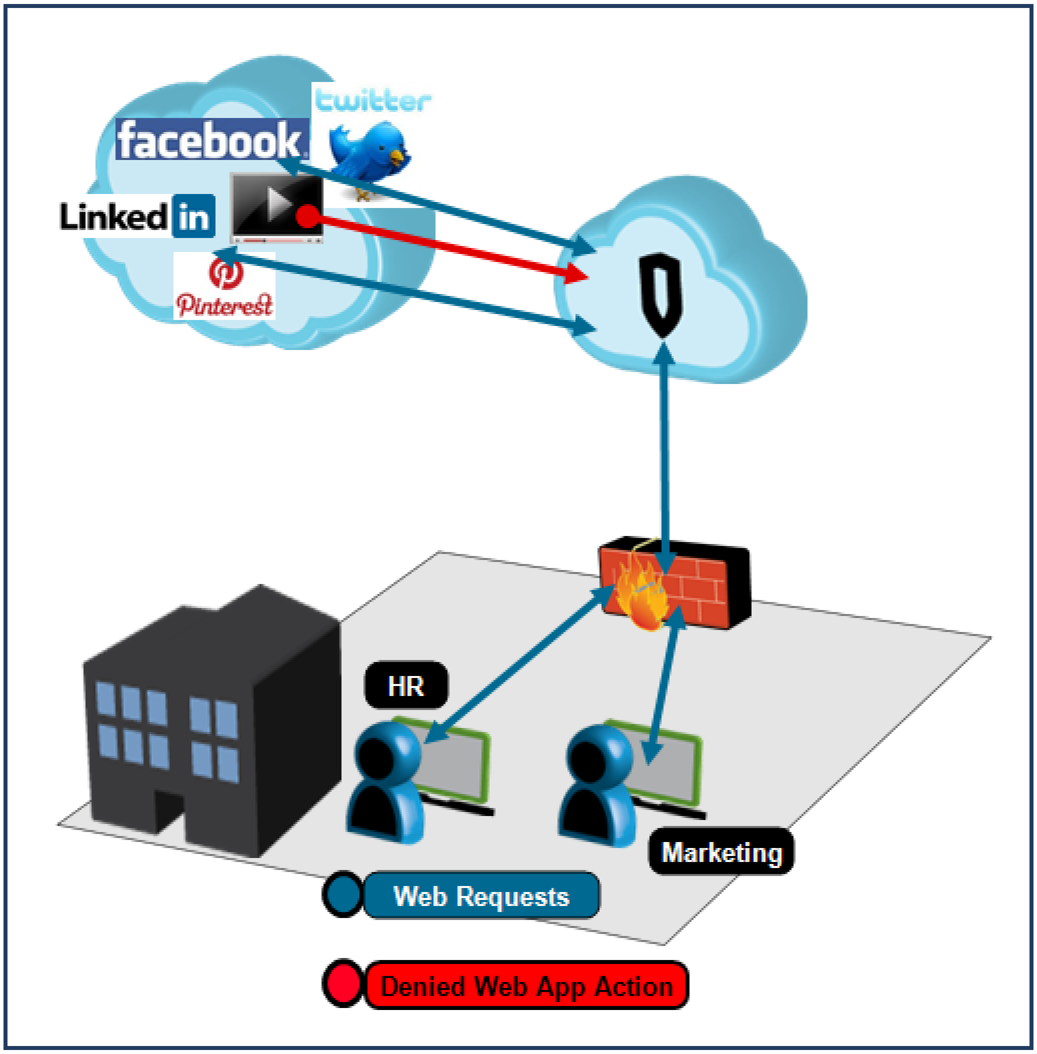
Always Block or Always Allow a Web Application

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.



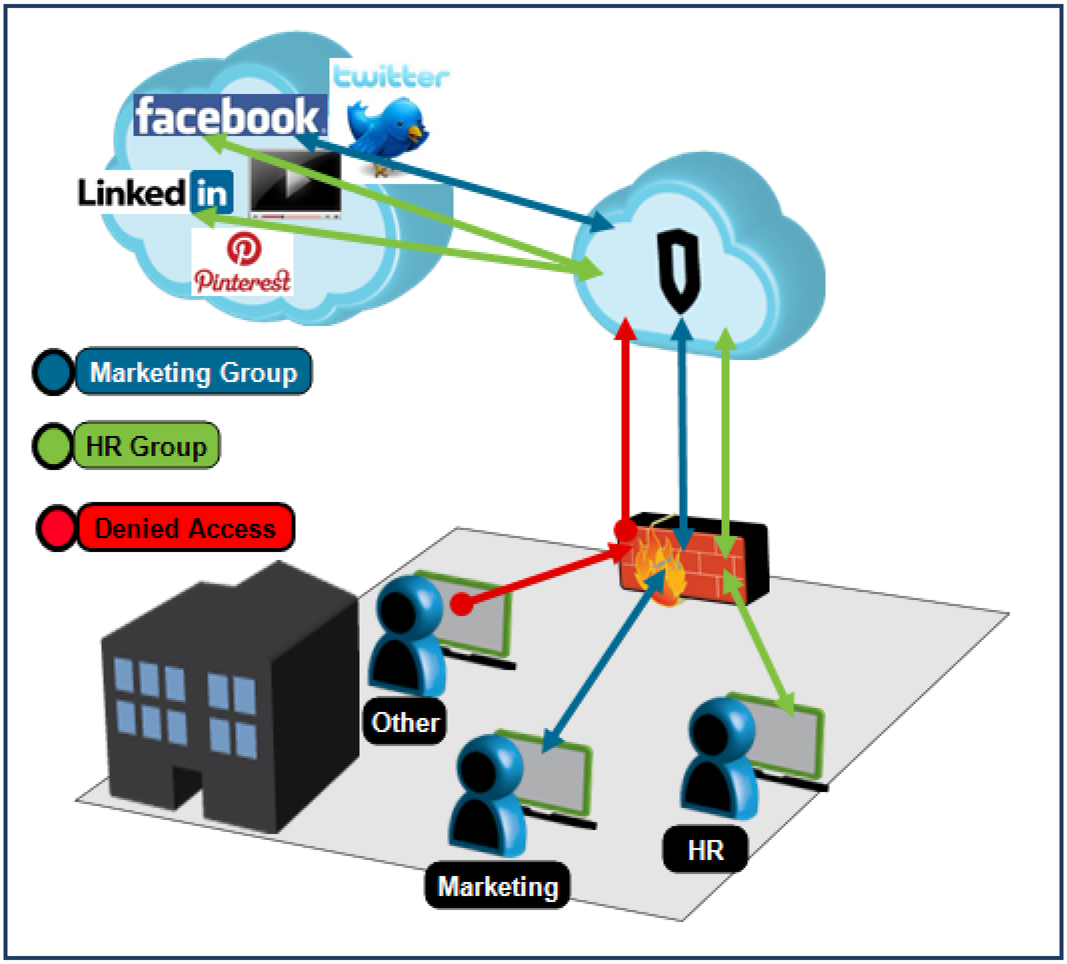
Allow a Web Application But Block an Action

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.

- Web Application Reference Article

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.

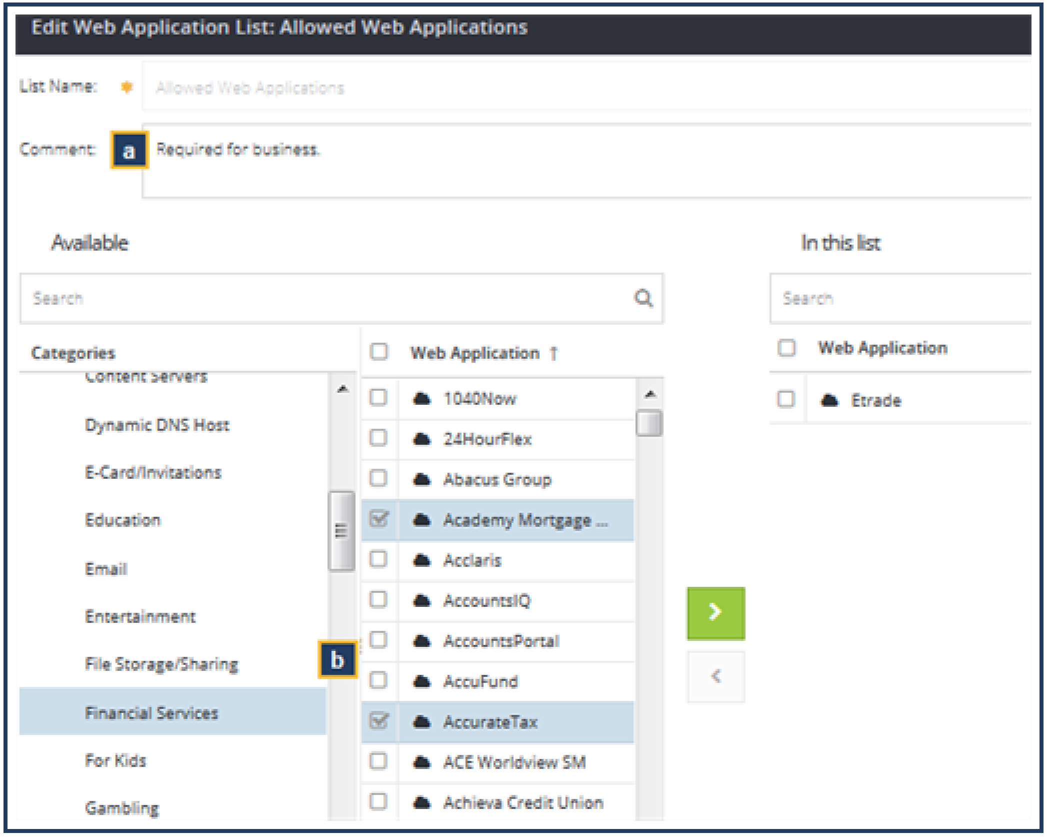
- Web Application Reference Article

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**.



Edit Web Application List: Allowed Web Applications

List Name: * Allowed Web Applications

Comment: Required for business.

Available

Categories

- Content Servers
- Dynamic DNS Host
- E-Card/Invitations
- Education
- Email
- Entertainment
- File Storage/Sharing
- Financial Services
- For Kids
- Gambling

□ Web Application ↑

- □ 1040Now
- □ 24HourFlex
- □ Abacus Group
- ☑ Academy Mortgage ...
- □ Acclaris
- □ AccountsIQ
- □ AccountsPortal
- □ AccuFund
- ☑ AccurateTax
- □ ACE Worldview SM
- □ Achieva Credit Union

In this list

□ Web Application

- □ Etrade

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

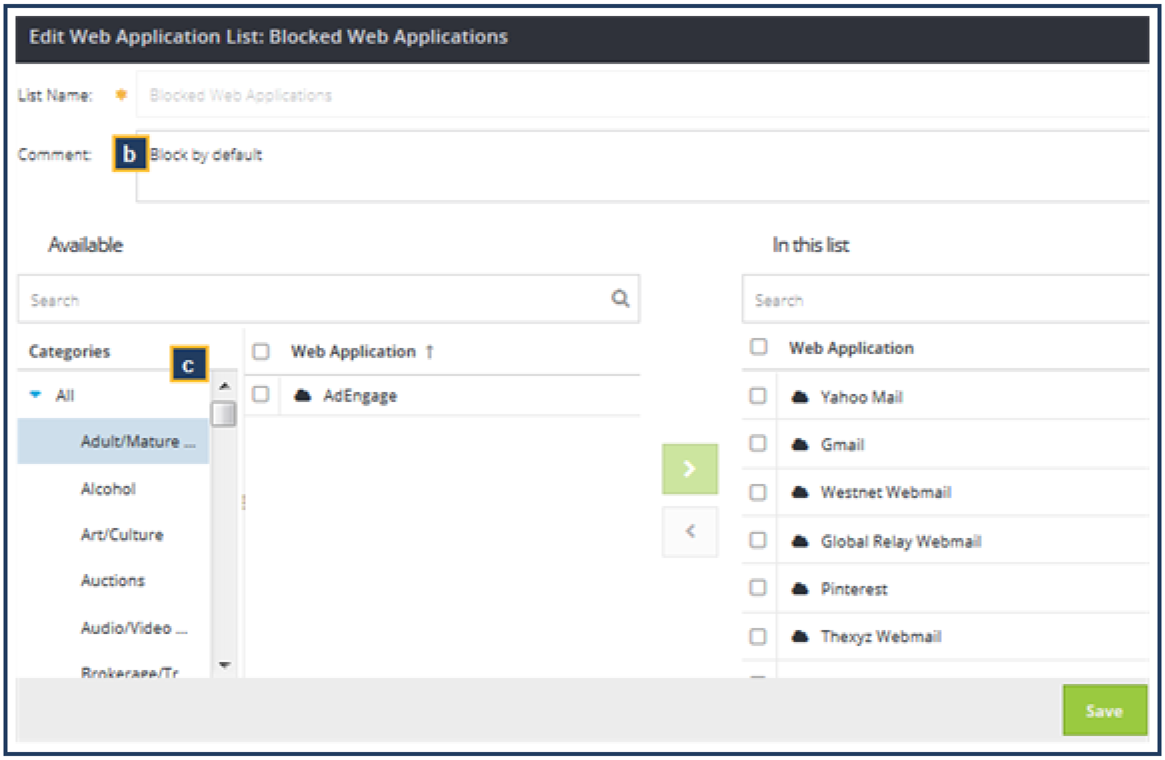
> **Tip:** Obtaining the Symantec CASB license exposes thousands of applications.

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

List Name: * Blocked Web Applications

Comment: Block by default

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.

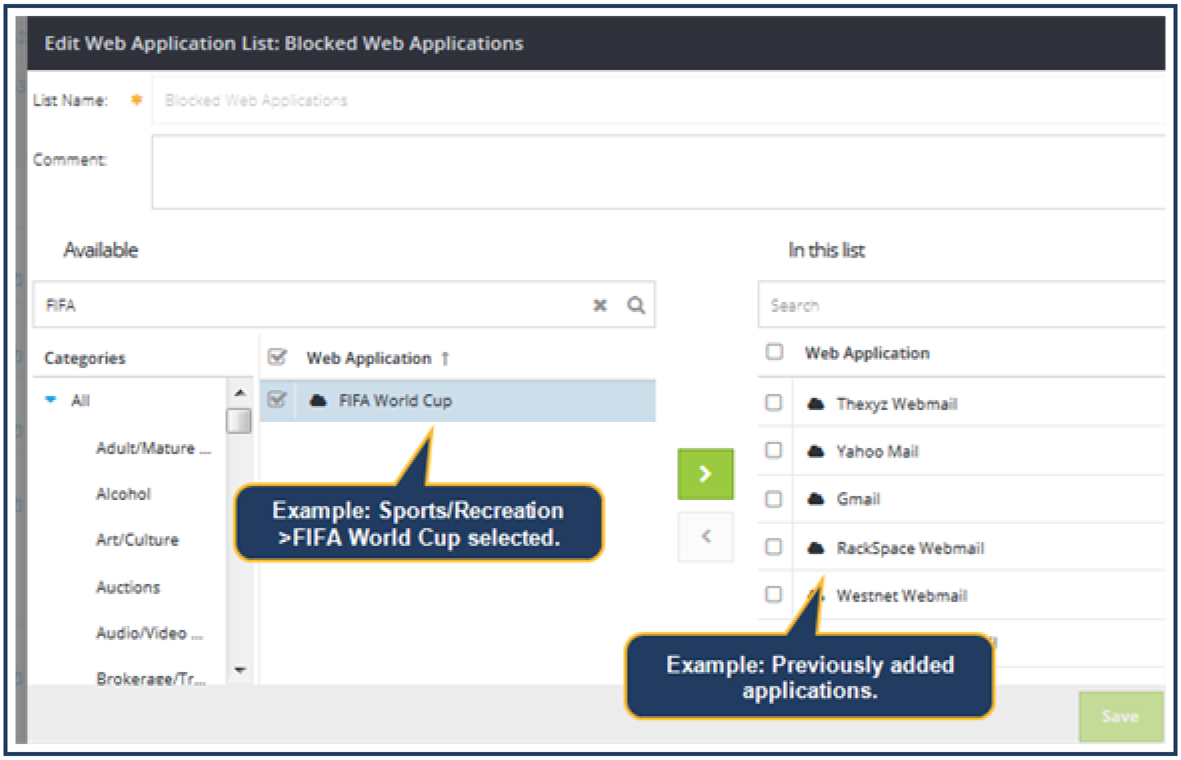
- The FIFA World Cup creates network bandwidth havoc every year; furthermore, reports indicate that Pinterest traffic is trending upward and you want to block access.
- Both Facebook and Twitter are productivity hindrance, yet are necessary marketing applications. You want to allow access only to the 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**.



Edit Web Application List: Blocked Web Applications

List Name: * Blocked Web Applications

Comment:

Available: FIFA

In this list: Search

☑ Web Application ↑

☑ FIFA World Cup

Example: Sports/Recreation >FIFA World Cup selected.

Example: Previously added applications.

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 **Social Networking** and **Sports** application.

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

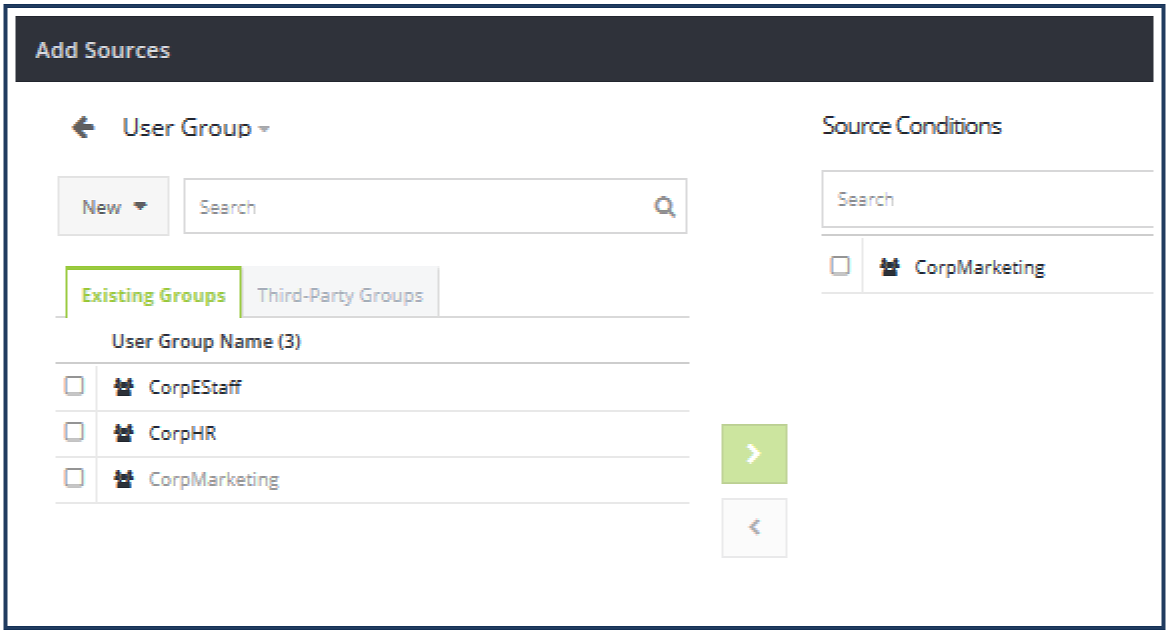
3. Allow Marketing access to Facebook and Twitter.

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.

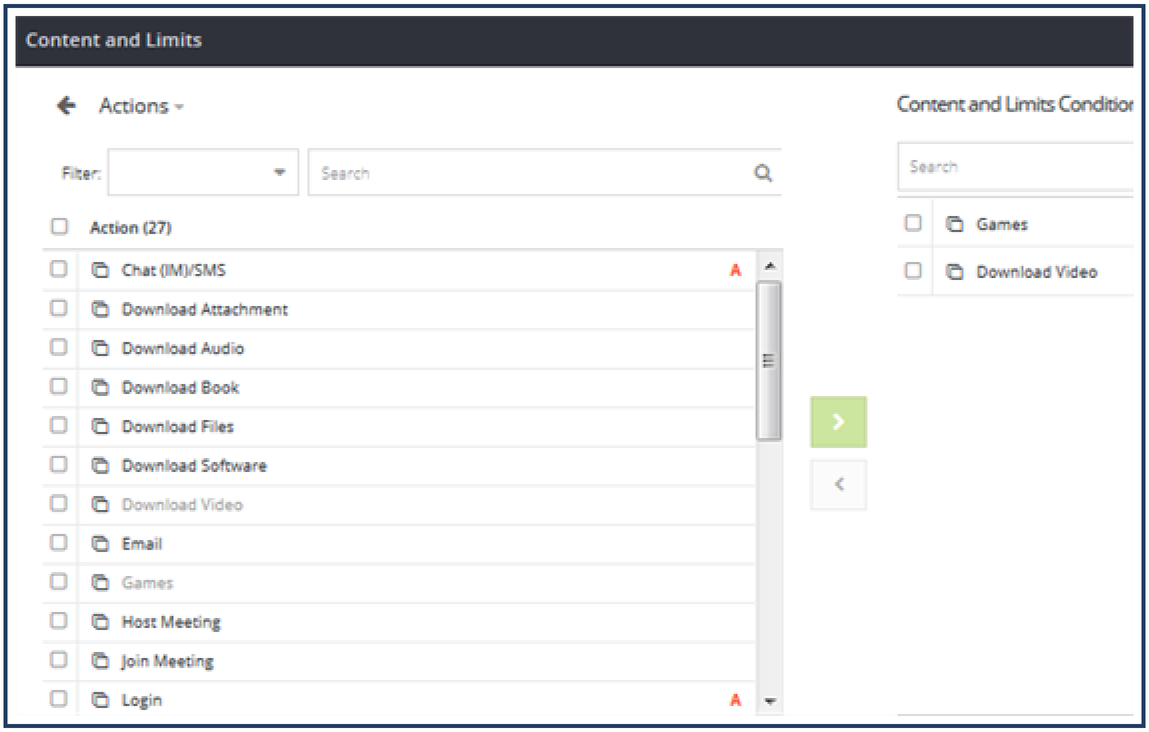
4. You now want to prevent Marketing employees from downloading attachments, playing games, and chatting from within Facebook.

   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**.



