Web Security Service

Connectivity:
Explicit Proxy and SEP Client

Revision: NOV.07.2020

Symantec
A Division of Broadcom

Copyrights

WSS Access Method: Explicit Proxy

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

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

This document describes how to use the PAC File Management Service (PFMS) to set up explicit proxy connections to the WSS for security scanning and policy checks on web-bound traffic. It includes how to implement the WSS and Symantec Endpoint Protection (SEP) solution.

Table Of Contents

WSS Access Method: Explicit Proxy 5
Table Of Contents 6
Connectivity: About Explicit Proxy 8
Why Select This Method? *10*
Connectivity: PAC File Management Service (EP) 12
Technical Requirements 12
Technical Limitations 12
Example Procedure–New PAC File 13
Edit *17*
Duplicate *17*
Import *17*
Connectivity: Set Browsers to Explicit Proxy 19
Technical Requirements 19
Connectivity: Publish PAC File With WPAD 22
Technical Requirements 22
Procedure 22
DHCP Method *22*
DNS Method *22*
Connectivity: About Symantec Endpoint Protection 24
Why Select This Method? *25*
Why Select This Method? *27*
Connection Methods *28*
Authentication Support *28*
Why Select This Method? *28*
Connectivity: WSS-SEP with Captive Portal 30
Technical Requirements 30
Technical Limitation 31
Best Practice 31
Procedure–Enable Web Traffic Redirection on SEP 31
PAC File Management in SEP 33
Connectivity: WSS-SEP-WTR With Seamless Identification 36
Technical Requirements 36
Technical Limitations 37
Best Practice 37

Procedure–Enable Web Traffic Redirection and Seamless Identification on SEP 37
Additional Support 42

Connectivity: WSS-SEP-NTR With Seamless Identification 43
Technical Requirements 43
Technical Limitation 43
Best Practice 43
Procedure–Enable Web Traffic Redirection and Seamless Identification on SEP 43
Additional Support 46

Connectivity: WSS-SEP Roaming SAML 47
Technical Requirements 47
Technical Limitations 48
Best Practice 48
Procedure–Enable Web Traffic Redirection and Seamless Identification on SEP 48
Additional Support 54

Prevent IP/Subnet From Routing to the Web Security Service 55
Notes 55
Procedure–Manually Add IP Addresses 55
Import IP Address Entries From a Saved List 56

Add an Explicit Proxy Location 57

Reference: Required Locations, Ports, and Protocols 59
Symantec Resource 59
Connectivity Methods 59
Authentication 61

Reference: Sample PAC File for Explicit Proxy 63

Connectivity: About Explicit Proxy

The Explicit Proxy Access Method refers to using proxy auto-config (PAC) files to direct internet-bound traffic to the Web Security Service or to specific proxy servers based on the destinations. It might also refer to the method of using the browser settings in client browsers to direct traffic to proxy servers that host PAC files.

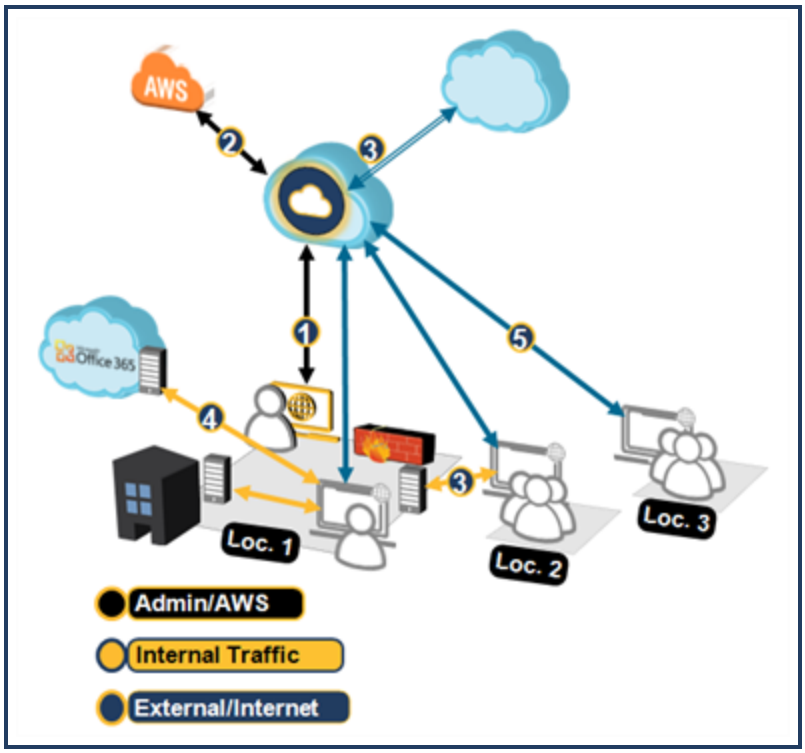
A PAC file is a JavaScript that automates which proxies web browsers communicate through to reach the internet.