Content and Limits

□ Action (27)

- □ Chat (IM)/SMS
- □ Download Attachment
- □ Download Audio
- □ Download Book
- □ Download Files
- □ Download Software
- □ Download Video
- □ Email
- □ Games
- □ Host Meeting
- □ Join Meeting
- □ Login

Content and Limits Conditio

- □ Games
- □ Download Video

e. Click **Save**.

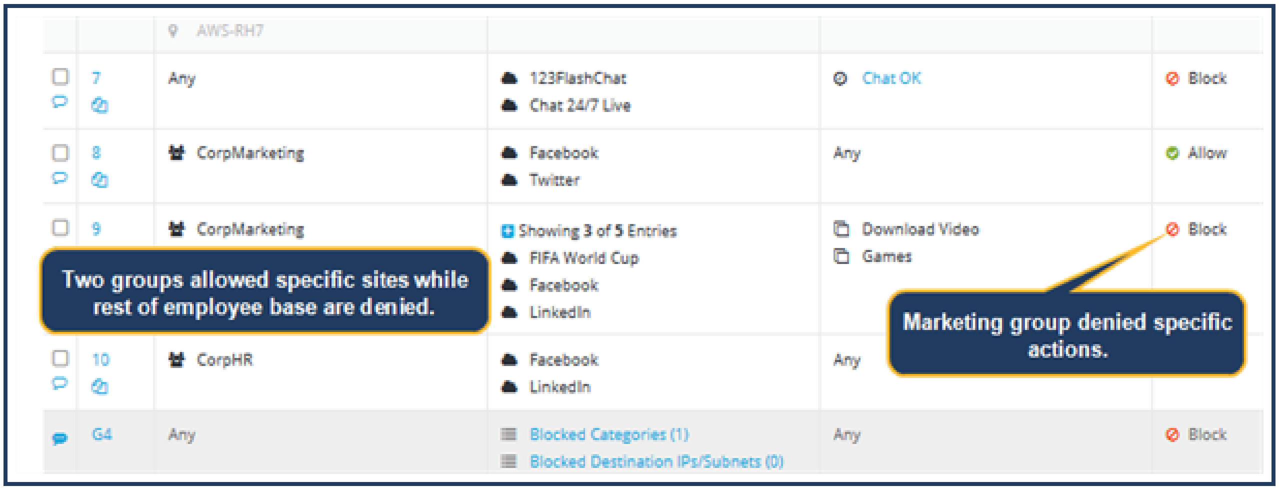
f. Set the **Verdict** construct to **Block**.

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.



		AWS-RH7			
□	7	Any	123FlashChat Chat 24/7 Live	Chat OK	Block
□	8	CorpMarketing	Facebook Twitter	Any	Allow
□	9	CorpMarketing	Showing 3 of 5 Entries FIFA World Cup Facebook LinkedIn	Download Video Games	Block
□	10	CorpHR	Facebook LinkedIn	Any	
	G4	Any	Blocked Categories (1) Blocked Destination IPs/Subnets (0)	Any	Block

Two groups allowed specific sites while rest of employee base are denied.

Marketing group denied specific actions.

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.

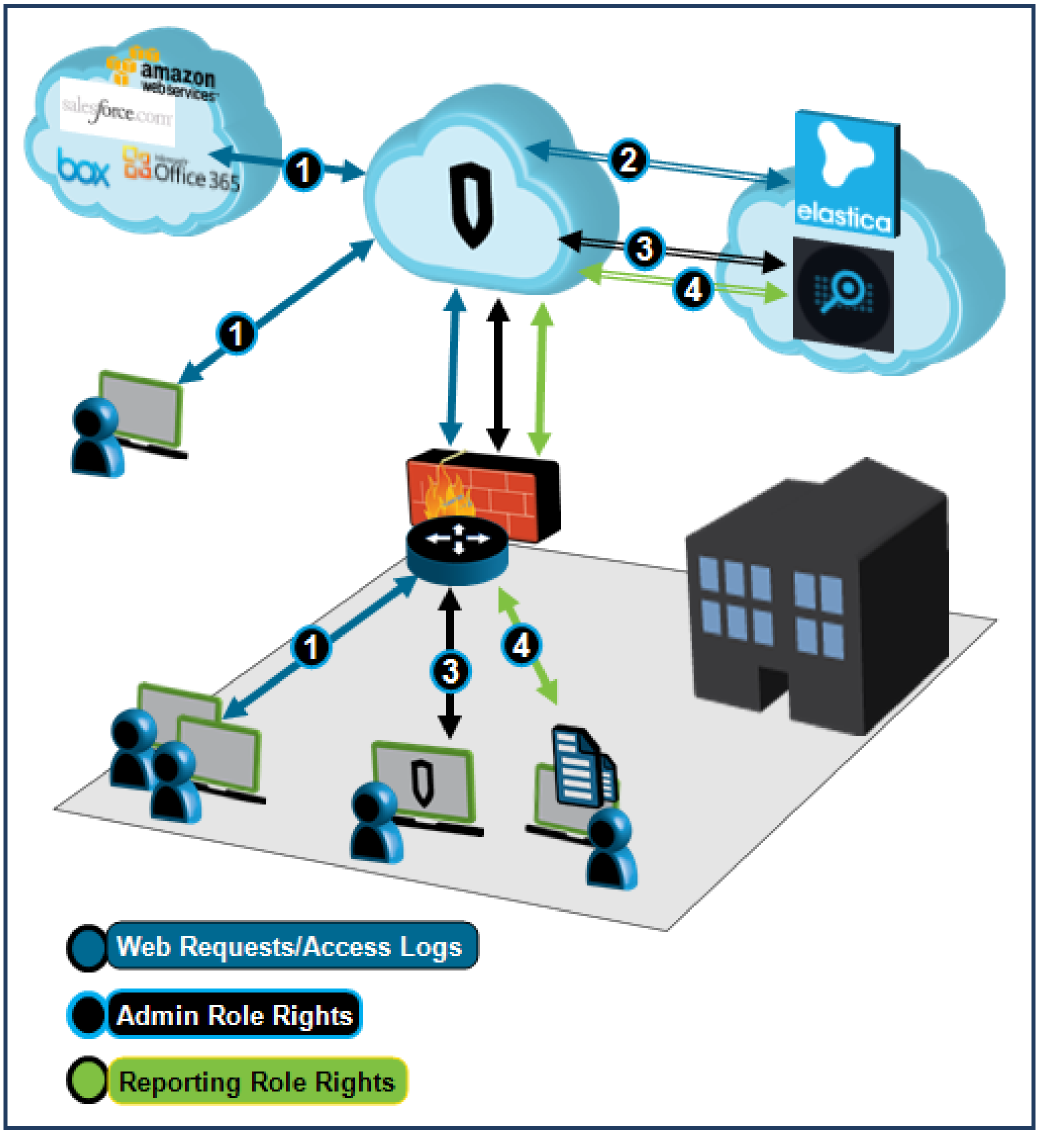
Connect to the CASB Audit Service

The CASB Audit Service provides visibility to 15,000 cloud applications plus over 60 attributes *per* application. This enables scalable policy to control Shadow IT and cloud application access.

The CASB Audit Service is an integration between the Web Security Service and the Symantec CloudSOC™ platform. The CloudSOC contains an Audit applet, which provides granular visibility of the web applications. With the supplemental CASB Audit Service license, you can connect to this Audit applet from your Web Security Service account portal and view web application reports. Analyzing these reports allows you to further refine your web application access and security policies.

Audit Service Topography

This topography assumes that you have the CASB Audit Service license and registered the service (which is discussed in more detail in the next section).



1—Regional employees (on campus or remote) perform requests for web applications. The Web Security Service processes the policy; allows or denies the content; and adds entries to the access logs. The Web Security Service uses these access logs for report generation.

2—Over a secure connection, an API connects the Web Security Service to the CloudSOC. The Web Security Service forwards the access logs to the CloudSOC.

3—A Web Security Service user in the Admin Role accesses the Web Security Service portal; from there, launches the CloudSOC service Audit application, which opens in a separate browser tab.

4—A Web Security Service user in the Reporting Role accesses the Web Security Service portal; from there, launches the CloudSOC service Audit application, which opens in a separate browser tab. Reporting Users can only perform basic reporting functions.

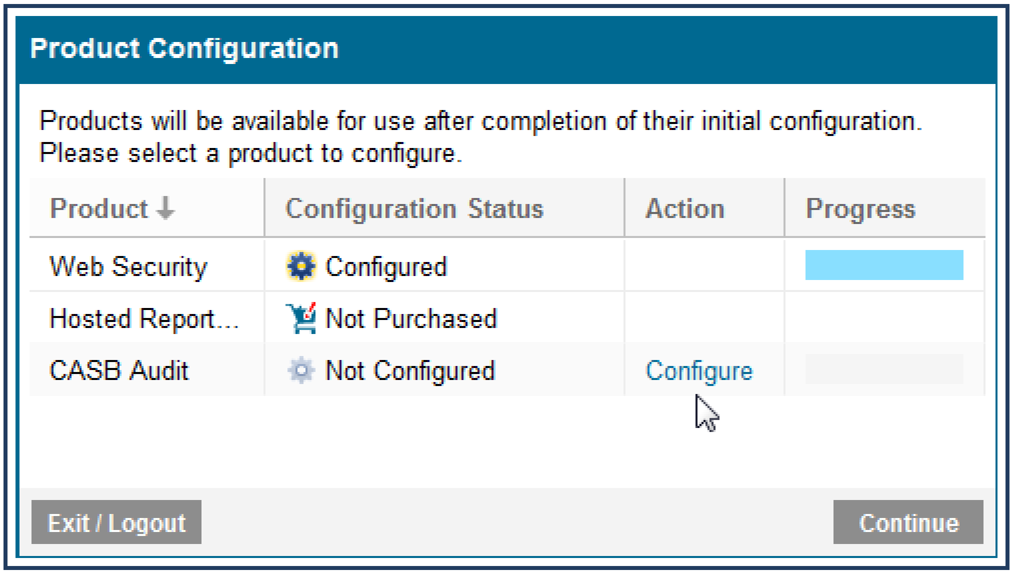
> **Note:** The Web Security Service maintains synchronicity with the WebPulse component of the Symantec Global Intelligence Network (GIN). Updates to the database occur each day.

Procedure

1. The next time you (as a Web Security Service admin) logs into the Web Security Service portal, the service matches the credentials against the entitlements, recognizes the new CASB Audit Service license, and displays the registration wizard page.

   > **Note:** If this is your first time registering any license/product on the Web Security Service, you must complete the admin credentials setup page.

   On the Product Configuration page, the Web Security Service displays the **CASB Audit** product as Not Configured.



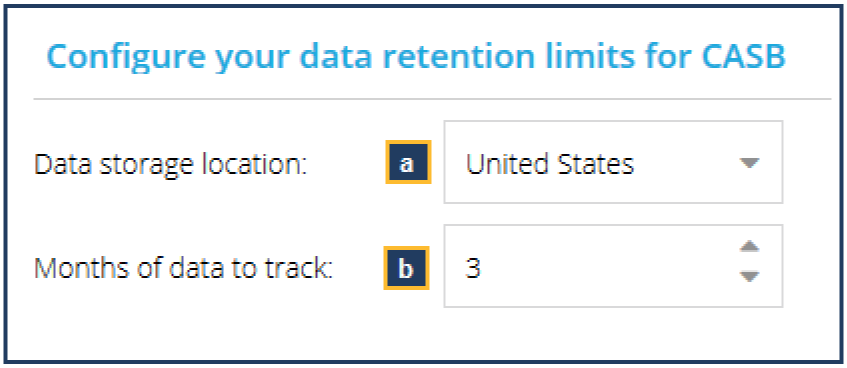
Product Configuration

Products will be available for use after completion of their initial configuration. Please select a product to configure.

Product ↓	Configuration Status	Action	Progress
Web Security	Configured		
Hosted Report...	Not Purchased		
CASB Audit	Not Configured	Configure	

   Click **Configure**.

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



Configure your data retention limits for CASB

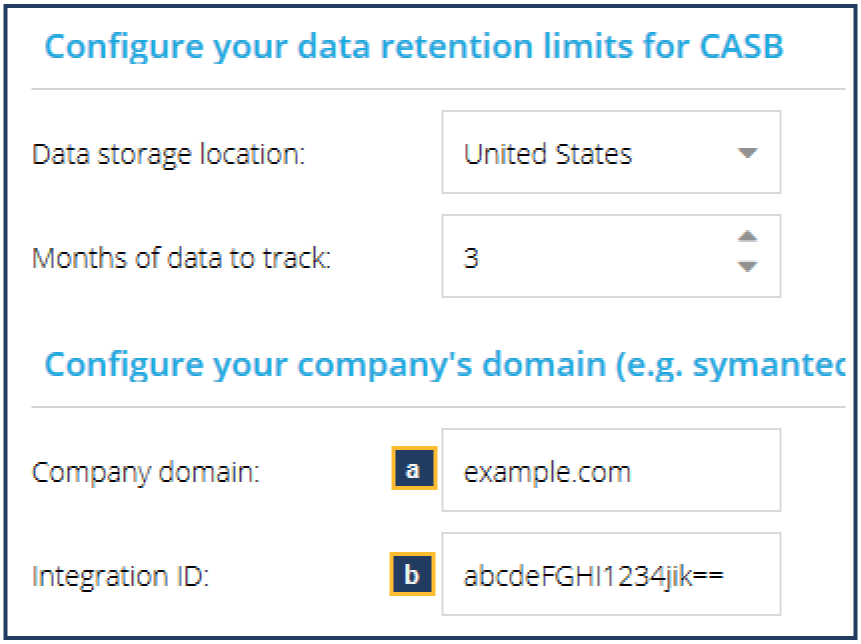
Data storage location: United States

Months of data to track: 3

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

Data storage location: United States

Months of data to track: 3

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

Company domain: example.com

Integration ID: abcdeFGHI1234jik==

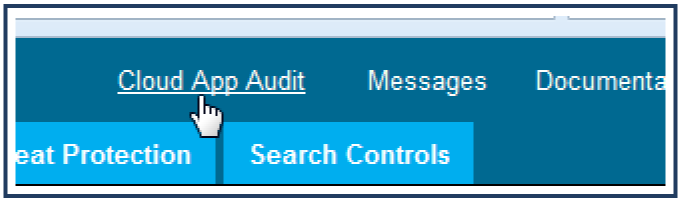
a. Enter your **Company Domain**.

b. Enter the **Integration ID** sent you by Symantec.

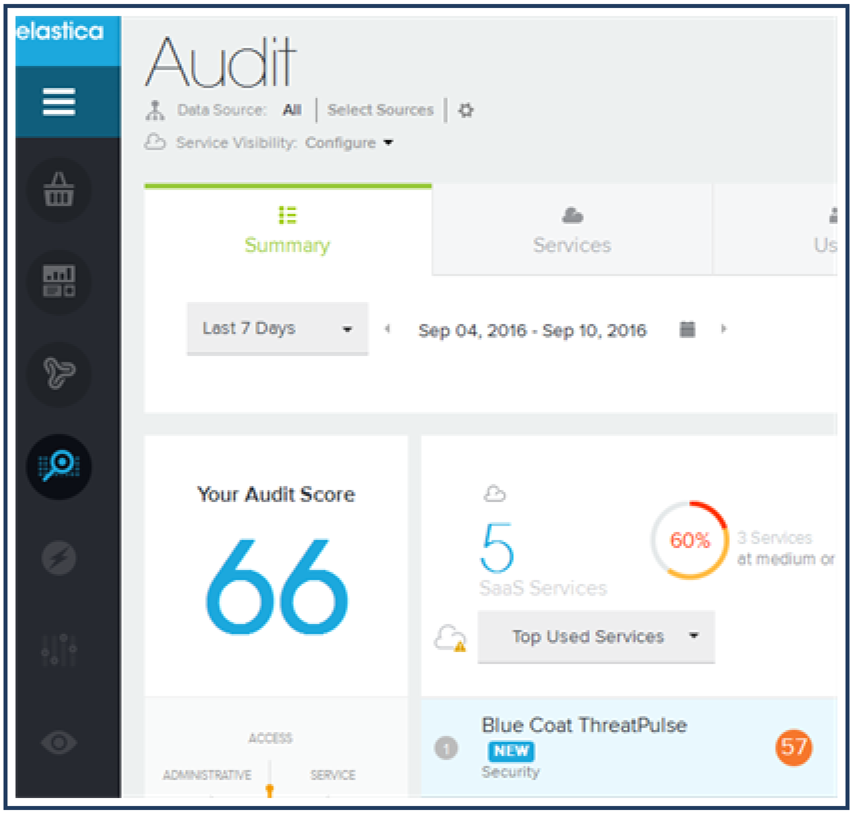
4. Click **Go To Product Setup**, which returns you to the Product Configuration page.
5. Click **Continue**.

Access the CASB Audit App

The top of Web Security Service portal has a link: **Cloud App Audit**.



When you click this link, the CloudSOC opens in a new browser tab.



The Audit page contains various data metrics, including report applets.

To learn more about using this Audit page, click the Help button (upper-right corner).

Reference: Supported Web Applications

This text file provides a list of the currently supported Web Applications when the CASB Audit license is active.

WSS_CASB_apps.txt

Web Application Policy

As web traffic begins flowing through your network, you now have the ability to define granular block/allow policy on the thousands of detected web applications. See Control Access to Web Applications.

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 access 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 > Users** page.

For more information, search for *roles* in the Solutions WebGuide.

CASB Policy and Reports

The CASB Audit Service is an integration between the Web Security Service and the Symantec CloudSOC™ platform. If you added the **CASB License** to your Web Security Service account, the web activity databases from which reports generate contain additional web application details.

Reference: Supported Web Applications

This text file provides a list of the currently supported Web Applications when the CASB Audit license is active.

WSS_CASB_apps.txt

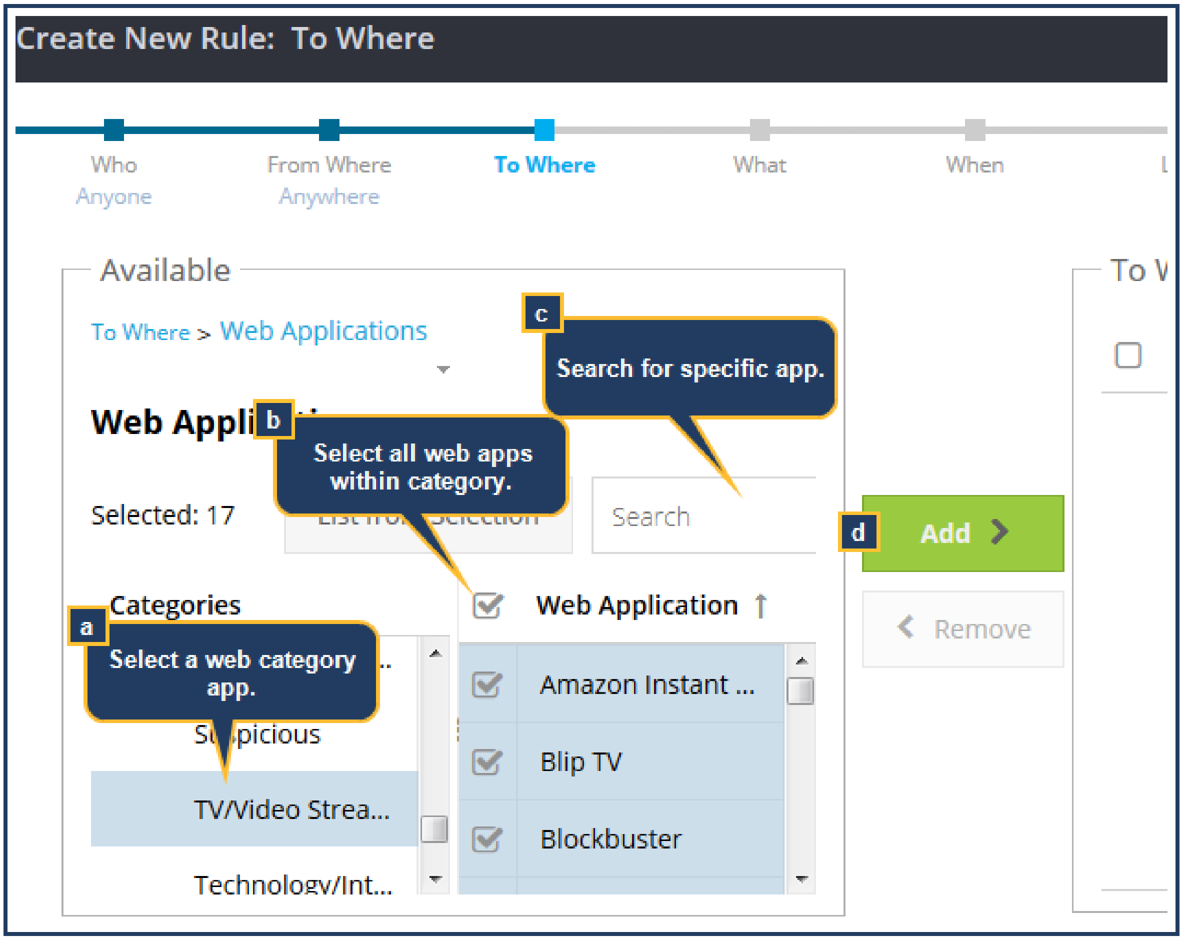
Take Action on Specific Web Applications

The CASB feed supplies the Content Filtering Policy Editor with thousands of web applications. This allows you to define as granular as a policy as is required to satisfy your organizations acceptable web use standards. There are two methods to achieve web application policy. Consider the following sections before implementing.

Application-Based

Example Use Case—You do not want any of your employees to use business assets to view streaming content, such as Hulu or Netflix. These applications are non-productive and consume high amounts of bandwidth.

1. Access the policy editor: **Solutions > Content Filtering > Policy**.
2. Click **Add Rule**. The portal displays the rule editor.
3. The first wizard page is **Who**. If you have a test **User** or **Group**, you can select that or allow the policy to apply to everyone by clicking **Next**.
4. The second page is **From Where**. Again, if you a test **Location** or **IP address**, select that or select sources as required.
5. The **To Where** page provides is where you select the web applications for this policy.



a. Continuing with the use case, this policy creator scrolls down to select **TV/Video Streams**.

b. Selecting this category populates the **Web Application** area with all of the detected apps that provide streaming services. You can select individual apps or click the head-level option to select all apps.

c. Click to **Add** to move the selected apps into the policy.

d. Click **Next**.

6. The next page, **What**, allows you select actions specific to these applications. The next section discusses this. For now, continue through the rule.

7. For now, continue through the rule, click **Next** for this and the next two pages to reach the **Verdict** page.

8. Select **Block** and click **Finish**.

   The service adds this rule to the **Content Filtering Rules** in **Group B** because the policy requires returned content responses to determine the blocked verdict.

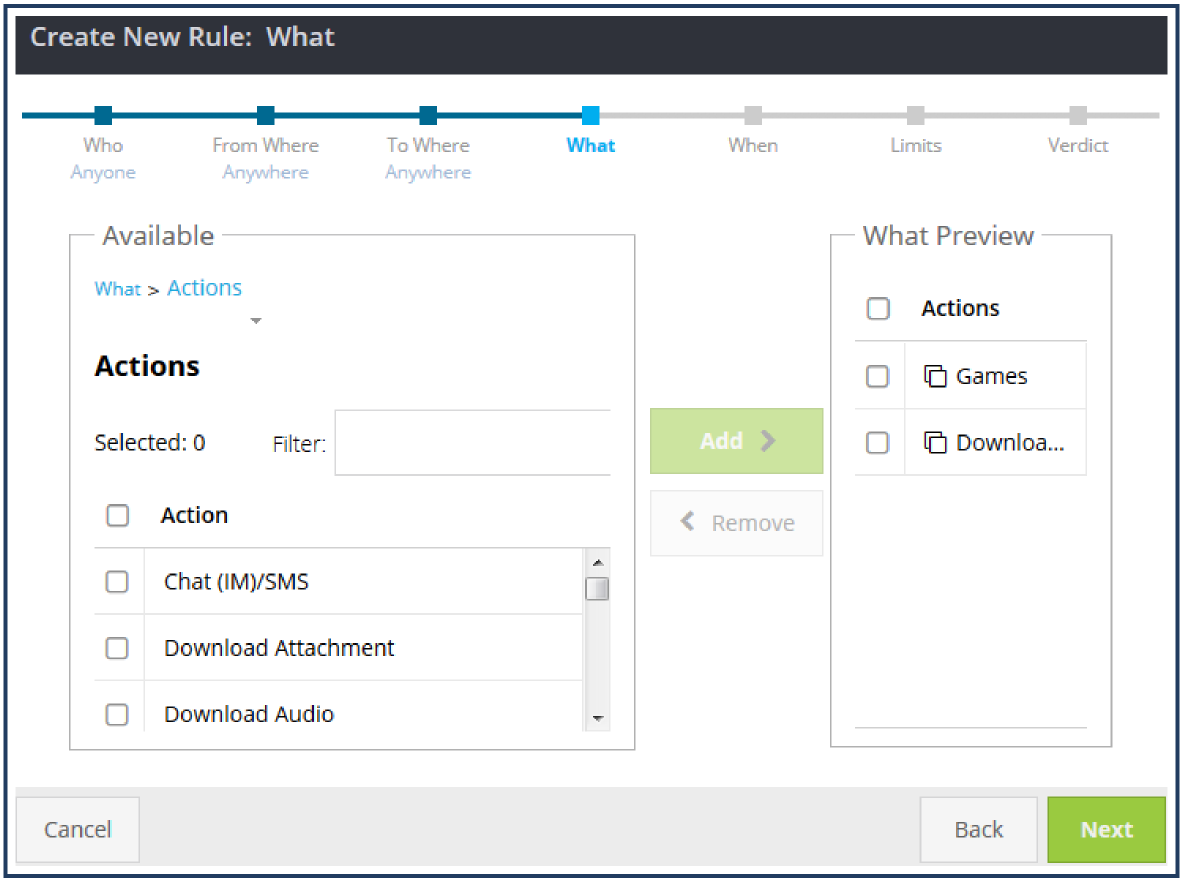
9. To initiate this policy, click **Activate**. If you are experimenting with the editor, you can select the row and click **Delete** or **Disable** (which retains the rule for future editing).

Action-Based

As mentioned in the previous example, the policy editor also allows you to define policy based on available actions or attributes *within* applications.

Example Use Case—Rather than trying to maintain per-application policy, you want to outright block all game playing or video downloading regardless of the requested application.

1. On the **From Where** page, do not select any web applications.
2. On the **What** page, the editor displays all of the available actions selectable for policy.



To continue with the use case, you select **Download Video** and **Games** and **Add** them to the policy.

3. Click **Next** to continue with the rule.
4. As demonstrated in the previous section, you can **Activate** the policy or remove/disable the test rule.

Combine Policy Elements

The above examples demonstrated the capabilities of web application policies afforded by the CASB data feed. Your network security and acceptable web use policies will likely require a more robust set of rules. The examples demonstrated the ability to define policy based on specific apps or actions by any app. Along with the other editor options, combining these two elements allows you to define the exact policy required to maximize your employee productivity while retaining network security and integrity.

Re-examining the policy, the following is an example rule that constructs several elements to allow streaming during lunch hours but the employees receive a coach notice.

- **From Where**: **TV/Video Streams**.
- **What**: **Play Audio**, **Play Video**.
- **Schedule**: **11:30** to **13:00**.
- **Verdict**: **Coach** (employees receive notice that their activity is logged).

View CASB 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 **Service** 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**

SSL Policy

Enable SSL interception and define policy.

About Scanning Encrypted Traffic

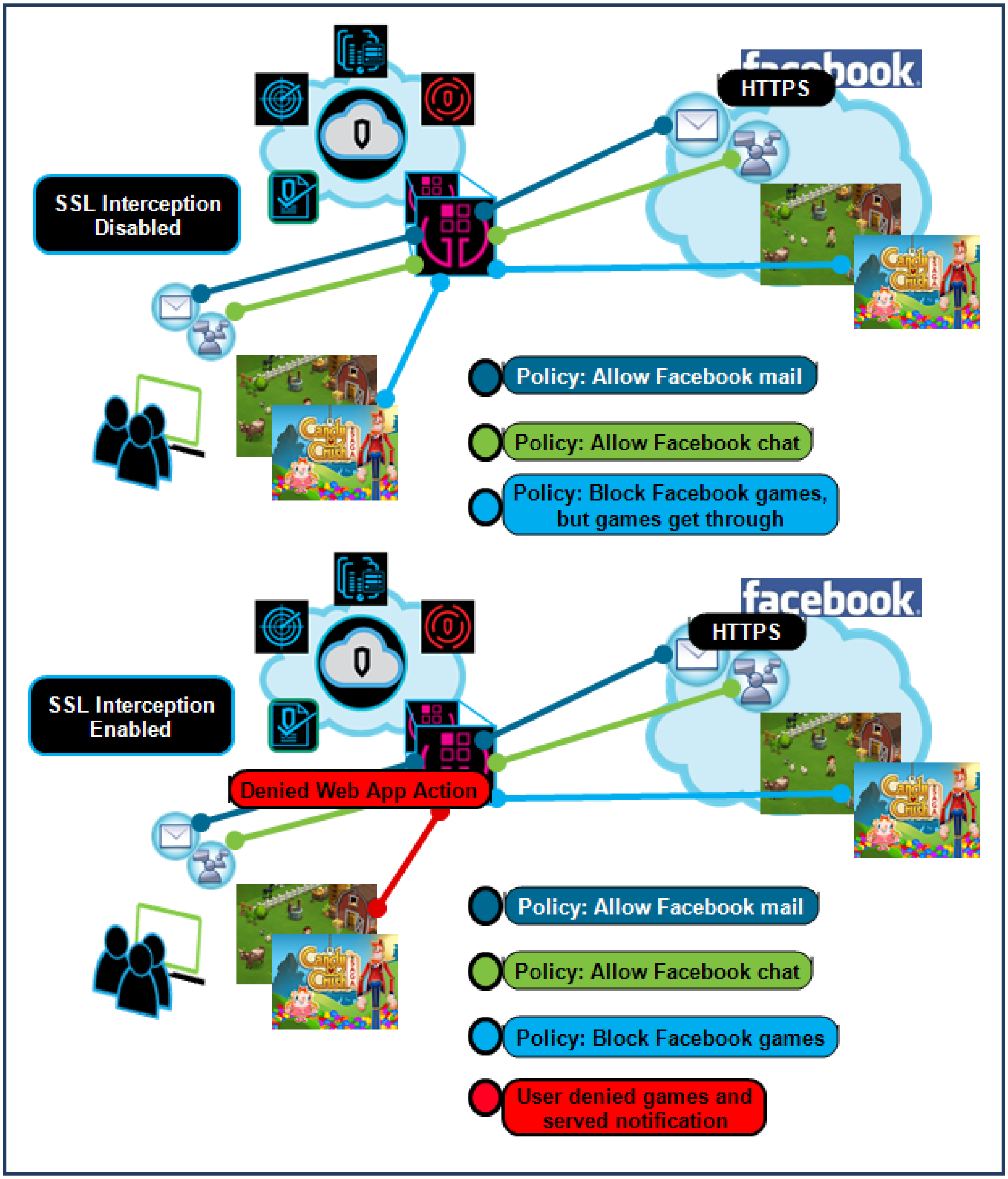
By default the Symantec Web Security Service does not intercept inbound HTTPS traffic from destination web locations and applications. With the default configuration, the Web Security Service applies content filtering policy to the furthest extent possible; however, it cannot apply policies to transactions that require deeper inspection, such as web application controls or malware scanning. Enabling SSL interception allows the Web Security Service 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 Web Security Service does not intercept HTTPS traffic categorized as **Brokerage/Trading**, **Financial Services**, and **Health**, because this content usually involves private, sensitive personal account information.

> **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 66.

Content Filtering Use Case

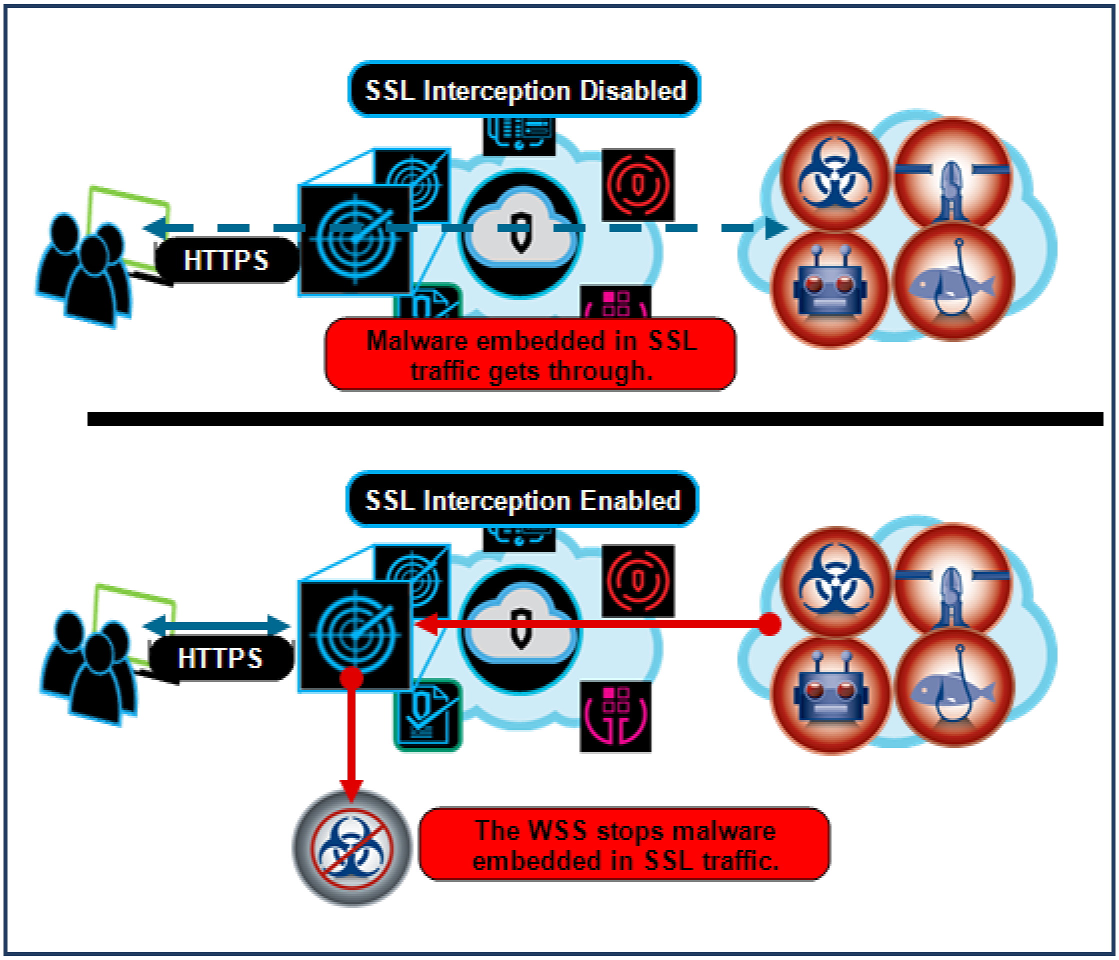
Some users configure their Facebook accounts for secure connections (**https://www.facebook.com/...**). With SSL interception enabled, the Web Security Service intercepts the inbound SSL connections and applies a policy check, such as **Block Games**.


SSL Interception Disabled
facebook
HTTPS
Policy: Allow Facebook mail
Policy: Allow Facebook chat
Policy: Block Facebook games, but games get through
SSL Interception Enabled
Denied Web App Action
facebook
HTTPS
Policy: Allow Facebook mail
Policy: Allow Facebook chat
Policy: Block Facebook games
User denied games and served notification

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 Web Security Service provides malware scanning by default.


SSL Interception Disabled
HTTPS
Malware embedded in SSL traffic gets through.
SSL Interception Enabled
HTTPS
The WSS stops malware embedded in SSL traffic.

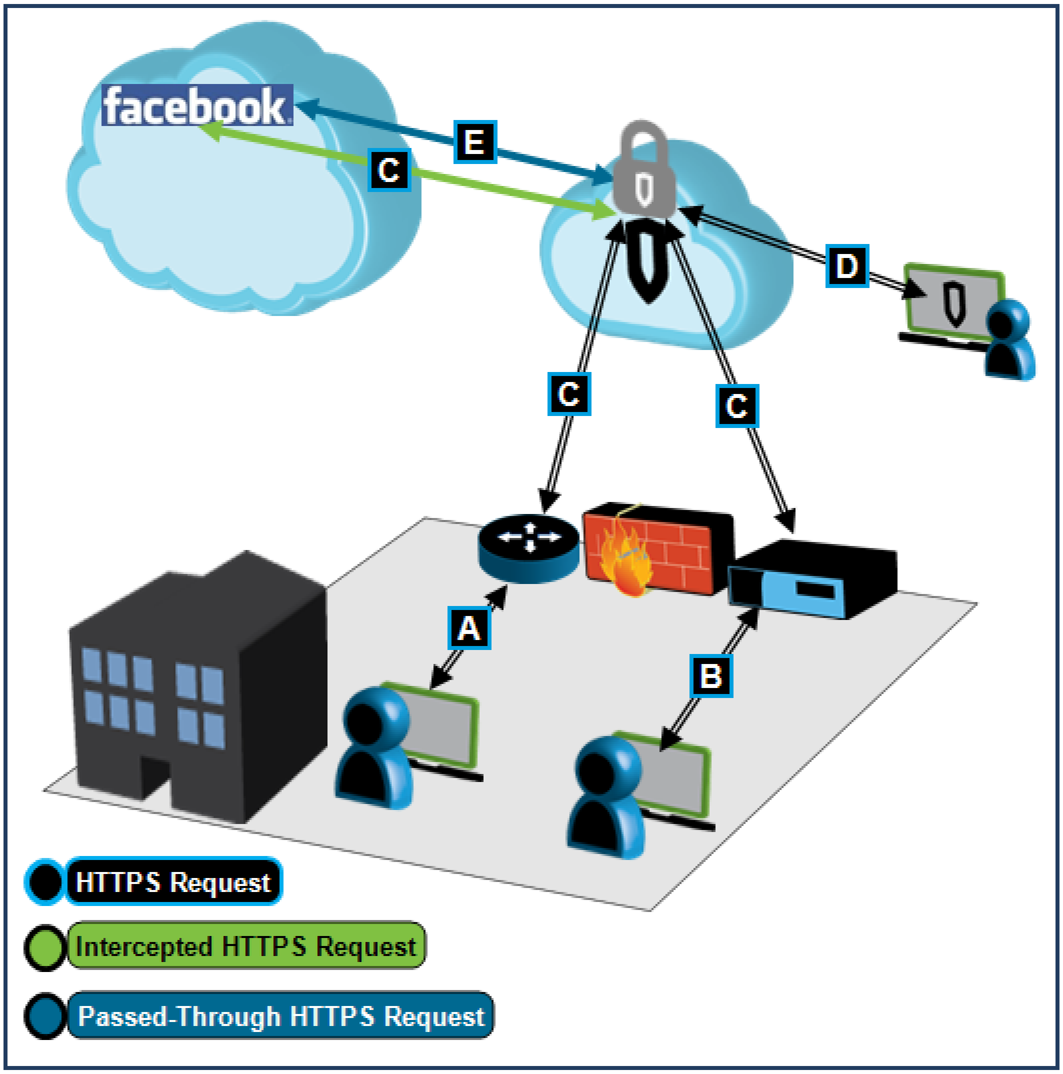
Without SSL intercept enabled, your network might still be at risk if the Web Security Service cannot intercept and inspect inbound SSL connections.

Granular SSL Policy

The Web Security Service allows you to selectively intercept HTTPS requests from specific network elements, such a 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 Web Security Service.



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

B—An employee connecting through the **Proxy Forwarding** Access 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 Web Security Service examines the returned HTTPS connection from Facebook.

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

E—The Web Security Service is configured to exempt all HTTPS traffic from Unified Agents from SSL interception.

> **Tip:** The default certificate uses the SHA-2 (specifically SHA-256) algorithm.

Next Step

- Enable? Proceed to "Examine Encrypted (HTTPS) Traffic" on page 83.
- 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" on page 88.

Examine Encrypted (HTTPS) Traffic

By default the Symantec Web Security Service does not intercept SSL connections. Enabling SSL interception allows the Web Security Service to terminate these connections, examine the contents, and perform policy checks.

Furthermore, the Web Security Service allows you to determine when the service intercepts SSL traffic. Specifically, you can specify sources and destinations that are exempt from SSL Interception when the feature is enabled. The policy is granular. 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.

About the Root Certificate Recommendation

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

> **Tip:** The default certificate uses the SHA-2 (specifically SHA-256) algorithm.

Want to learn more?

- "About Scanning Encrypted Traffic" on page 79
- "Install Encrypted Traffic Certificates" on page 88

Procedure

Step 1—Download the SSL Root Certificate.

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 Web Security Service. To prevent this security prompt, download the certificate and propagate it to all client browsers.

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

The Web Security Service Solutions WebGuide describes how to install certificates on all supported browsers. The following procedure is for Internet Explorer.

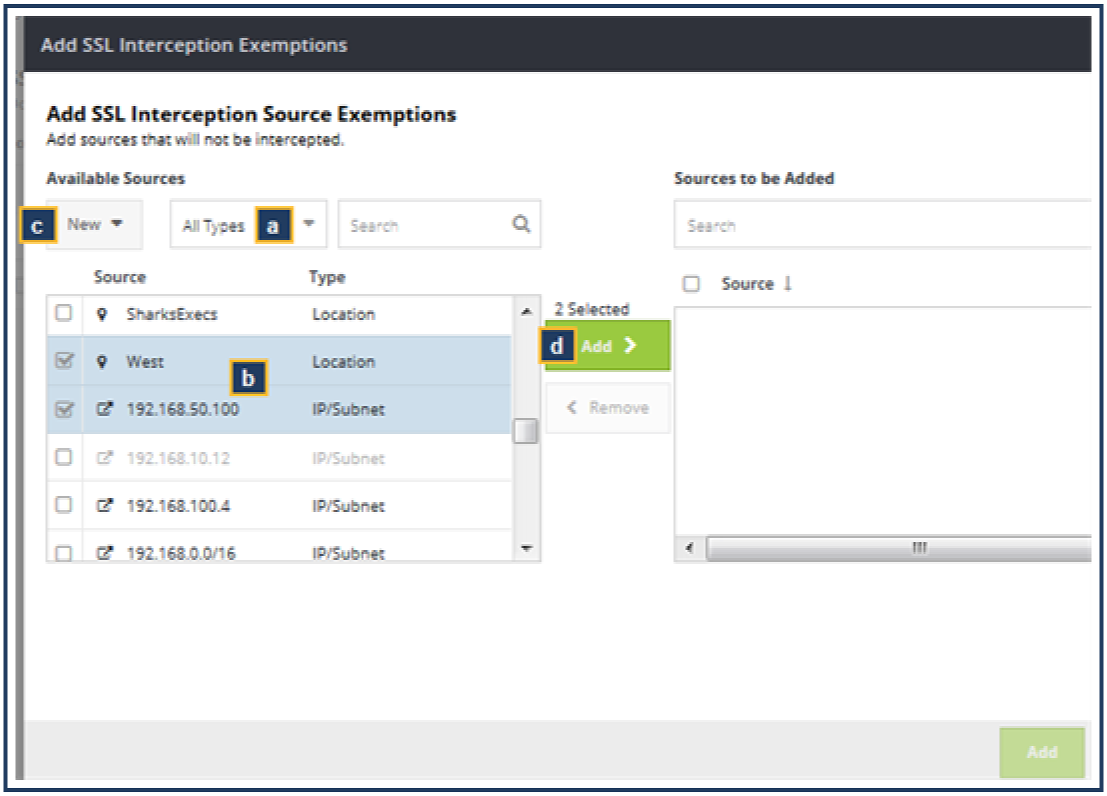
1. In the browser:
   a. Navigate to where you downloaded the file.
   b. Right-click the file, and select **Install Certificate**.
   c. You might be prompted for admin credentials and/or a confirmation prompt.
2. On the first wizard screen, click **Next**.
3. On the Certificate Store screen:
   a. 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**.

Step 3—(Optional) Exempt a source element

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.