- Requests for external websites or requests made by company-owned computers using an external IP address are routed through the service.
- Computers inside the firewall are given access to sites on the corporate intranet without routing through WSS.

The Explicit Proxy connectivity method protects endpoints at a fixed location (clients reside behind a single-IP egress device) or roaming clients.

About the PAC File Management Service

The WSS PAC File Management Service (PFMS) enables deployment flexibility as you manage PAC files and PAC file location association through the cloud service. Furthermore, you can create and update bypass lists and other configurations directly in the WSS portal. With the PFMS, you can create up to 100 PAC files and assign them to different locations. For example, you want on-premises work stations in one location to use one PAC file that bypasses specific servers and Office 365 requests. But connections from other remote locations always connect through WSS.



1–For various locations, the Admin generates a PAC file in the WSS portal, possibly providing custom bypassing of specific servers. The PAC files are installed on client browsers, either through your IT infrastructure or to Symantec Endpoint Protection (SEP) agents.

2–The PFMS manages the created PAC files, which are available for updating. Amazon Web Services (AWS) stores the PAC files; AWS provides the automatic health checks and failover infrastructure.

> **Note:** PAC file edits might experience up to a one minute delay for world-wide propagation.

3–By default, the PAC file script identifies the internal IP address based on the RFC 1918 standard. Direct access to the internal URL is granted.

4–Location 1's PAC file instructs the browser to bypass WSS for Office 365 requests.

5–For other locations, the PAC files proxies all internet-bound traffic through the nearest WSS datacenter.

Why Select This Method?

Benefits–

- Valid if your environment has a PAC-managed proxy.
- Your environment has infrastructure and IP address space.
- You do not want to install an agent.

Select another method if–

- Your network egress is not a static IP address or it requires traversing a NAT devices.
- You require Client IP-based policy, as addresses are not visible to WSS.

Is this the method you require?

- "Connectivity: PAC File Management Service (EP)" on page 12.

About the Default PAC File

WSS provides a default PAC file: `https://portal.threatpulse.com/pac`.

> **Tip:** Currently, this is intended for backward compatibility and will be deprecated in a future service update. The best practice is to create a custom PAC file with the PFMS.

Is this the method you require?

- "Connectivity: Set Browsers to Explicit Proxy" on page 19.
- "Connectivity: Publish PAC File With WPAD" on page 22.

Connectivity: PAC File Management Service (EP)

The Web Security Service provides a Proxy Auto Configuration (PAC) File Management Service (PFMS) to facilitate the Explicit Proxy connectivity method. This system allows you to create more than one PAC file, assign them to different locations, and customize them to allow or bypass specific web destinations. Then you can create WSS policy based on these locations or traffic routed from specific PAC files.

You can also create PAC files for roaming endpoints. For example, you plan to integrate the Symantec Endpoint Protection (SEP) with the WSS. You want a separate PAC file to be used only for the SEP agent connections.

Technical Requirements

- Know the single static public egress IP address.
- Browsers and operating systems are able to accept and use PAC files.
- Firewall rules:
    - Open port 443.
    - If your firewall allows white-listing by DNS, white-list `pfms.wss.symantec.com`; this is the preferred method.
    - If your firewall does *not* allow white-listing by DNS, allow the following static IP address: `34.120.17.44` (November 7, 2020).

      If you employed the PFMS before November 7, 2020, the following IP addresses were used. Firewall rules for these IP addresses can remain in place in the near-term as a precaution for failover or fallback. A follow up announcement will be made after the existing IPs have been fully decommissioned.

        - `35.155.165.94`
        - `35.162.233.131`
        - `52.21.20.251`
        - `52.54.167.220`
        - `199.247.42.187`
        - `199.19.250.187`
- The WSS supports up to 100 different PAC files.
- The PFMS supports existing, supported authentication methods (Auth Connector, SAML, Captive Portal).