- Detected authentication elements (**User**, **User Group**)—As provided by the authentication method (Auth Connector/SAML).
- **IP/Subnet**—Select from previously entered IP addresses/subnets that were defined in **Solutions** mode **> Overview > Object Library > Global Objects**.
- **Locations**—Exempt entire locations defined that are defined in **Service** mode **> Network > Locations**.
- **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.
- Lists (**User**, **User Group**, **Location**, **IP/Subnet**)—These are previously defined object lists. To create a list to use specifically for this SSL policy, navigate to **Solutions** mode **> Overview > Object Library > User Defined Objects**.

1. In the **SSL Interception Exemptions** area, click **Add**. Show screen...



Add SSL Interception Exemptions

Add SSL Interception Source Exemptions

Add sources that will not be intercepted.

Available Sources

	Source	Type
☐	SharksExecs	Location
☑	West	Location
☑	192.168.50.100	IP/Subnet
☐	192.168.10.12	IP/Subnet
☐	192.168.100.4	IP/Subnet
☐	192.168.0.0/16	IP/Subnet

2 Selected

Sources to be Added

   a. By default, the service displays all currently available elements. From the **Available Sources** drop-down list, select an element to filter the view.

   b. Select one or more objects to exempt.

   c. (Optional)—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.

   d. Click **Add**.

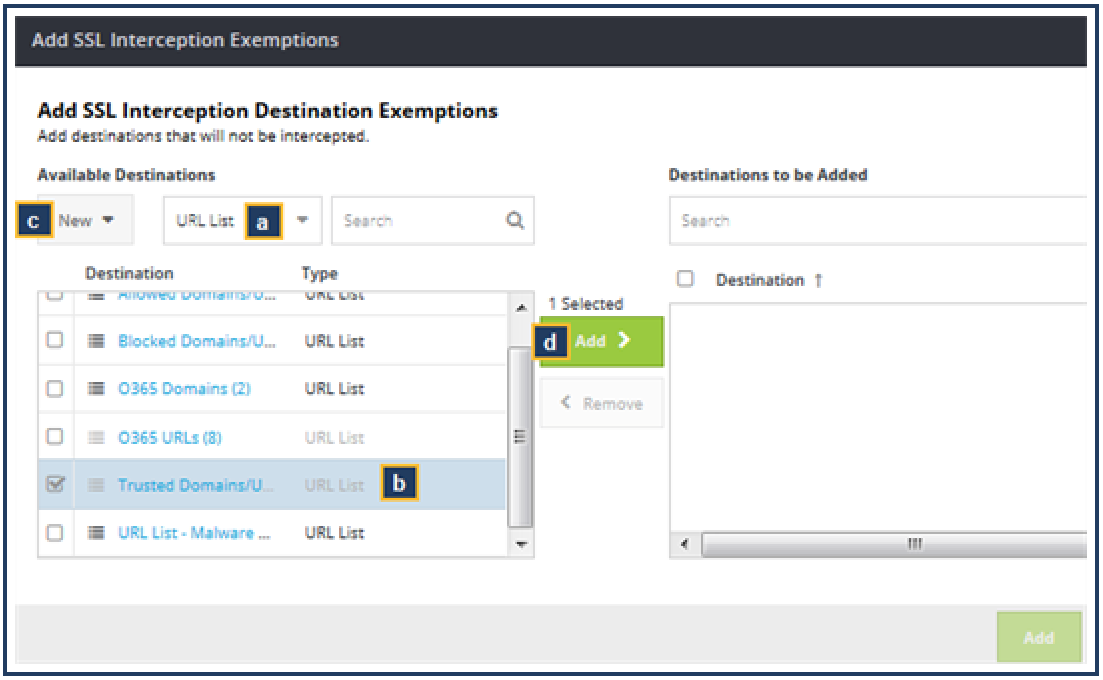
2. Click **Add**.

Step 4—(Optional) Exempt a destination element.

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.

- **Category**—Exempt web traffic that belongs to specific categories.
- **URL** and **IP/Subnet**—Exempt specific URLs or IP addresses. Select from previously entered domains that were defined in **Solutions** mode **> Overview > Object Library > Global Objects**.
- Lists (**Category List**, **URL List**, **IP/Subnet List**)—These are previously defined object lists. To create a list to use specifically for this SSL policy, navigate to **Solutions** mode **> Overview > Object Library > User Defined Objects**.

1. In the **SSL Interception Exemption/Destinations** area, click **Add**. Show screen...



Add SSL Interception Exemptions

Add SSL Interception Destination Exemptions

Add destinations that will not be intercepted.

Available Destinations

	Destination	Type
□	Allowed Domains/U...	URL List
□	Blocked Domains/U...	URL List
□	O365 Domains (2)	URL List
□	O365 URLs (8)	URL List
☑	Trusted Domains/U...	URL List
□	URL List - Malware ...	URL List

1 Selected

Destinations to be Added

   a. By default, the service displays all currently available elements. From the **Available Destinations** drop-down list, select an element to filter the view.

   b. Select one or more objects to exempt.

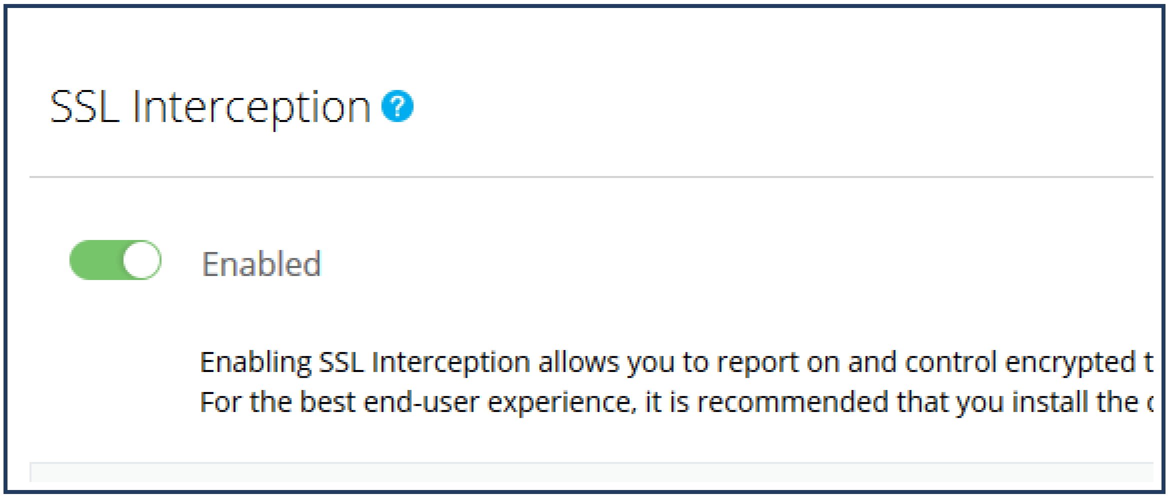
   c. (Optional)—The **New** drop-down list allows you to create a new object and add it to the policy from this dialog. This might be helpful if you are immediately troubleshooting from a destination that is not currently part of a custom list.

   d. Click **Add**.

2. Click **Add**.

Step 5—Activate SSL Interception

After defining the exemption policies, enable SSL interception.



SSL Interception

Enabled

Enabling SSL Interception allows you to report on and control encrypted t
For the best end-user experience, it is recommended that you install the c

1. On the **Network > SSL Interception** page, select **Enable SSL Interception**.

2. Click **Activate**; the Web Security Service now intercepts SSL traffic per the defined policy.

Warning: Enabling SSL on the Web Security Service might introduced unintended results for some websites. If your clients experience dropped connections, consult the information in "Troubleshoot Dropped SSL Connections" on page 95.

Install Encrypted Traffic Certificates

While root certificates a *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 Web Security Service 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.

Obtain Certificate and Propagate

Step 1—Download the SSL Root Certificate.

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 Web Security Service. To prevent this security prompt, download the certificate and propagate it to all client browsers.

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

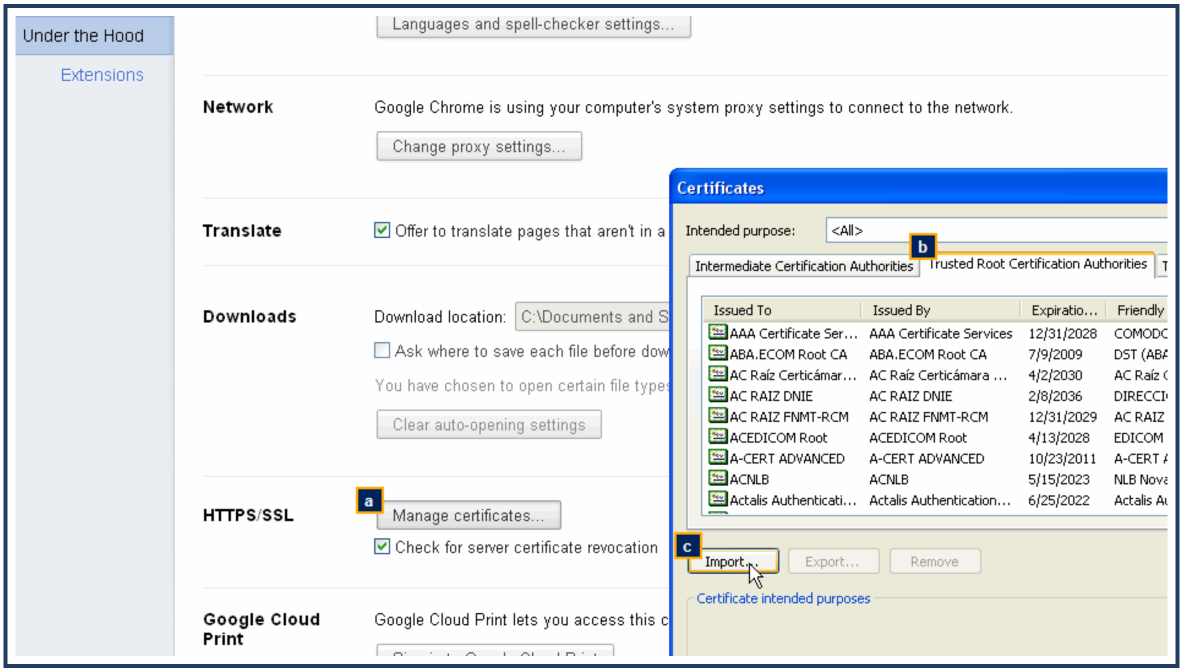
- "About Scanning Encrypted Traffic" on page 79
- "Examine Encrypted (HTTPS) Traffic" on page 83

Install SSL Root Certificate for Chrome Browsers

Enabling SSL intercept on the Symantec Web Security Service requires you to also install an SSL root certificate, downloadable from the service portal, on each employee client browser. If you do not perform this procedure, employees receive certificate error pop-up dialogs for each SSL connection attempt.

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.


Under the Hood
Extensions
Languages and spell-checker settings...
Network
Change proxy settings...
Translate
Downloads
Clear auto-opening settings
HTTPS/SSL
a
Manage certificates...
Google Cloud Print
Certificates
b
Intermediate Certification Authorities
Trusted Root Certification Authorities
c
Import...
Export...
Remove
Certificate intended purposes

Google Chrome is using your computer's system proxy settings to connect to the network.

☑ Offer to translate pages that aren't in a

Download location: C:\Documents and S

☐ Ask where to save each file before dow

You have chosen to open certain file types

☑ Check for server certificate revocation

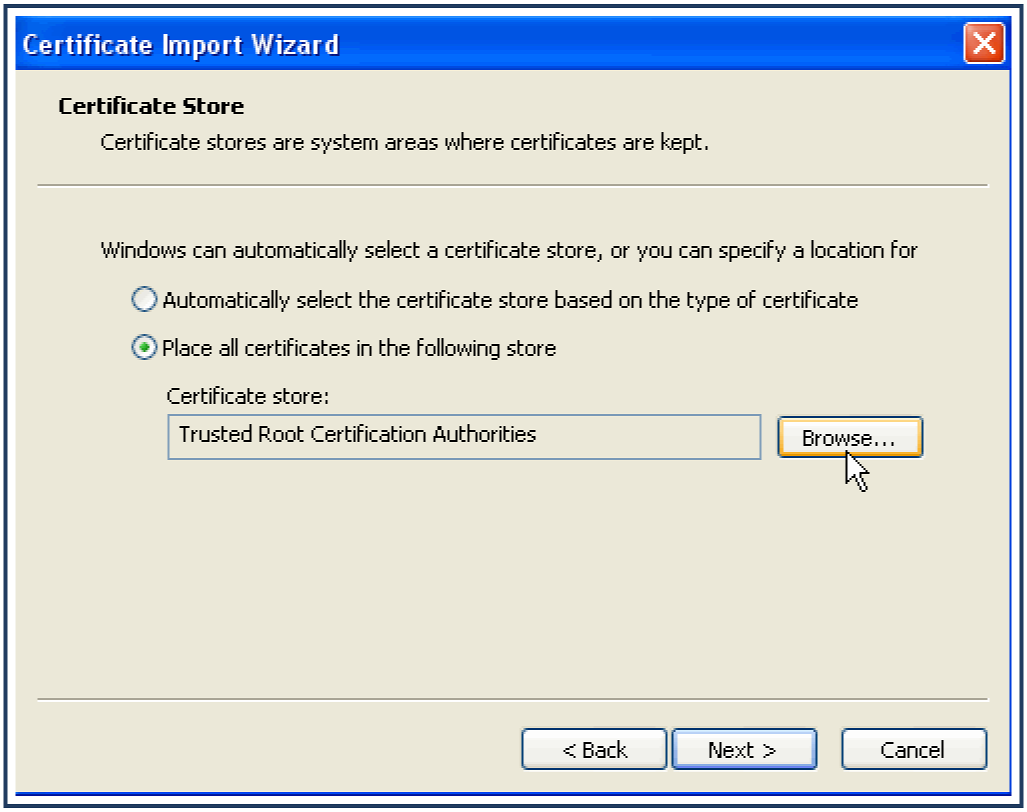
Google Cloud Print lets you access this c

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly
AAA Certificate Ser...	AAA Certificate Services	12/31/2028	COMODC
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009	DST (ABA
AC Raíz Certicámar...	AC Raíz Certicámara ...	4/2/2030	AC Raíz (
AC RAIZ DNIE	AC RAIZ DNIE	2/8/2036	DIRECCI
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	12/31/2029	AC RAIZ
ACEDICOM Root	ACEDICOM Root	4/13/2028	EDICOM
A-CERT ADVANCED	A-CERT ADVANCED	10/23/2011	A-CERT A
ACNLB	ACNLB	5/15/2023	NLB Nova
Actalis Authenticati...	Actalis Authentication...	6/25/2022	Actalis Au

   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.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

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**.

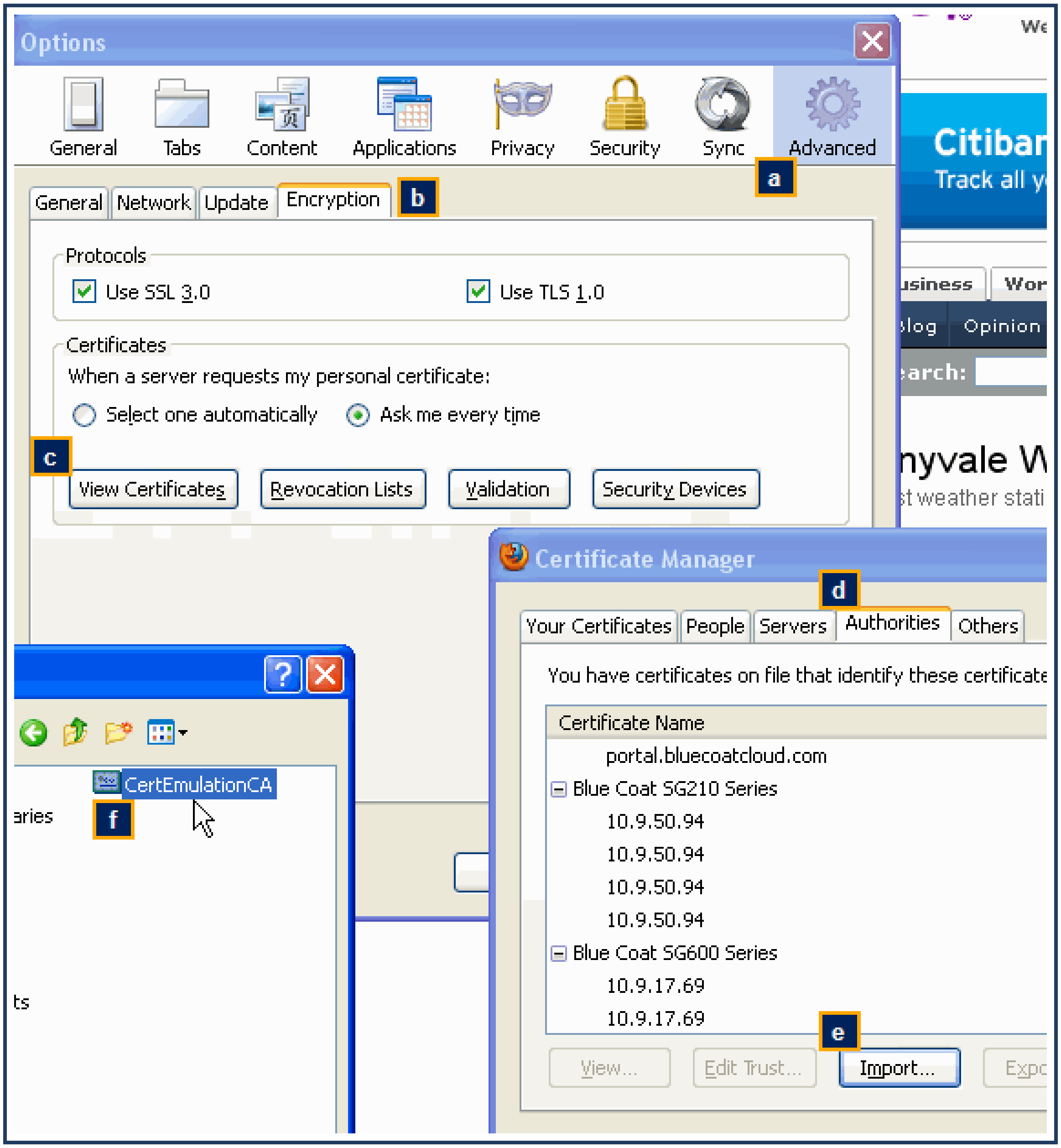
Return to "Examine Encrypted (HTTPS) Traffic" on page 83.

Install SSL Root Certificate for Mozilla Firefox Browsers

Enabling SSL intercept on the Symantec Web Security Service requires you to also install an SSL root certificate, downloadable from the service portal, on each employee client browser. If you do not perform this procedure, employees receive certificate error pop-up dialogs for each SSL connection attempt.

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.



☑ Use SSL 3.0 ☑ Use TLS 1.0

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

You have certificates on file that identify these certificate

Certificate Name
portal.bluecoatcloud.com
⊟ Blue Coat SG210 Series
10.9.50.94
10.9.50.94
10.9.50.94
10.9.50.94
⊟ Blue Coat SG600 Series
10.9.17.69
10.9.17.69

a. Select **Advanced**.

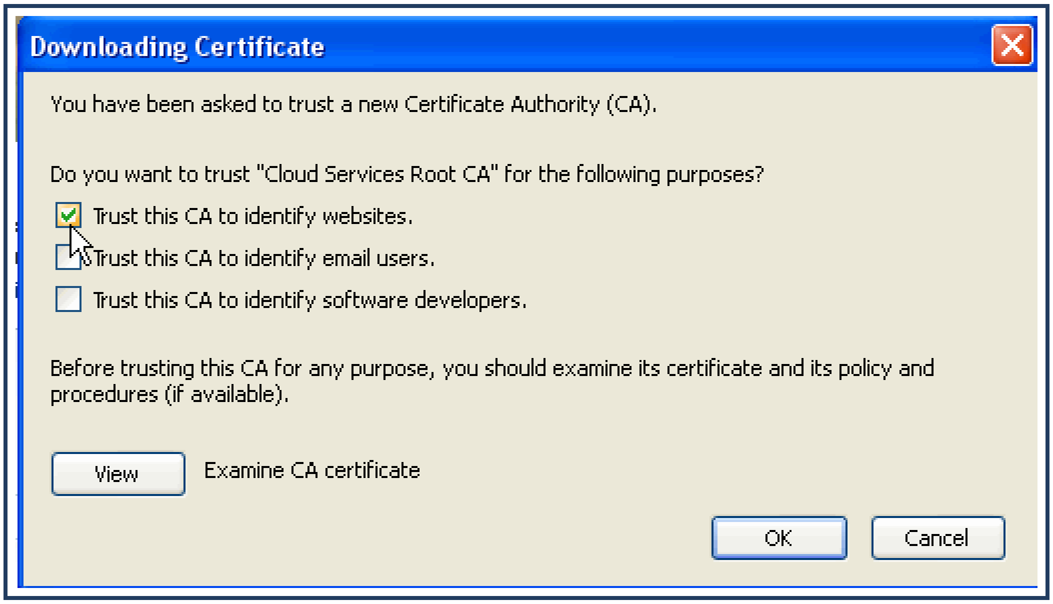
b. Select the **Encryption** tab.

   c. Click **View Certificates**. The browser displays the Certificate Manager dialog.

   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**.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Cloud Services Root CA" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

OK Cancel

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

Return to "Examine Encrypted (HTTPS) Traffic" on page 83.

Install SSL Root Certificate for Microsoft Internet Explorer Browsers

Enabling SSL intercept on the Symantec Web Security Service requires you to also install an SSL root certificate, downloadable from the service portal, on each employee client browser. If you do not perform this procedure, employees receive certificate error pop-up dialogs for each SSL connection attempt.

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**.

Return to "Examine Encrypted (HTTPS) Traffic" on page 83.

Install SSL Root Certificate for Safari Browsers

Enabling SSL intercept on the Symantec Web Security Service requires you to also install an SSL root certificate, downloadable from the service portal, on each employee client browser. If you do not perform this procedure, employees receive certificate error pop-up dialogs for each SSL connection attempt.

Perform the following steps for Apple Safari browsers. The procedures assume that you have downloaded the root certificate from your Web Security Service 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**.

Return to "Examine Encrypted (HTTPS) Traffic" on page 83.

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..

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 set captive portal surrogate type and refresh times.
- I want to set authentication policy based on location.
- I want to create custom lists of objects and network elements to use in multiple polices.
- 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

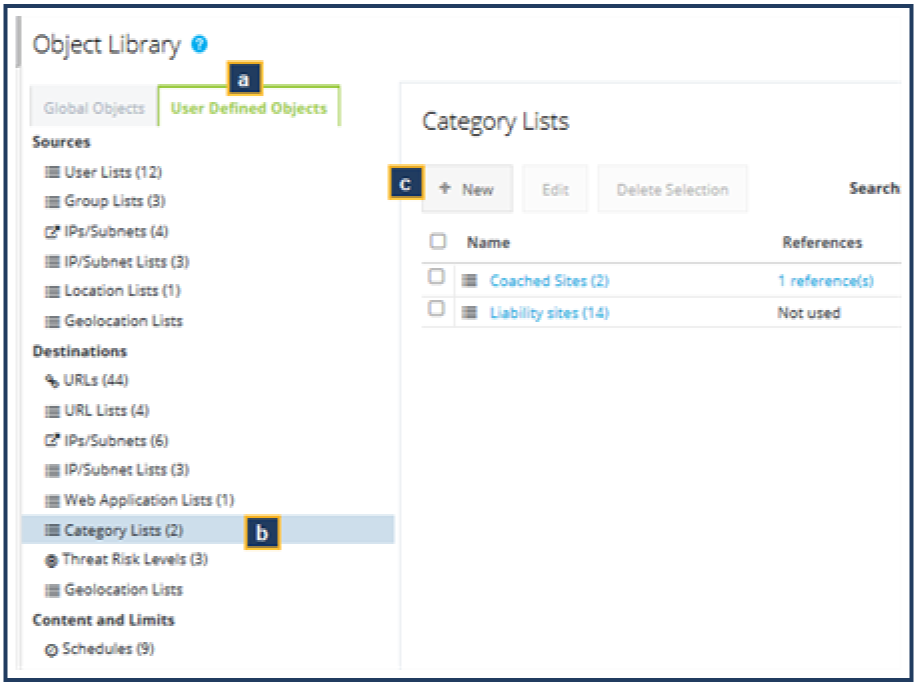
The Symantec Web Security Service Content Filtering Rules policy editor enables you to create or select network objects such as usernames, IP addresses, URLs, and categories. A more efficient method is to create objects that contain lists of related values and then select that object when creating policy.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



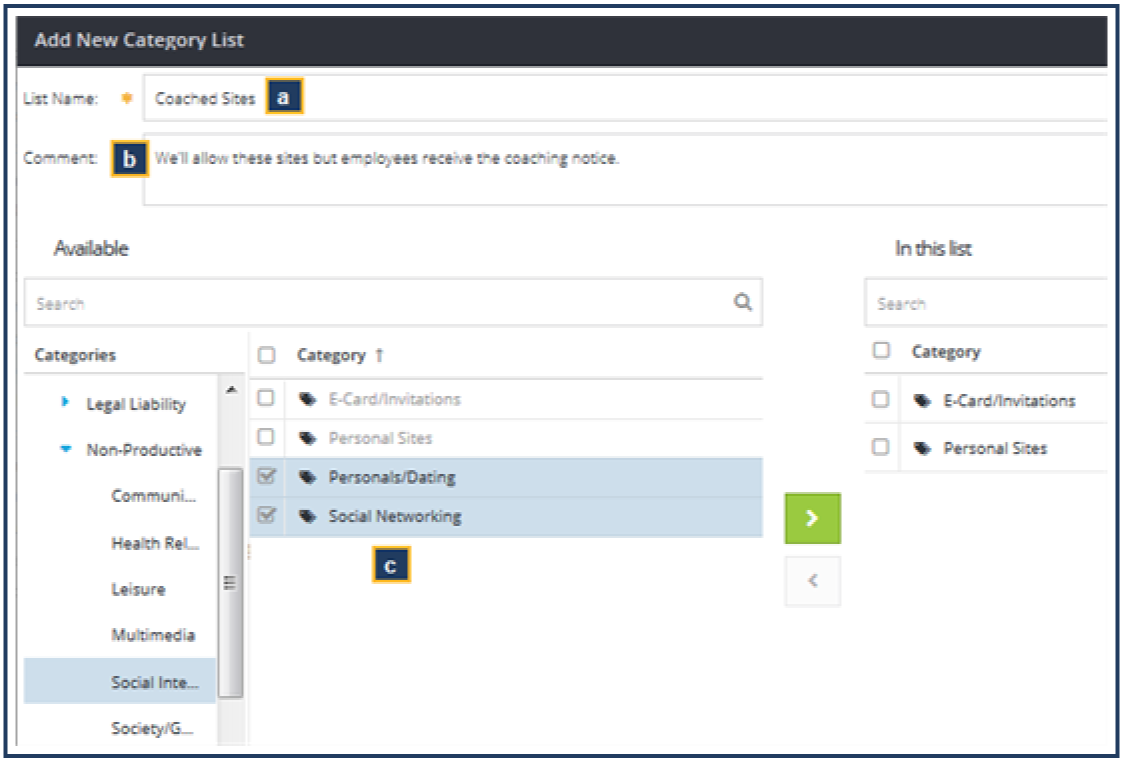
□	Name	References
□	Coached Sites (2)	1 reference(s)
□	Liability sites (14)	Not used

   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.



Add New Category List

List Name: * Coached Sites

Comment: We'll allow these sites but employees receive the coaching notice.

Available

□	Category ↑
□	E-Card/Invitations
□	Personal Sites
☑	Personals/Dating
☑	Social Networking

In this list

□	Category
□	E-Card/Invitations
□	Personal Sites

   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**.

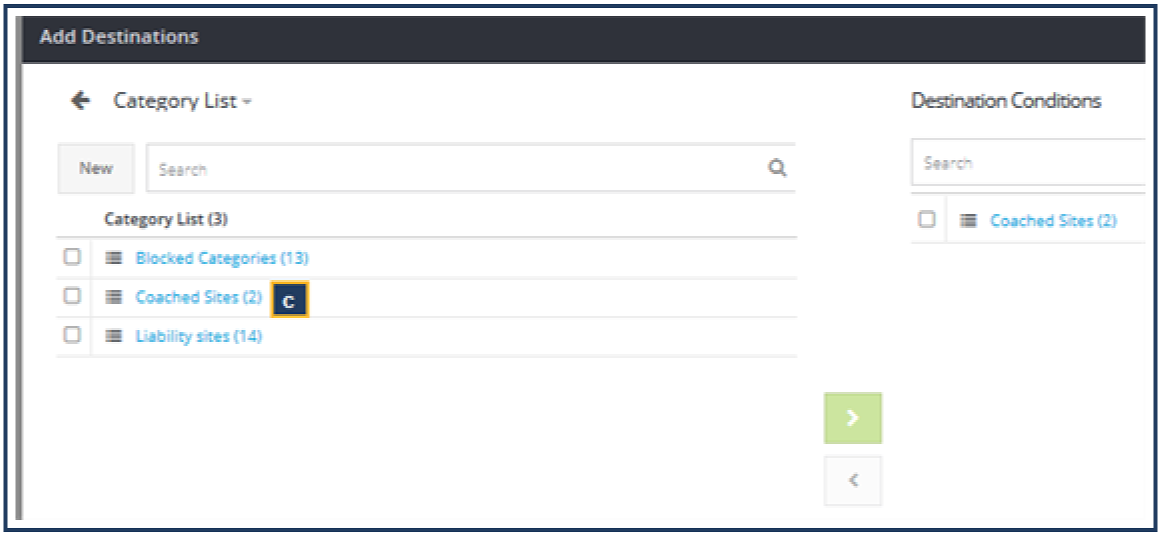
   f. An orange triangle next to the object indicates new objects are in **Pending** state and remain so until you click **Activate**.

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**.

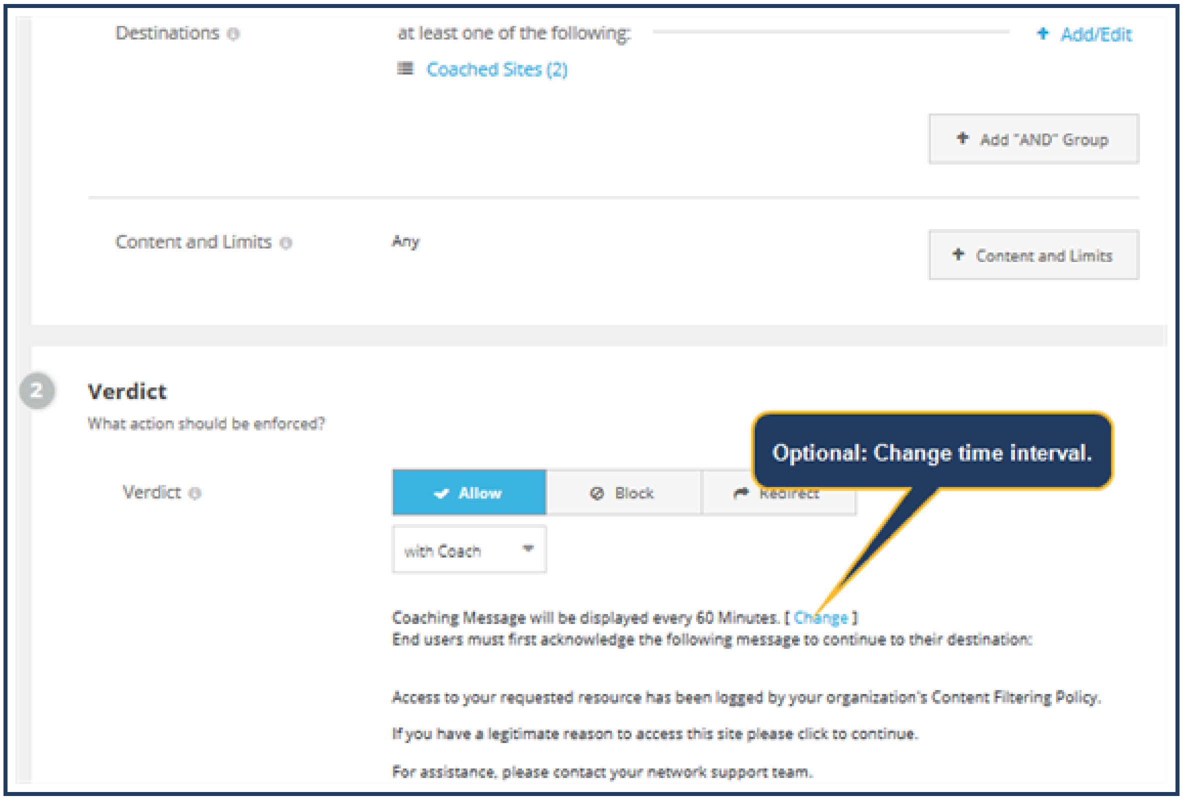
   b. Click the **Category Lists** item.



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**.



Optional: Change time interval.

Coaching Message will be displayed every 60 Minutes. [Change]
End users must first acknowledge the following message to continue to their destination:

Access to your requested resource has been logged by your organization's Content Filtering Policy.

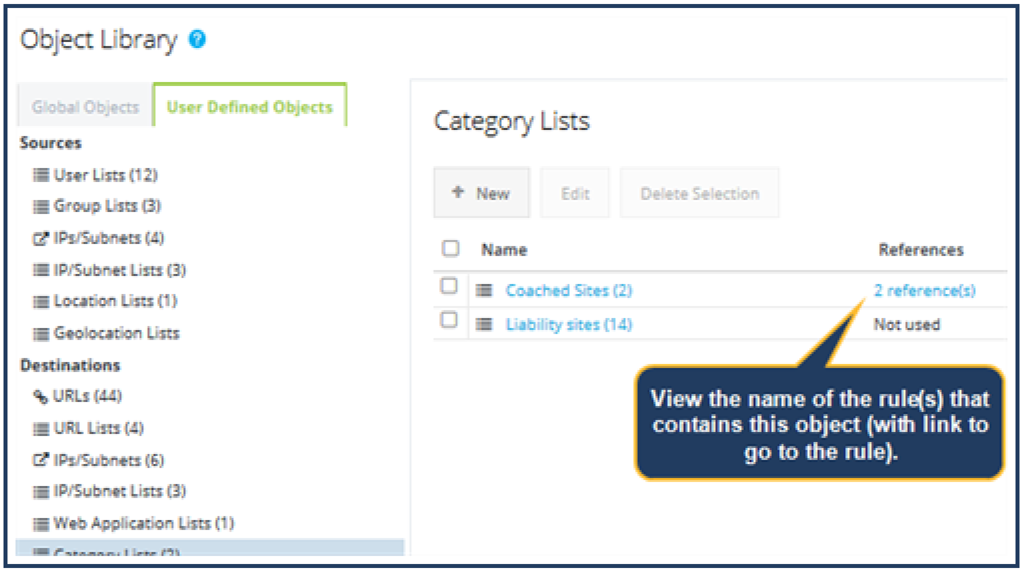
If you have a legitimate reason to access this site please click to continue.

For assistance, please contact your network support team.

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.



Object Library

Category Lists

☐	Name	References
☐	Coached Sites (2)	2 reference(s)
☐	Liability sites (14)	Not used

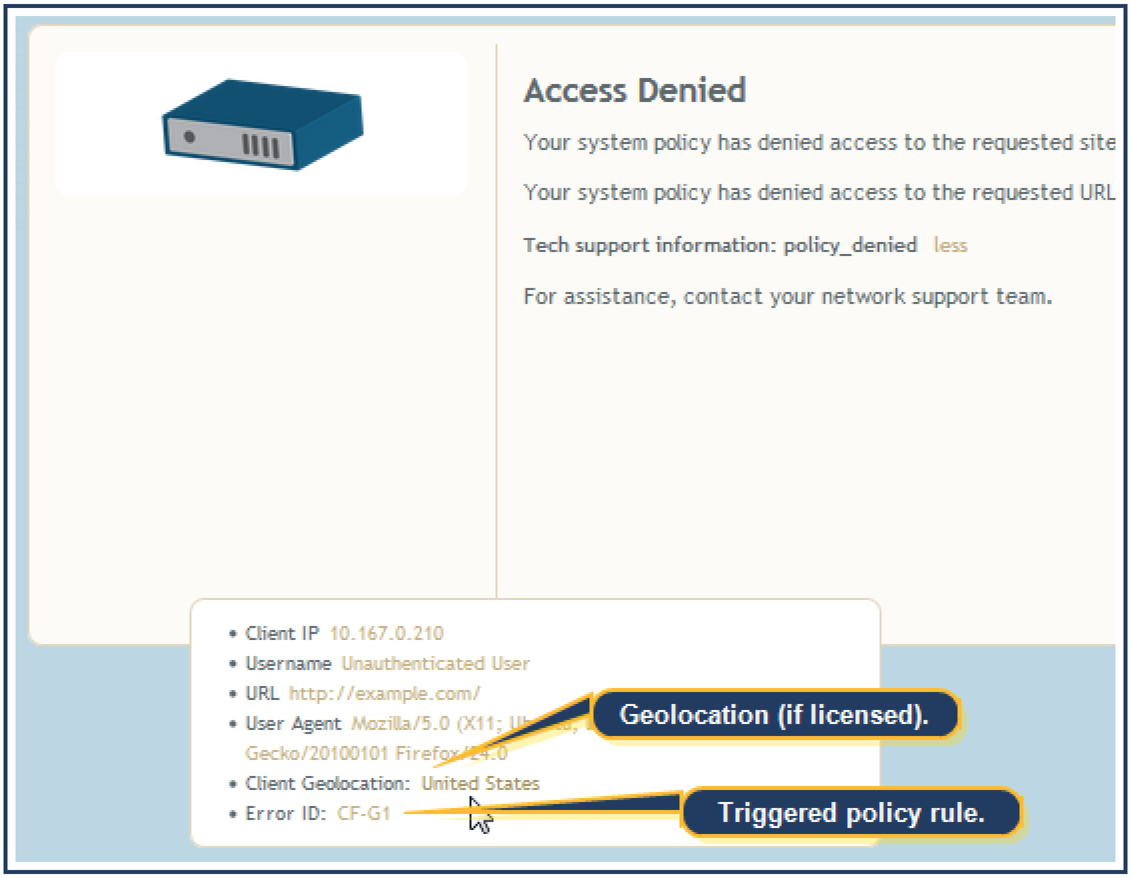
View the name of the rule(s) that contains this object (with link to go to the rule).

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 12.

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 Web Security Service 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).



Access Denied

Your system policy has denied access to the requested site

Your system policy has denied access to the requested URL

Tech support information: policy_denied less

For assistance, contact your network support team.

- Client IP 10.167.0.210
- Username Unauthenticated User
- URL http://example.com/
- User Agent Mozilla/5.0 (X11; [illegible] Gecko/20100101 Firefox/24.0
- Client Geolocation: United States
- Error ID: CF-G1

Geolocation (if licensed).

Triggered policy rule.

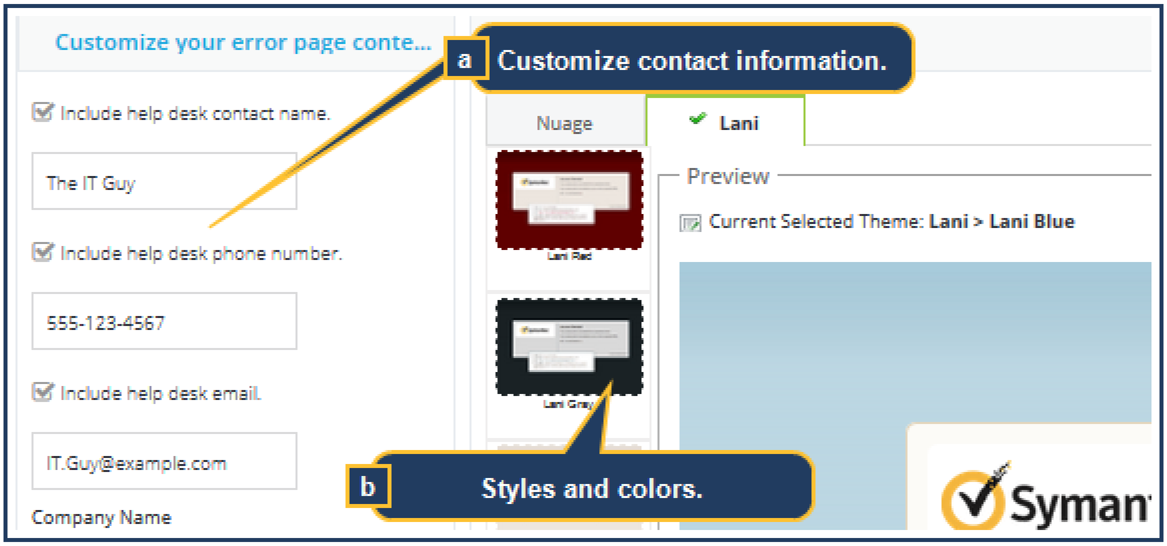
- The Web Security Service allows you to modify this page, including selecting a color scheme, adding contact information and changing the displayed logo and company name. For example, add your IT group email address so that users can contact IT to dispute a rating or ask a question about the policy.
- If your Web Security Service 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 12.
- 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 105.

Additionally, English, French (European), German, Italian, Japanese, and Spanish (European) language web browsers displays these pages in the respective languages.

This task requires Web Security Service portal Admin Role credentials.

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



Customize your error page conte...

a Customize contact information.

☑ Include help desk contact name.

The IT Guy

☑ Include help desk phone number.

555-123-4567

☑ Include help desk email.

IT.Guy@example.com

Company Name

Current Selected Theme: Lani > Lani Blue

b Styles and colors.

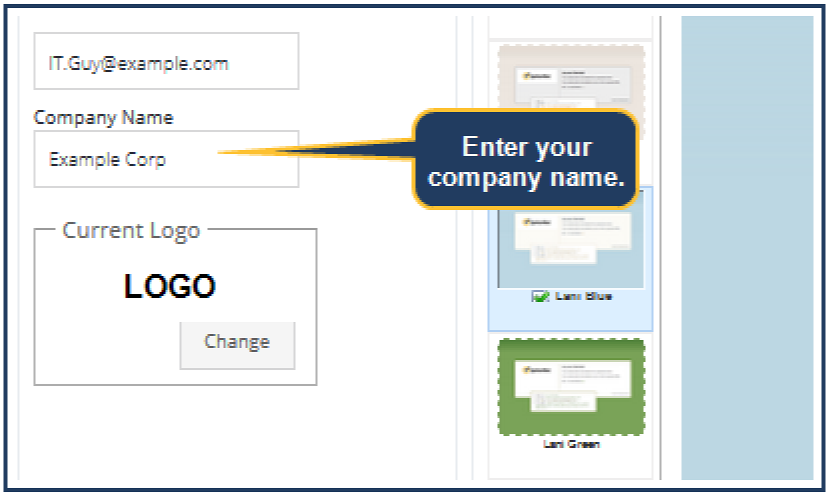
   a. Select which additional text options to include on the page. In addition to letter and numbers, only spaces and plus signs (+) are valid characters.

   b. Select the page style and color.

   c. Click **Save**.

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

> **Note:** If you enabled the Web Security Service after November 15th, 2013, this field automatically displays your registered company name.



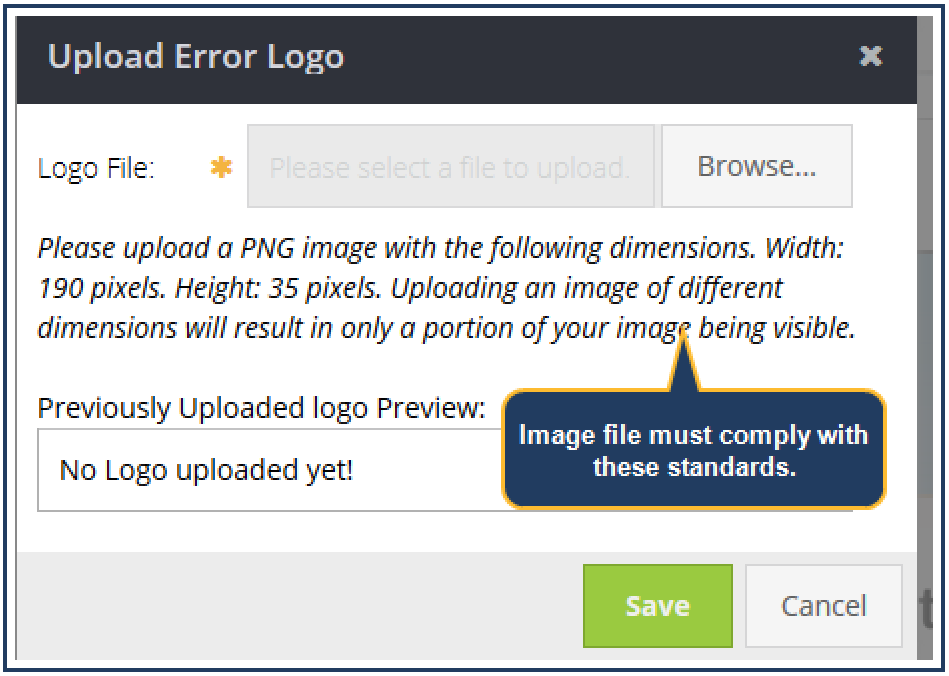
IT.Guy@example.com

Company Name

Example Corp

Enter your company name.