Technical Limitations

- Use Firefox 57.0.2+; older versions of Firefox may not apply PAC file correctly. This is third-party limitation with the Firefox browser.
- Internet Explorer versions 11, Edge, and newer might cache old PAC file execution results for a particular host. If this occurs, restart Internet Explorer.

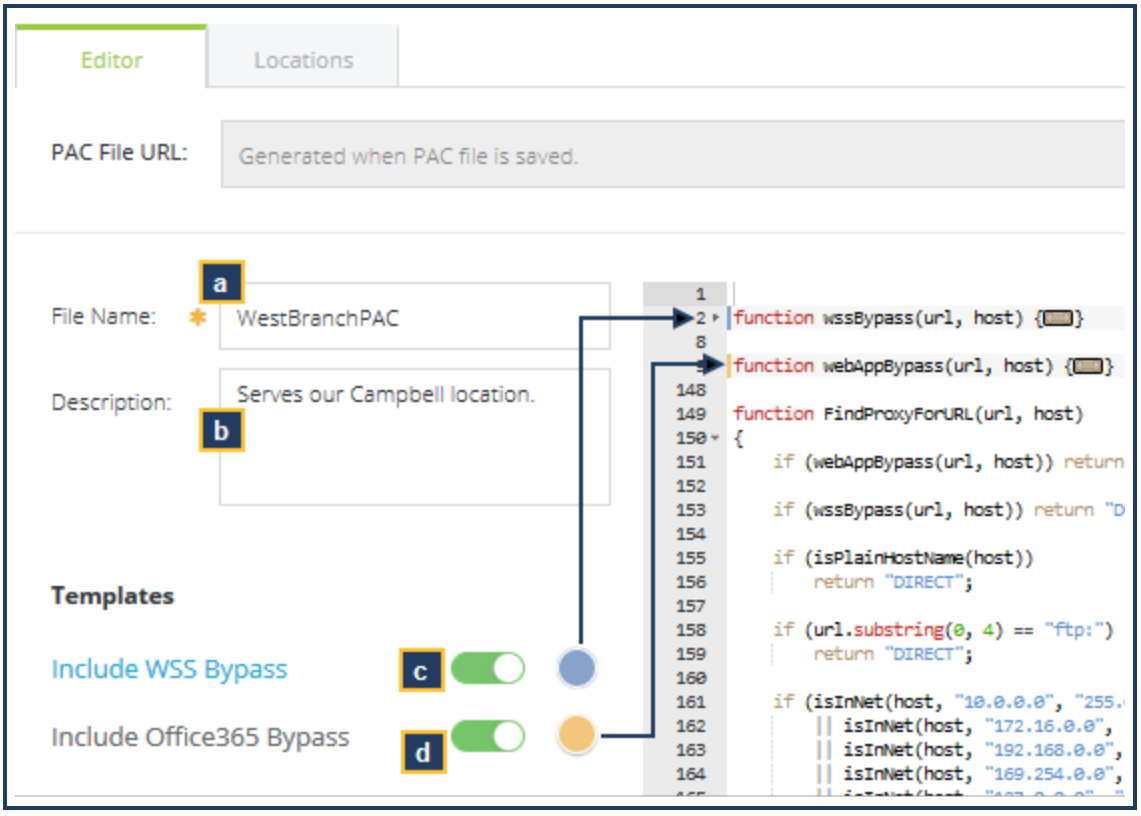
- If the browser does not accept cookies or PAC files, supportability becomes difficult.
- If the user agent is unable to process the PAC file, there will be no protection or exceptions.

Example Procedure–New PAC File

One option is to duplicate the default PAC file and modify it.

To demonstrate the PAC File Management feature, the following steps create a *new* PAC file and designate its use for the SEP test Explicit Proxy location (previously entered on the **Connectivity > Locations** page).

1. In the WSS portal, navigate to **Connectivity > PAC Files**.
2. Click **New File**. The portal switches to the PAC File Editor.



a. **Name** the PAC file.