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 Web Security Service from a third-party service provider, their logo might display instead. The logo you add here overrides that configuration.


Upload Error Logo
Logo File:
Please select a file to upload.
Browse...
Previously Uploaded logo Preview:
Save
Cancel

Please upload a PNG image with the following dimensions. Width: 190 pixels. Height: 35 pixels. Uploading an image of different dimensions will result in only a portion of your image being visible.

No Logo uploaded yet!

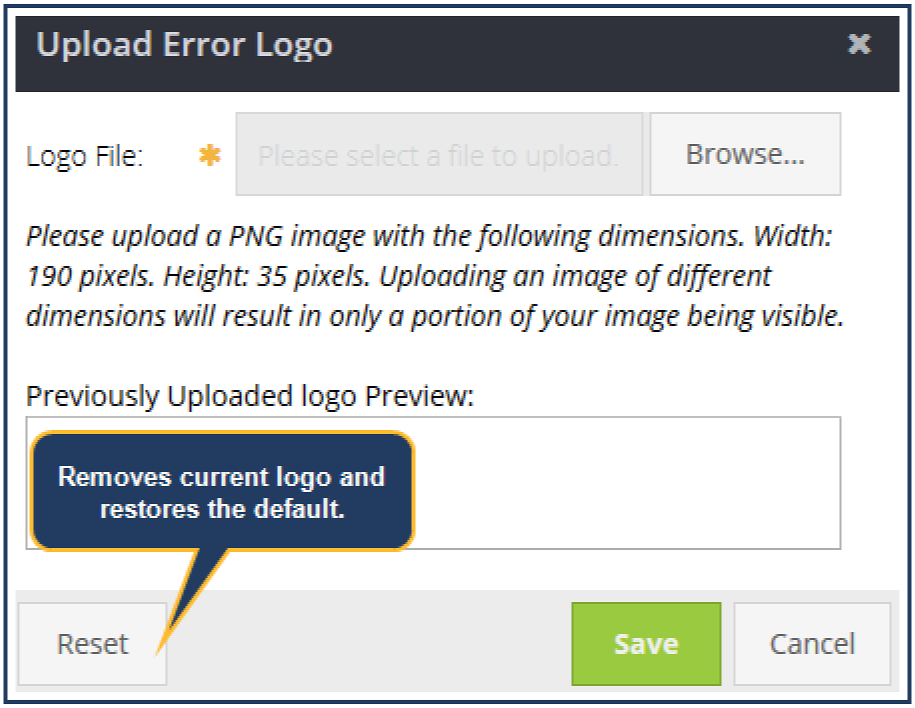
Image file must comply with these standards.

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**.


Upload Error Logo
Logo File:
Please select a file to upload.
Browse...
Previously Uploaded logo Preview:
Reset
Save
Cancel

Please upload a PNG image with the following dimensions. Width: 190 pixels. Height: 35 pixels. Uploading an image of different dimensions will result in only a portion of your image being visible.

Removes current logo and restores the default.

4. Click **Save**.

> **Note:** If the Web Security Service 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.

Customize the User Notification Template

As configured on the **Error Pages** tab (**Solutions** mode **> Notifications > Error Pages**), the Symantec Web Security Service 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.

Tips

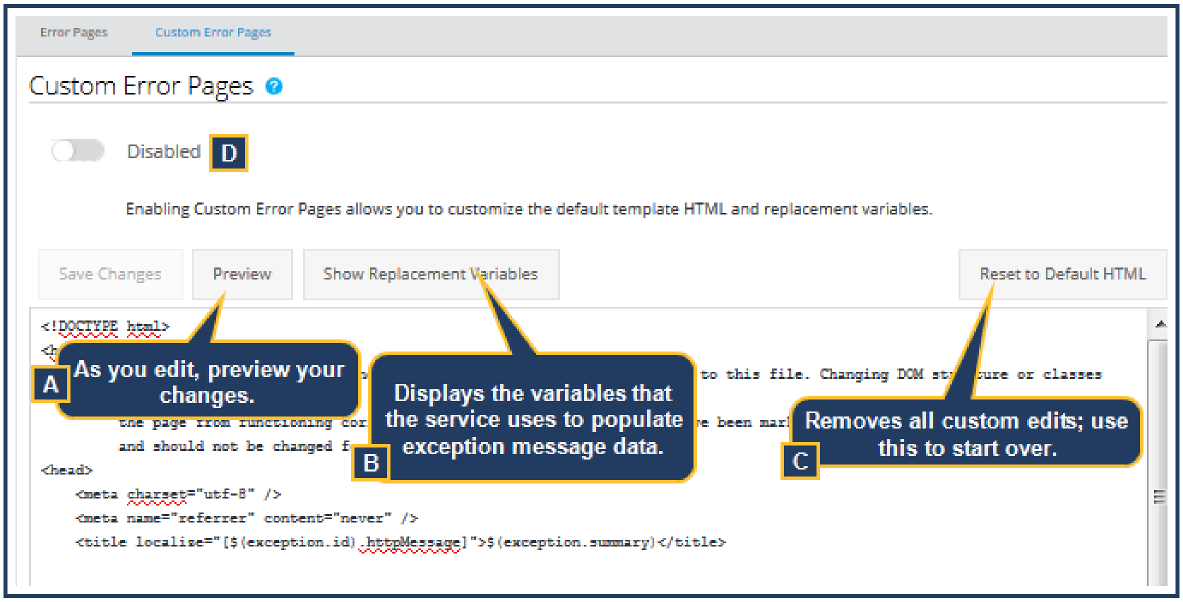
- Symantec considers customizing the notification template an advanced feature. As such, only admin-level Web Security Service users are able to modify the template contents.
- Symantec recommends considerable knowledge of HTML and CSS before performing edits beyond simple string replacements.

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.

The Editor

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

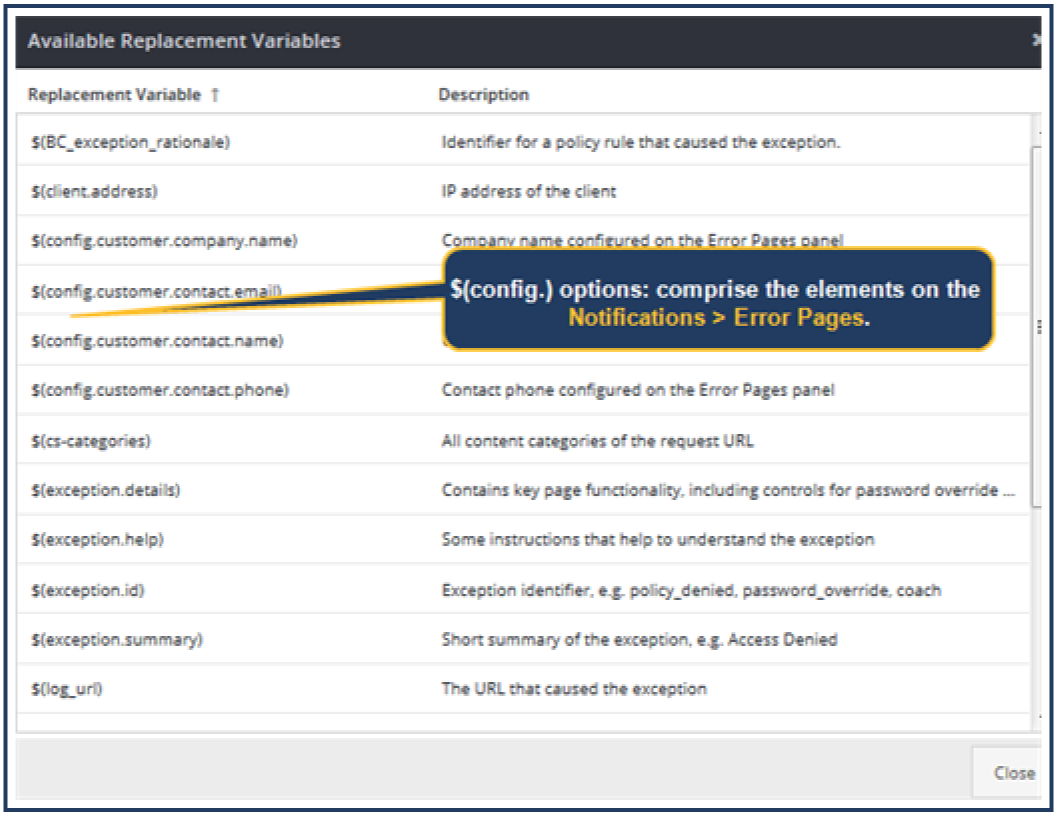

Error Pages
Custom Error Pages
Custom Error Pages
Disabled
D
Save Changes
Preview
Show Replacement Variables
Reset to Default HTML
A
As you edit, preview your changes.
B
Displays the variables that the service uses to populate exception message data.
C
Removes all custom edits; use this to start over.

Enabling Custom Error Pages allows you to customize the default template HTML and replacement variables.

```
<!DOCTYPE html>
<h
                                   to this file. Changing DOM st      ure or classes
        the page from functioning cor                    e been mar
        and should not be changed f
<head>
    <meta charset="utf-8" />
    <meta name="referrer" content="never" />
    <title localize="[$(exception.id).httpMessage]">$(exception.summary)</title>
```

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.



Replacement Variable ↑	Description
$(BC_exception_rationale)	Identifier for a policy rule that caused the exception.
$(client.address)	IP address of the client
$(config.customer.company.name)	Company name configured on the Error Pages panel
$(config.customer.contact.email)	
$(config.customer.contact.name)	
$(config.customer.contact.phone)	Contact phone configured on the Error Pages panel
$(cs-categories)	All content categories of the request URL
$(exception.details)	Contains key page functionality, including controls for password override ...
$(exception.help)	Some instructions that help to understand the exception
$(exception.id)	Exception identifier, e.g. policy_denied, password_override, coach
$(exception.summary)	Short summary of the exception, e.g. Access Denied
$(log_url)	The URL that caused the exception

$(config.) options: comprise the elements on the Notifications > Error Pages.

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.

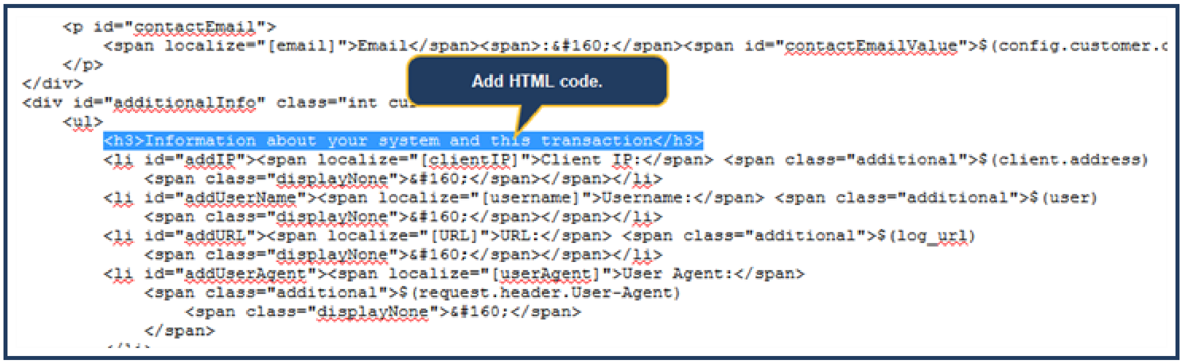
D—When you click **Enable** custom error pages, the system might override any custom edits to the **Notifications > Error Pages**. For example, if you add contact telephone number to the field on that page, but comment out the field in the **Custom Error Page** template, the service does not display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

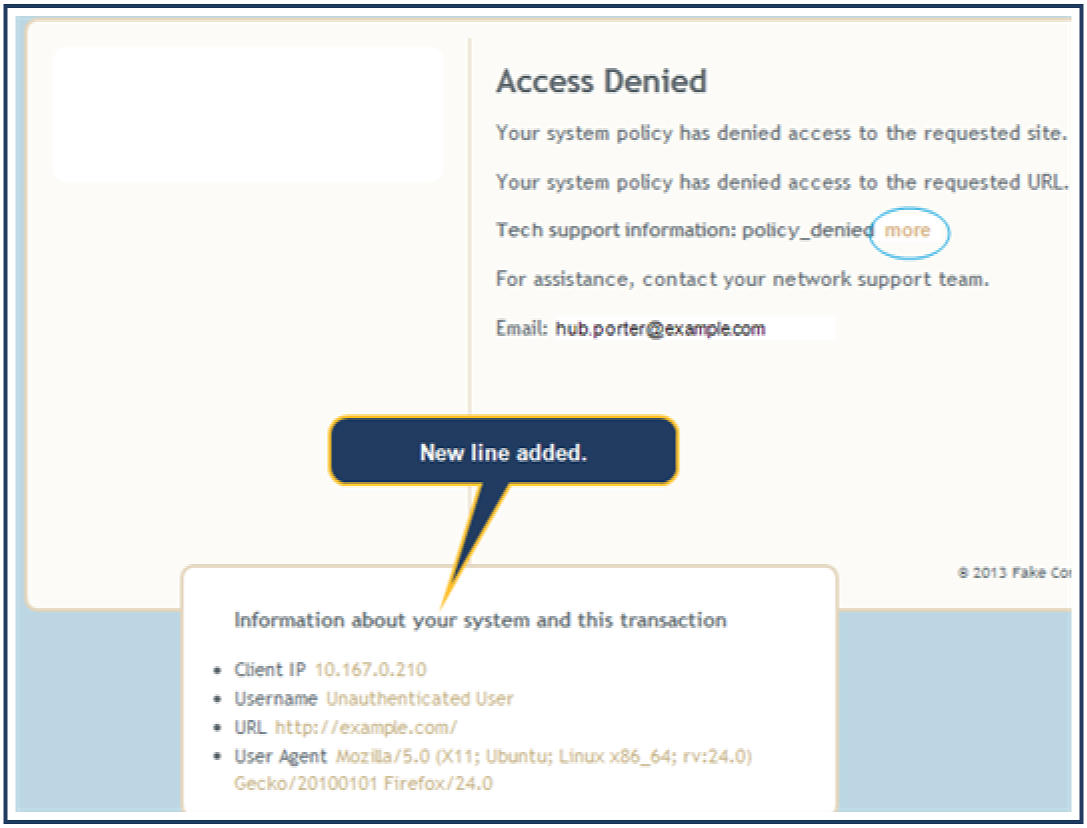
Supplement the notification with custom text. The following example adds a new line to **Tech support information** drop-down (accessed by clicking **more**).



Add HTML code.

```
    <p id="contactEmail">
        <span localize="[email]">Email</span><span>:&#160;</span><span id="contactEmailValue">$(config.customer.c
    </p>
</div>
<div id="additionalInfo" class="int cu
    <ul>
        <h3>Information about your system and this transaction</h3>
        <li id="addIP"><span localize="[clientIP]">Client IP:</span> <span class="additional">$(client.address)
            <span class="displayNone">&#160;</span></span></li>
        <li id="addUserName"><span localize="[username]">Username:</span> <span class="additional">$(user)
            <span class="displayNone">&#160;</span></span></li>
        <li id="addURL"><span localize="[URL]">URL:</span> <span class="additional">$(log_url)
            <span class="displayNone">&#160;</span></span></li>
        <li id="addUserAgent"><span localize="[userAgent]">User Agent:</span>
            <span class="additional">$(request.header.User-Agent)
                <span class="displayNone">&#160;</span>
            </span>
```

Click **Preview** to see how the service will display the page.



Access Denied

Your system policy has denied access to the requested site.

Your system policy has denied access to the requested URL.

Tech support information: policy_denied more

For assistance, contact your network support team.

Email: hub.porter@example.com

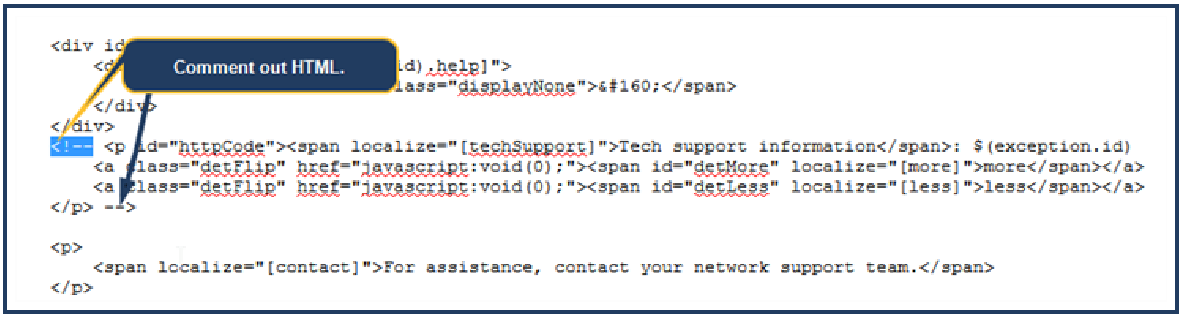
© 2013 Fake Co

Information about your system and this transaction

- Client IP 10.167.0.210
- Username Unauthenticated User
- URL http://example.com/
- User Agent Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:24.0) Gecko/20100101 Firefox/24.0

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 -->`**.



```
<div id
    <d                                      id).help]">
                                          lass="displayNone">&#160;</span>
    </div>
</div>
<!-- <p id="httpCode"><span localize="[techSupport]">Tech support information</span>: $(exception.id)
    <a class="detFlip" href="javascript:void(0);"><span id="detMore" localize="[more]">more</span></a>
    <a class="detFlip" href="javascript:void(0);"><span id="detLess" localize="[less]">less</span></a>
</p> -->

<p>
    <span localize="[contact]">For assistance, contact your network support team.</span>
</p>
```

IMPORTANT: Some span tag contain the `localize` attribute. Regardless of any customized text, this attribute instructs the Web Security Service 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.

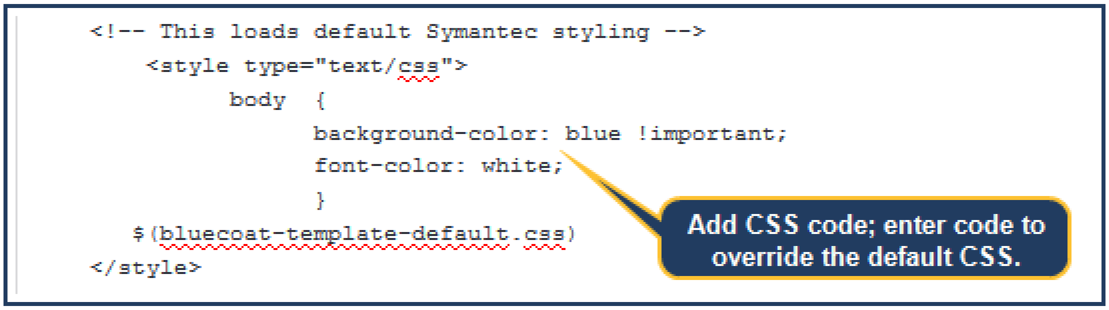
```
<p id="httpCode"><span localize="[techSupport]">Tech support information</span>: $(exception.id)
```

This line provides the custom text: Tech support information.

```
<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.



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

Add CSS code; enter code to override the default CSS.

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

Best Practices

- 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 encoded directly in the HTML.
    - The template can contain CSS stylesheets.
- The Web Security Service 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.

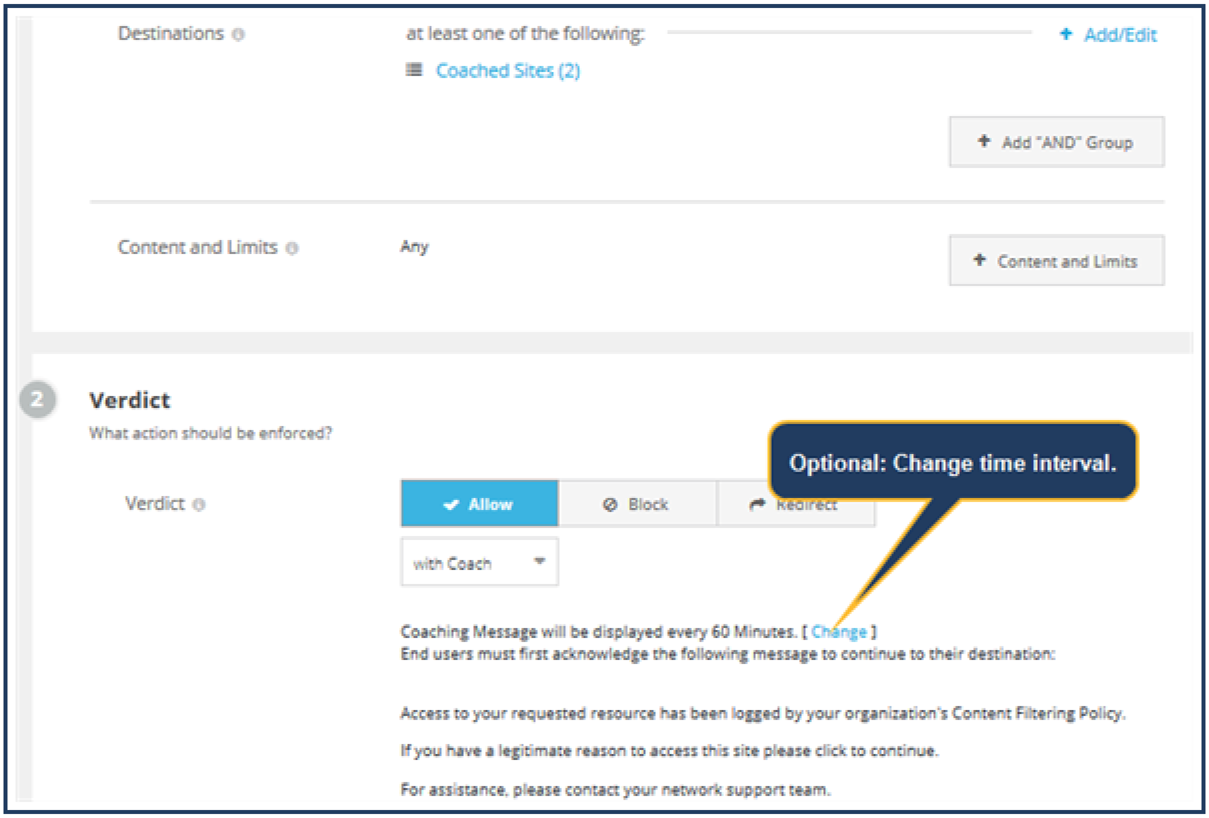
Provide Browsing Coaching to Users

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.



Optional: Change time interval.

Coaching Message will be displayed every 60 Minutes. [Change]
End users must first acknowledge the following message to continue to their destination:

Access to your requested resource has been logged by your organization's Content Filtering Policy.

If you have a legitimate reason to access this site please click to continue.

For assistance, please contact your network support team.

   a. Select **Allow** and select **with Coach**. The service displays the **Coaching Message** text. This text is what employees see.

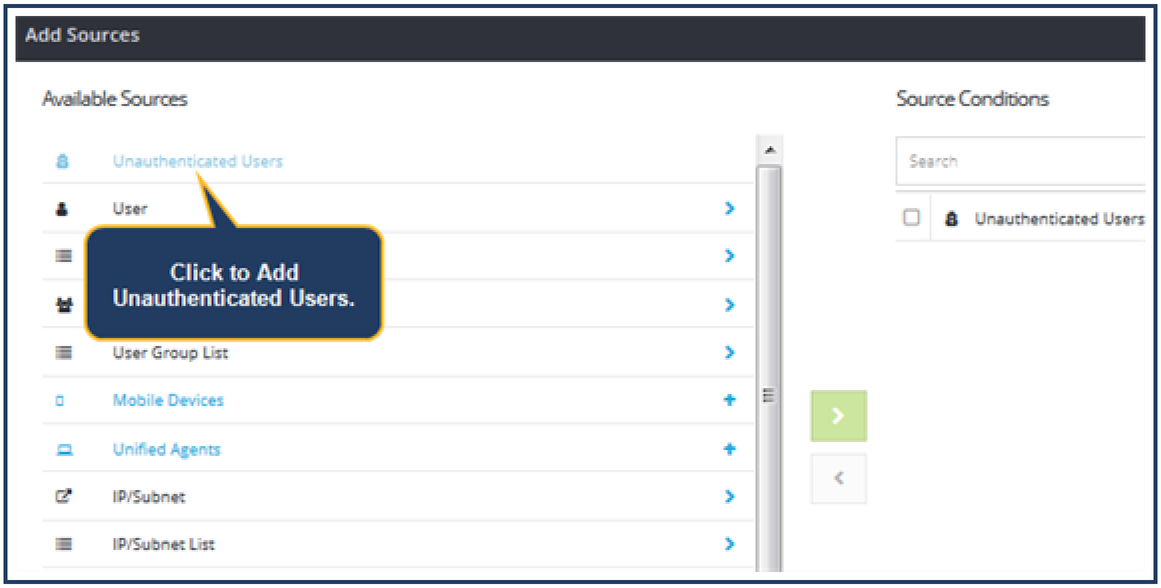
   b. (Optional) By default, the Coaching Message displays upon first content request and then not again for 60 minutes. Click the **Change** link to set a different duration: **Midnight** or **End of Session** (browser close/reopen). Click **Save** (

3. To complete this non-conditional rule, click **Finish**. You can edit its elements, such as select categories to which coaching applies.

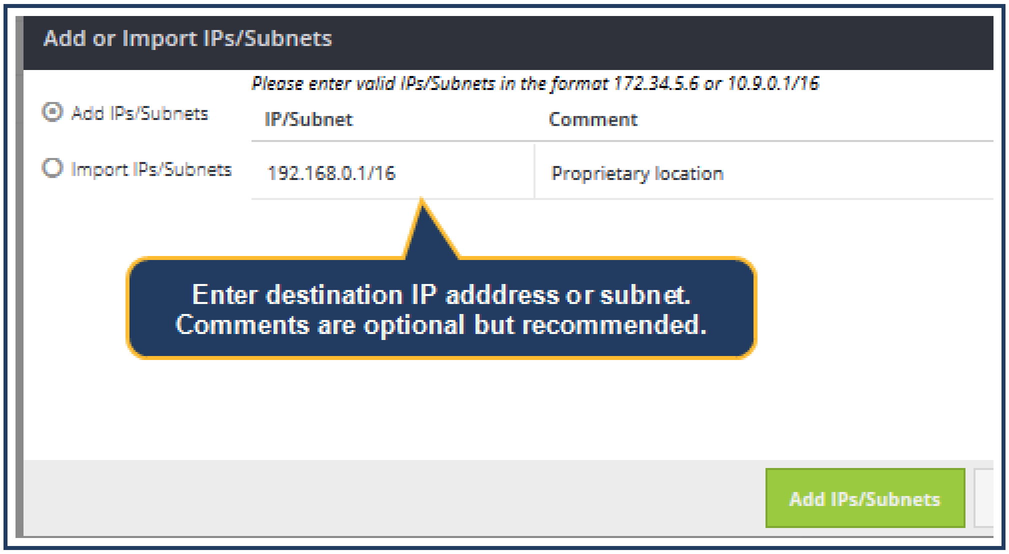
Policy Example—Prevent Unauthenticated User Access to Content

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**.



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.



Please enter valid IPs/Subnets in the format 172.34.5.6 or 10.9.0.1/16

IP/Subnet	Comment
192.168.0.1/16	Proprietary location

Enter destination IP adddress or subnet.
Comments are optional but recommended.

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**.

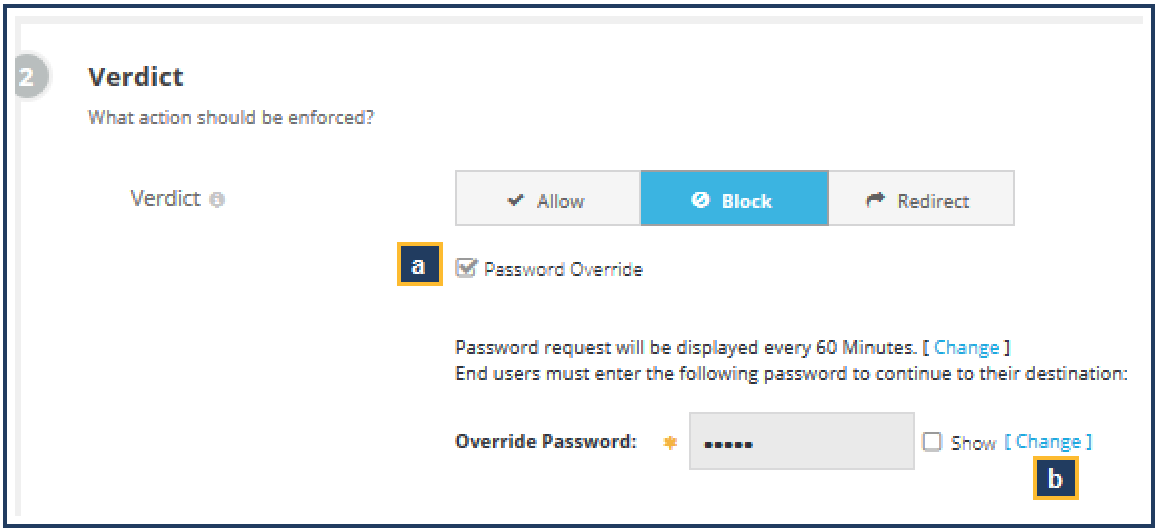
Allow Individuals Access to Blocked Content

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.



Verdict
What action should be enforced?

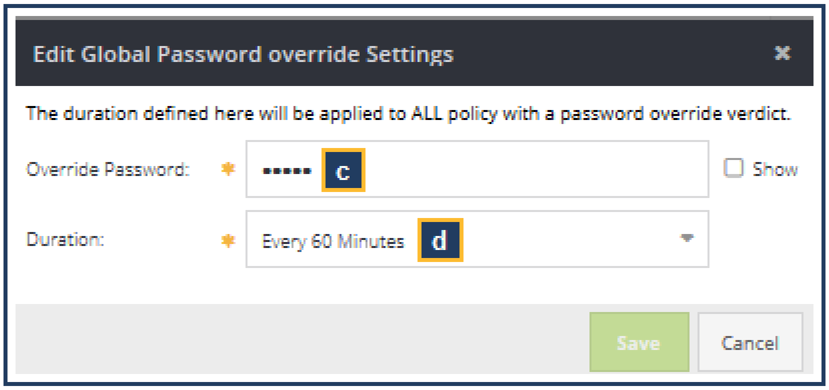
Verdict: ✓ Allow | Block | Redirect

☑ Password Override

Password request will be displayed every 60 Minutes. [Change]
End users must enter the following password to continue to their destination:

Override Password: * ••••• □ Show [Change]

   a. Select **Block** and select **Password Override**.
   b. Click **Change**. The service displays the Edit Global Password Override Settings dialog.



Edit Global Password override Settings

The duration defined here will be applied to ALL policy with a password override verdict.

Override Password: * ••••• □ Show

Duration: * Every 60 Minutes

   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

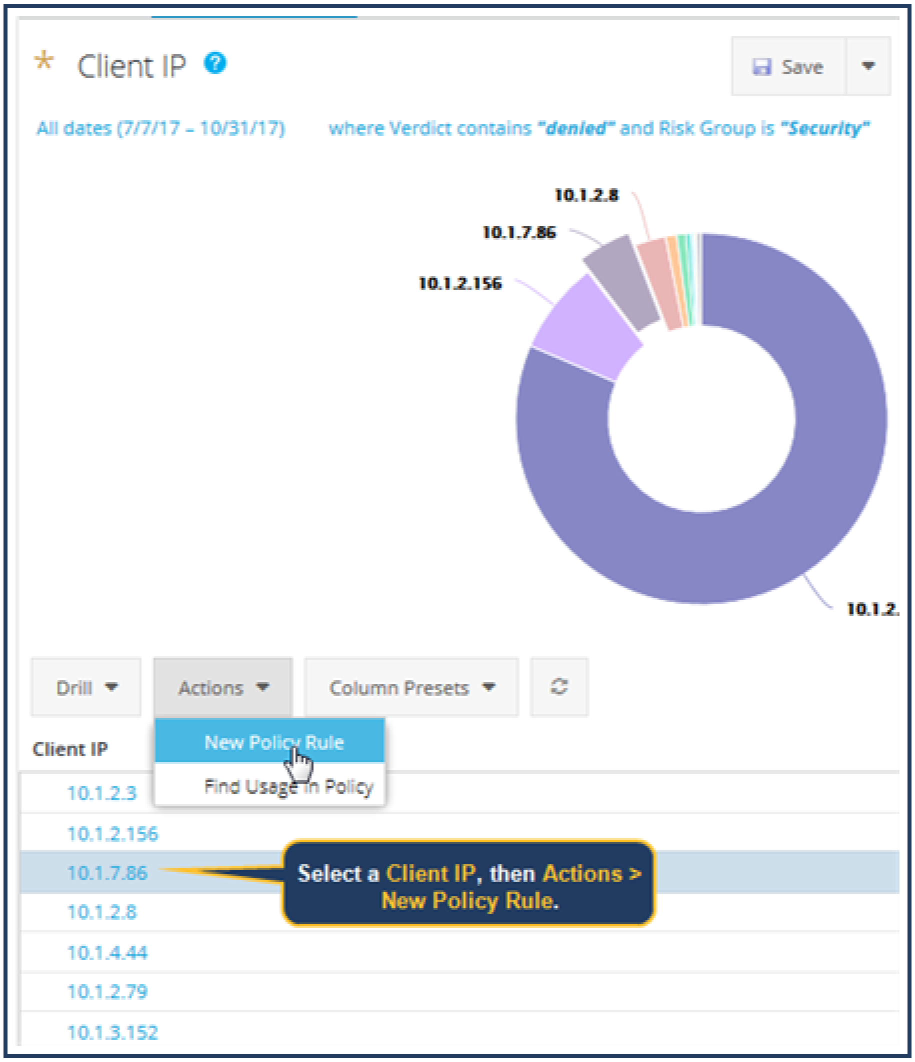
As you generate and view Web Security Service reports, you might observe suspicious activity from a client or user and want to instantly create a policy directly from the report.

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.



All dates (7/7/17 – 10/31/17)   where Verdict contains "*denied*" and Risk Group is "*Security*"

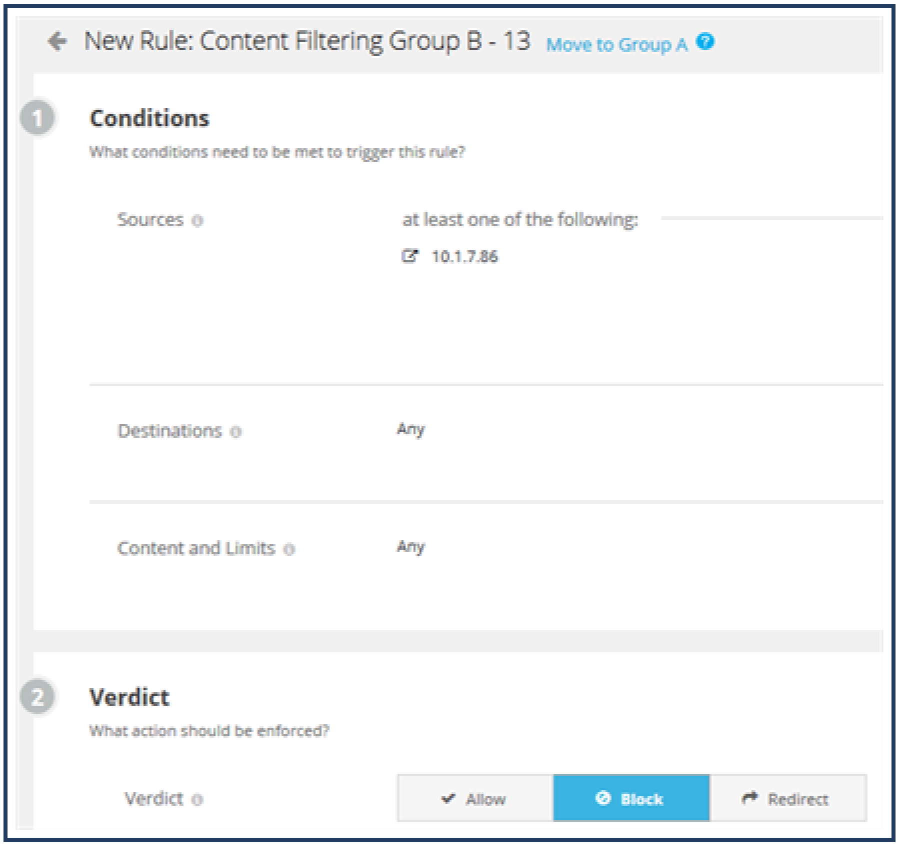
Client IP
10.1.2.3
10.1.2.156
10.1.7.86
10.1.2.8
10.1.4.44
10.1.2.79
10.1.3.152

Select a Client IP, then Actions > New Policy Rule.

   a. Select graphic element or table row. This is the user or client that requires a policy change.

   b. In the table header, select **Actions > New Policy Rule**. The service displays the New Policy Rule dialog.

2. Define the policy.



New Rule: Content Filtering Group B - 13 Move to Group A

1 **Conditions**

What conditions need to be met to trigger this rule?

Sources: at least one of the following:
10.1.7.86

Destinations: Any

Content and Limits: Any

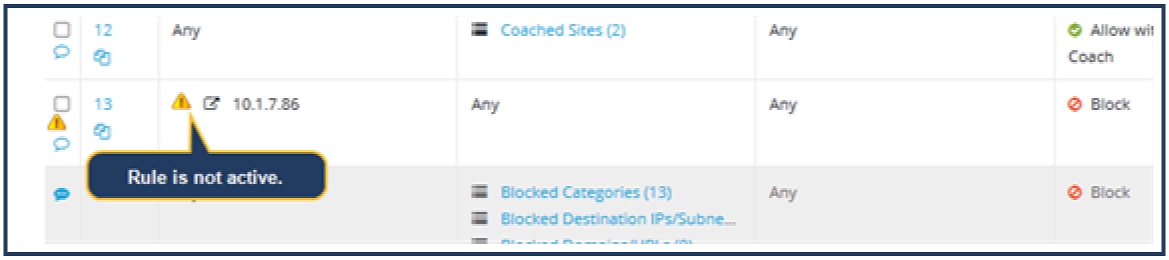
2 **Verdict**

What action should be enforced?

Verdict: ✓ Allow | ● Block | Redirect

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.



□	12	Any	Coached Sites (2)	Any	Allow wi Coach
□	13	10.1.7.86	Any	Any	Block
			Blocked Categories (13) Blocked Destination IPs/Subne...	Any	Block

Rule is not active.

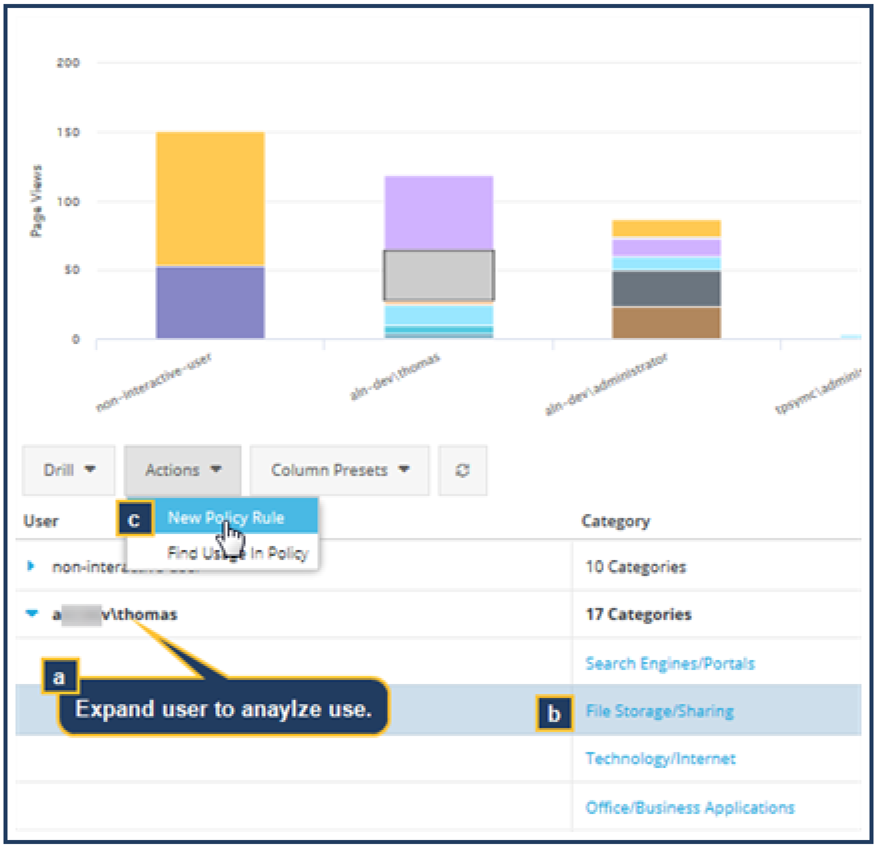
You must click **Activate** to enable the policy.

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.



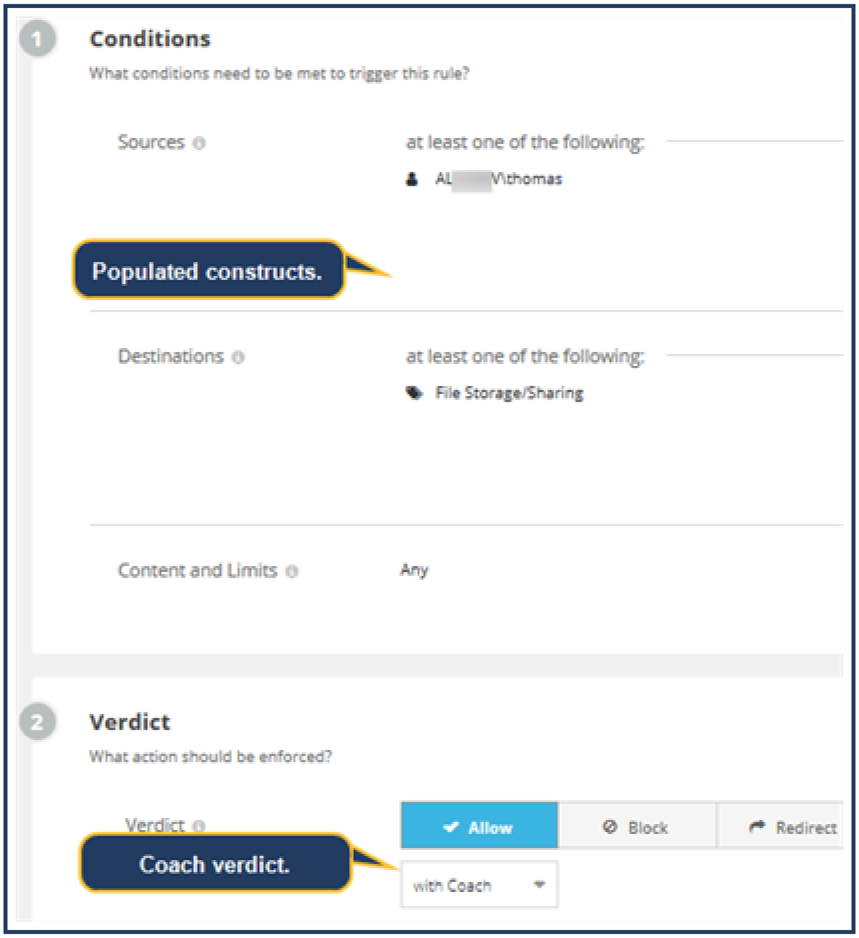
User	Category
non-inter	10 Categories
a[redacted]v\thomas	17 Categories
	Search Engines/Portals
	File Storage/Sharing
	Technology/Internet
	Office/Business Applications

a. Scroll and scan the report to identify which users require coaching.

b. Select a row that requires coaching.

c. In the table header, select **Actions > New Policy Rule**. The service displays the New Policy Rule dialog.

2. Define the policy.



1 **Conditions**

What conditions need to be met to trigger this rule?

Sources: at least one of the following:

AL[redacted]Vthomas

Populated constructs.

Destinations: at least one of the following:

File Storage/Sharing

Content and Limits: Any

2 **Verdict**

What action should be enforced?

Verdict: ✓ Allow | Block | Redirect

with Coach

Coach verdict.

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

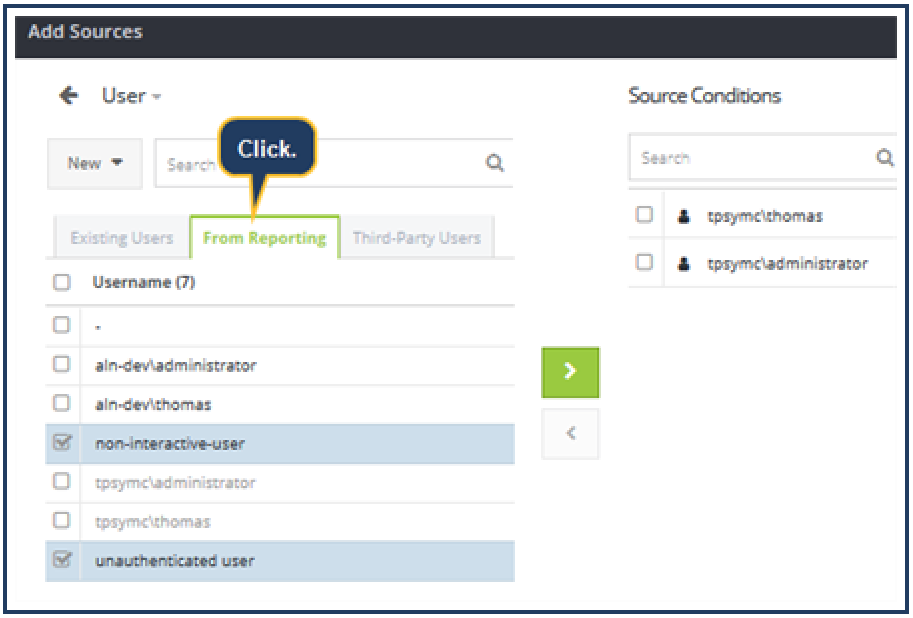
Your Symantec Web Security Service account serves a small business, all your clients use the Unified Agent, and you do not need an Active Directory deployment. You can create global policies for all of these users and create specific policies for a few of the users.

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**.

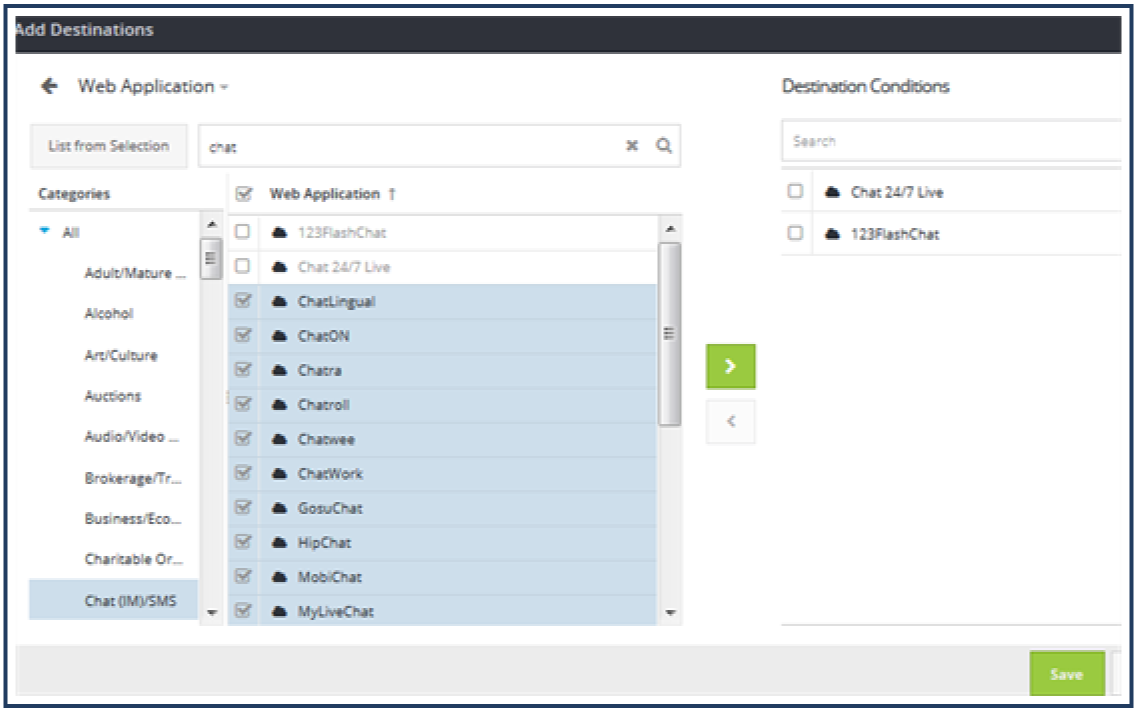


   a. Click **From Reporting**.
   b. Select the **Usernames** for this policy.
3. Click **Save** and continue defining the rule as required.

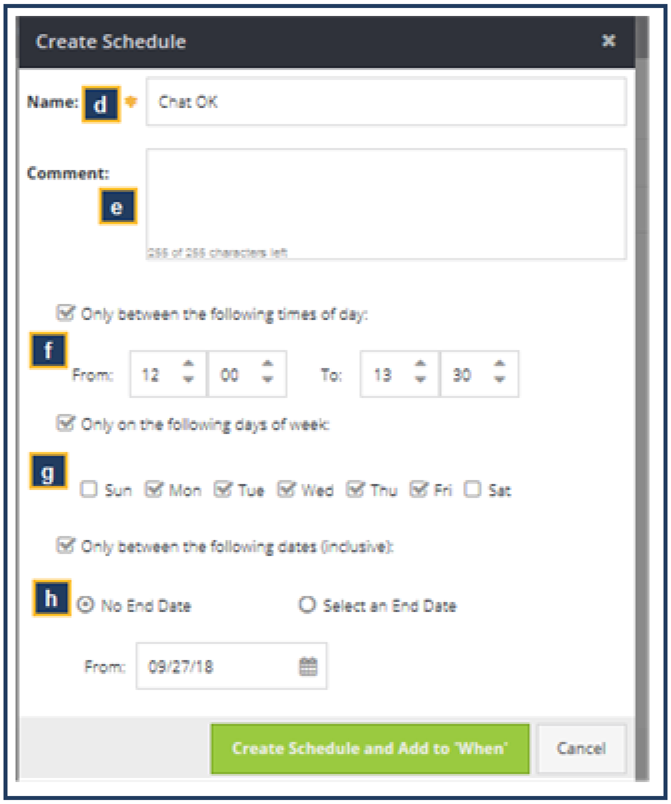
Advanced Policy Example—Set Web Access Times

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**.



Create Schedule

Name: Chat OK

Comment:

255 of 255 characters left

☑ Only between the following times of day:

From: 12 00 To: 13 30

☑ Only on the following days of week:

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

☑ Only between the following dates (inclusive):

● No End Date ○ Select an End Date

From: 09/27/18

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'**.

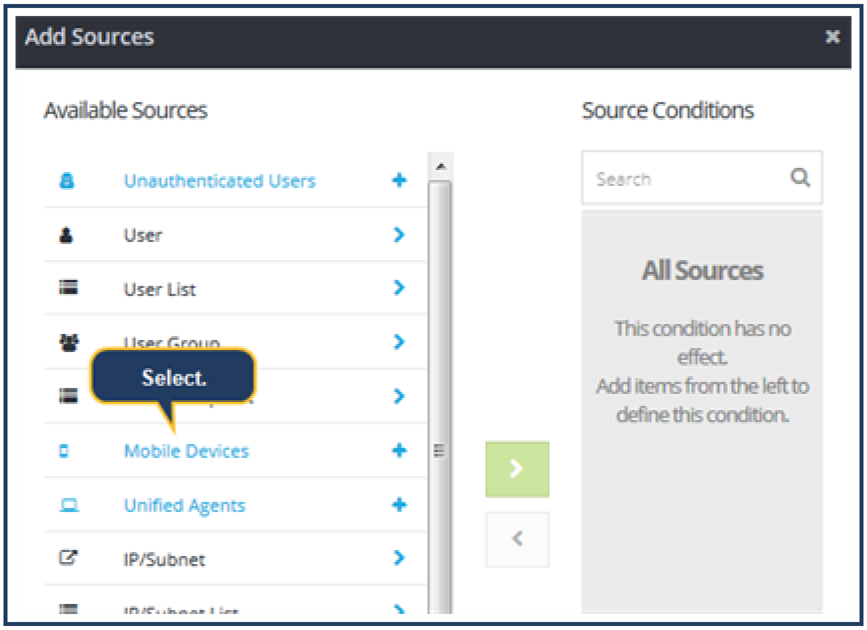
j. Click **Next**.

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 anytime 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**.

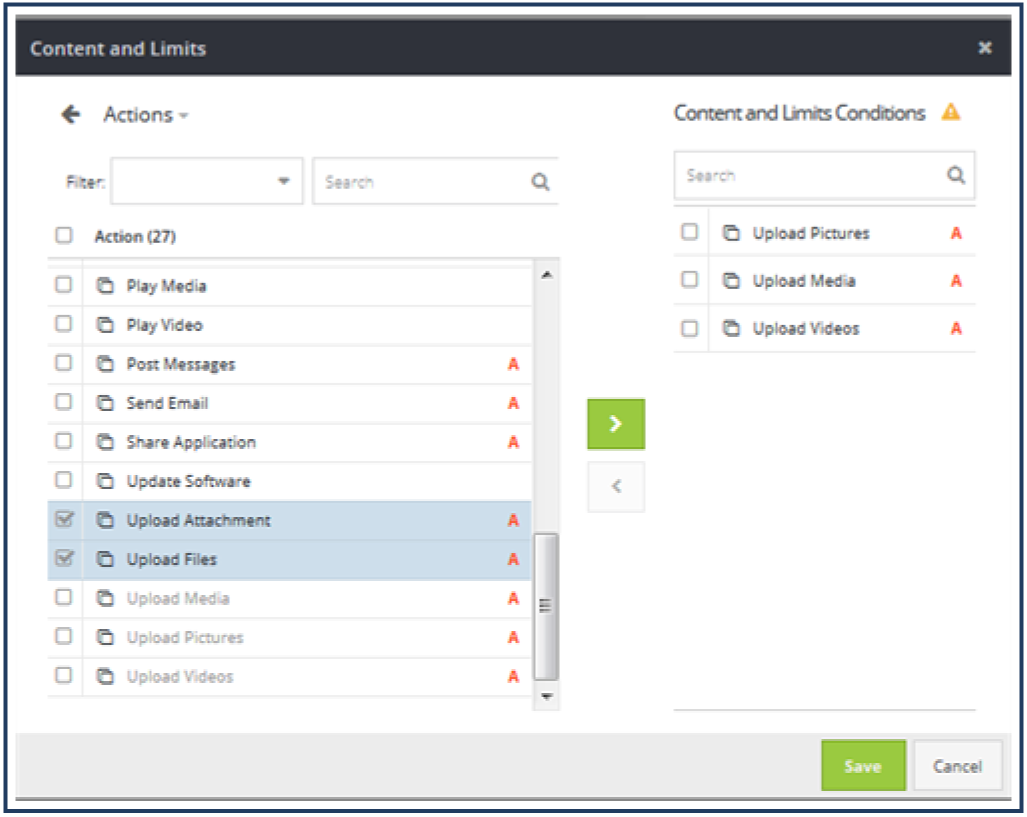


3. Click **Next** and continue to define the policy for mobile devices.

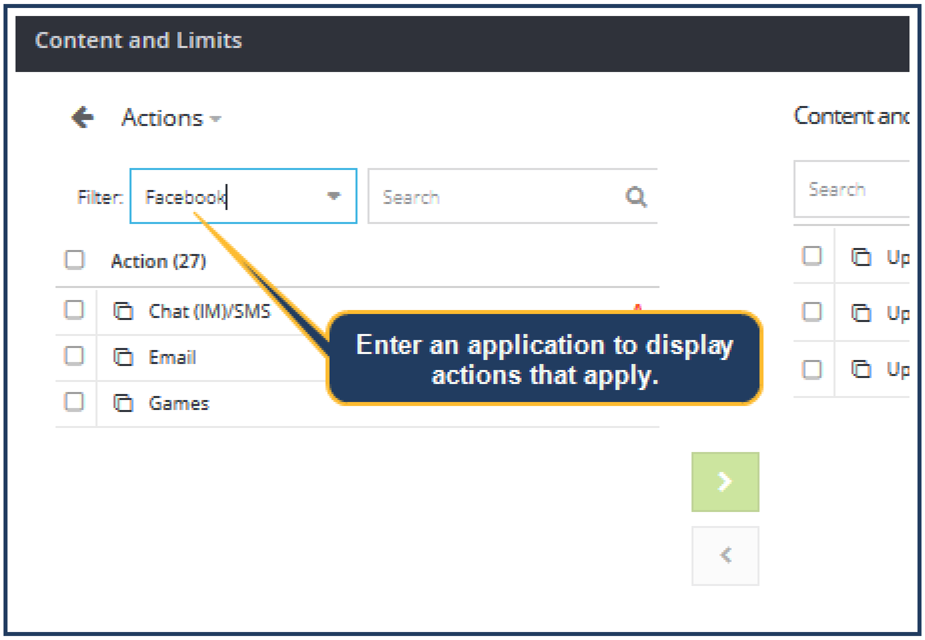
Policy Example—Block Application Actions

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**.

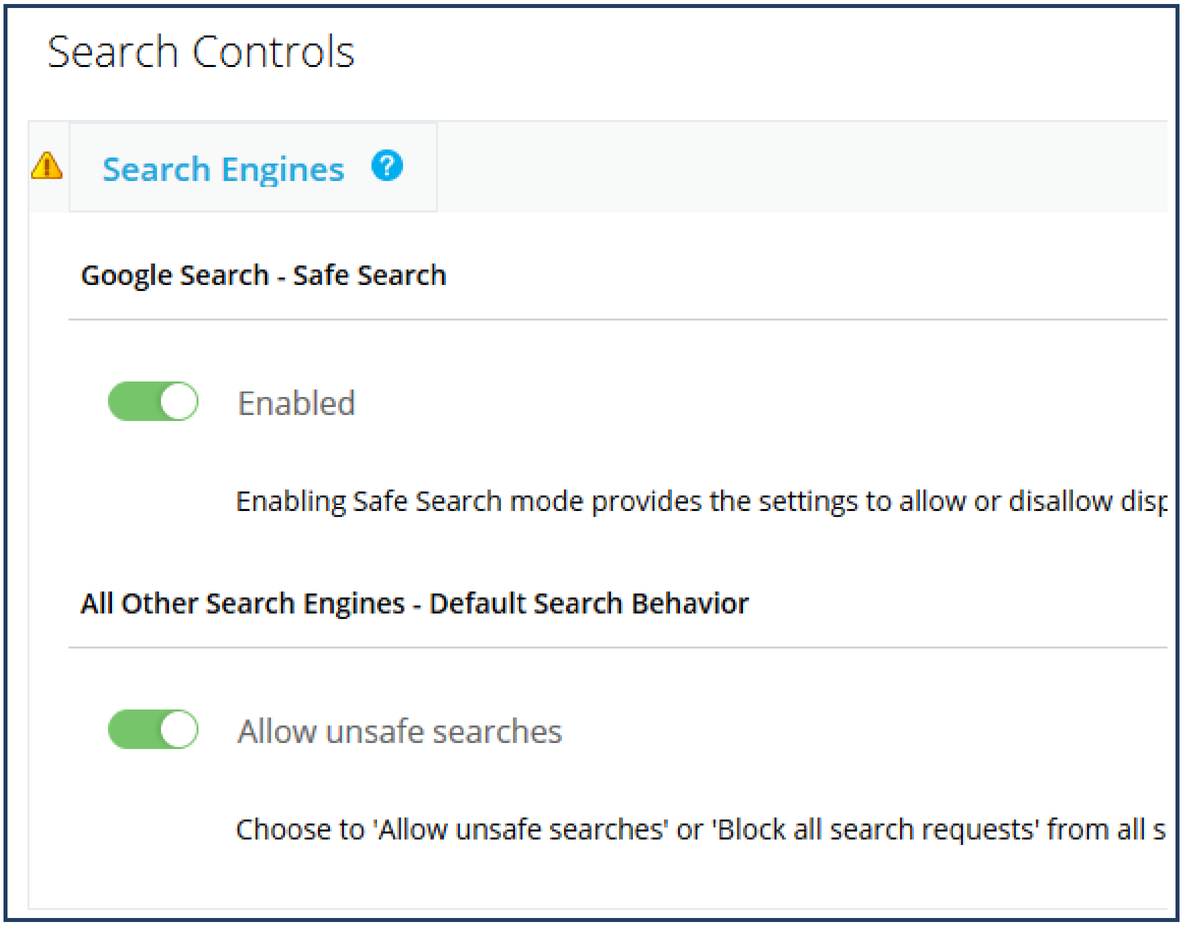
Force Safe Searches

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 88 and "Examine Encrypted (HTTPS) Traffic" on page 83.

1. In **Solutions** mode, select **Content Filtering > Search Controls**. Show screen...



Search Controls

Search Engines

Google Search - Safe Search

Enabled

Enabling Safe Search mode provides the settings to allow or disallow disp

All Other Search Engines - Default Search Behavior

Allow unsafe searches

Choose to 'Allow unsafe searches' or 'Block all search requests' from all s

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

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.

Current Whitepaper.

Name	Previous Name (if applicable)	Definition
Alcohol	Same	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.
Chat (IM)/SMS	Chat/Instant Messaging	Sites that provide chat, text messaging (SMS), or instant messaging capabilities or client downloads.
Computer/Information Security	(New)	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.
Controlled Substances	Illegal Drugs	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 *not* include alcohol, tobacco, or marijuana sites as these have dedicated categories.
E-Card/Invitations	Greeting Cards	Sites that facilitate the sending of electronic greeting cards, invitations, or similar electronic messages typically used to mark an event or special occasion.
Entertainment	Same	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.
File Storage/Sharing	Online Storage	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.

Name	Previous Name (if applicable)	Definition
Financial Services	Same	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.
Hacking	Same	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.
Health	Health	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.
Internet Connected Devices	(New)	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.
Malicious Sources/Malnets	Malicious Sources	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).
Marijuana	(New)	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.
Mixed Content/Potentially Adult	Open/Mixed Content	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.
Non-Viewable/ Infrastructure	Non-Viewable	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.
Office/Business Applications	Web Applications	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.

Name	Previous Name (if applicable)	Definition
Personal Sites	Blogs/Personal Pages	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.
Piracy/Copyright Concerns	(New)	Sites that provide information or technology for cracking or pirating software or other protected intellectual property, and sites that distribute such media.
Political/Social Advocacy	Political/Activist Groups	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.
Scam/Questionable/Illegal	Same	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.
Sexual Expression	Alternative Sexuality/Lifestyles	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.
Software Downloads	Same	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.
Technology/Internet	Computers/Internet	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.
Tobacco	Same	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.
Uncategorized	Unrated	
Web Ads/Analytics	Web Ads	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).
Web Hosting	Same	Sites of organizations that provide top-level domain pages, as well as web communities, blog hosting sites, and other hosting services.

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.

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—StuffIt (Macintosh)
- sitx—StuffIt (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—PowerINSPECT 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/dbase 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

8BF	APP	BPL	class	COFF
com	DCU	DOL	EAR	EGT
ELF	jar	XPI	Mach-O	nlm
s1es	VAP	WAR	XBE	XCOFF
VBX	ocx	TLB		

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

ani	bat	chm	cmd	com
cur	dll	exe	hta	hlp
msi	pif	reg	scr	vb
vbs	wmf	wsc	wsf	wsh

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
- MGF—MicroGrafx Font
- OTF—OpenType Font
- PCF—Portable Compiled Font
- PFA—Printer Font ASCII
- PFB—Printer Font Binary" ; Adobe
- PFM—Printer Font Metrics" ; Adobe
- FOND—Font Description resource" ; Mac OS
- SFD—FontForge spline font database Font
- SNF—Server Normal Format
- TFM—TeX font metric
- TTF—TrueType Font
- TTC—TrueType Font

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
- CGM—Computer Graphics Metafile an ISO Standard
- 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 (.3dmf)
- 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—DuupeCheck 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
- HWPML—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
- APPLESCRIPT—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
- VBS—Visual Basic Script

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
- TLB—Windows Type Library

Source Code for Computer Programs

- ADA, ADB, 2.ADA—Ada (body) source
- ADA, ADB— Ada (body) source
- ;ADS, 1.ADA—Ada (specification) source
- ADS—Ada (specification) source
- ASM, S—Assembly Language source
- BAS—BASIC, Visual Basic module
- BB—Blitz3D
- BMX—BlitzMax
- C—C source
- CLS—Visual Basic class
- COB, CBL—Cobol source
- CPP, CC, CXX, C—C++ source
- CS—C# source
- CSPROJ—C# project (Visual Studio .NET)
- D—D source
- DBA—DarkBASIC source
- DBPro—DarkBASIC Professional project
- E—Eiffel source
- EFS—EGT Forever Source File
- EGT—EGT Asterisk Source File, could be J, C#, VB.net, EF 2.0 (EGT Forever)
- EL—Emacs Lisp source
- FOR—Fortran source
- FTN—Fortran source
- F—Fortran source
- F77—Fortran source
- F90—Fortran source
- FRM—Visual Basic form

- FRX—Visual Basic form stash file (binary form file)
- 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)