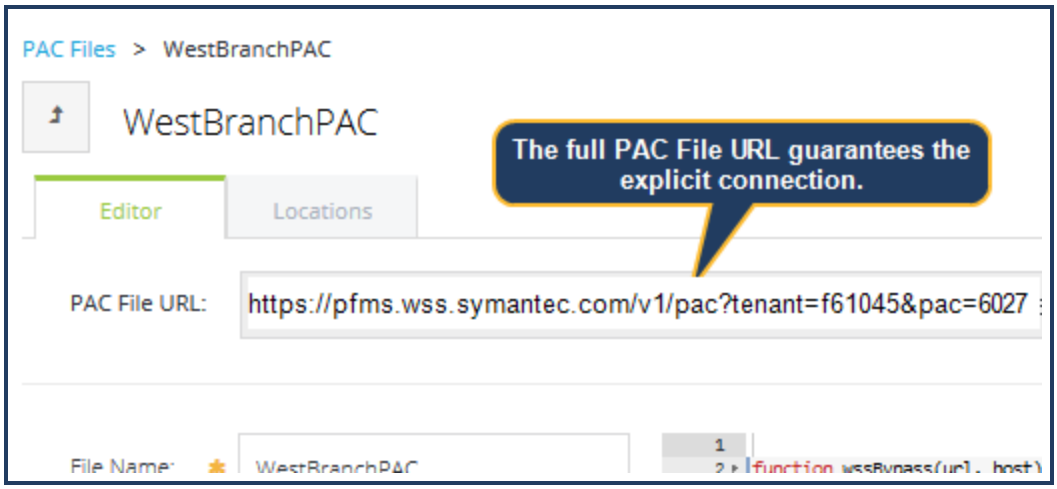
b. (Optional) **Describe** the purpose of this PAC file.

c. **Include WSS Bypass** adds any IP addresses or domains that were previously added to the portal bypass lists (**Connectivity > Bypassed Traffic**). You can click the expander to view those entries; however, you cannot edit those entries here.

> **Tip:** Bypass lists cannot exceed 256 KB in size.

d. **Include Office 365 Bypass** adds all of the currently known Microsoft Office web application domains.

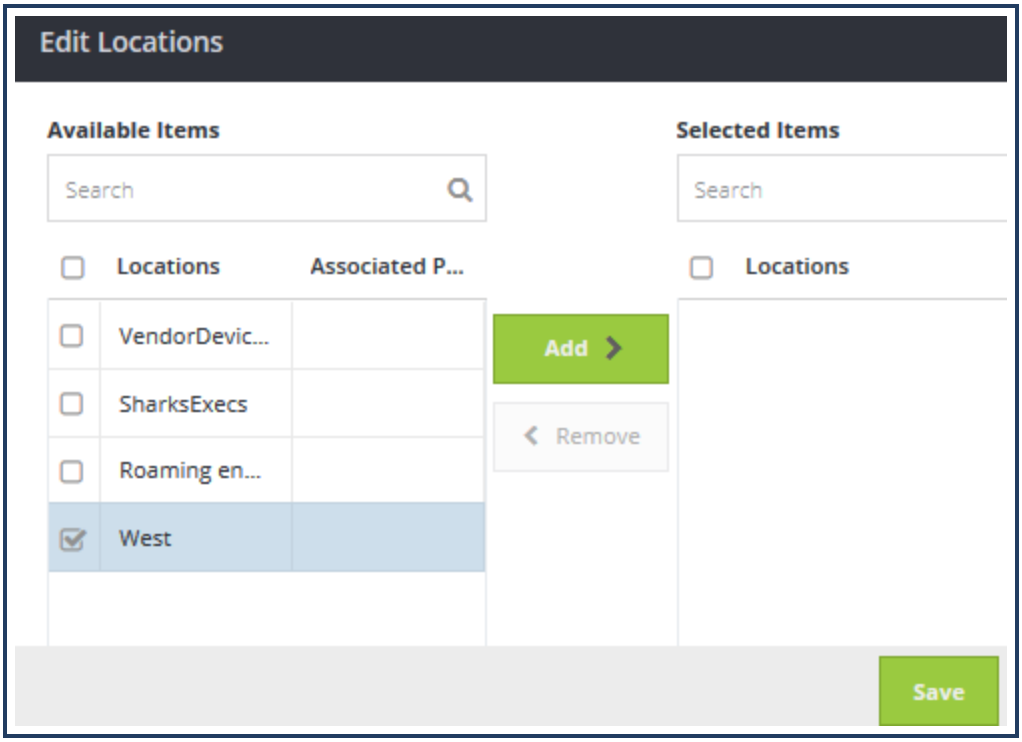
3. Click **Save**.



The portal generates an explicit PAC File URL. You can copy this URL and use it for an explicit proxy configuration to guarantee that this PAC is used. For example, you can send this to the Admin who is configuring the SEP clients to direct traffic to WSS.

4. Continuing with the example, click the **Locations** tab.

a. Click **Edit Locations**.

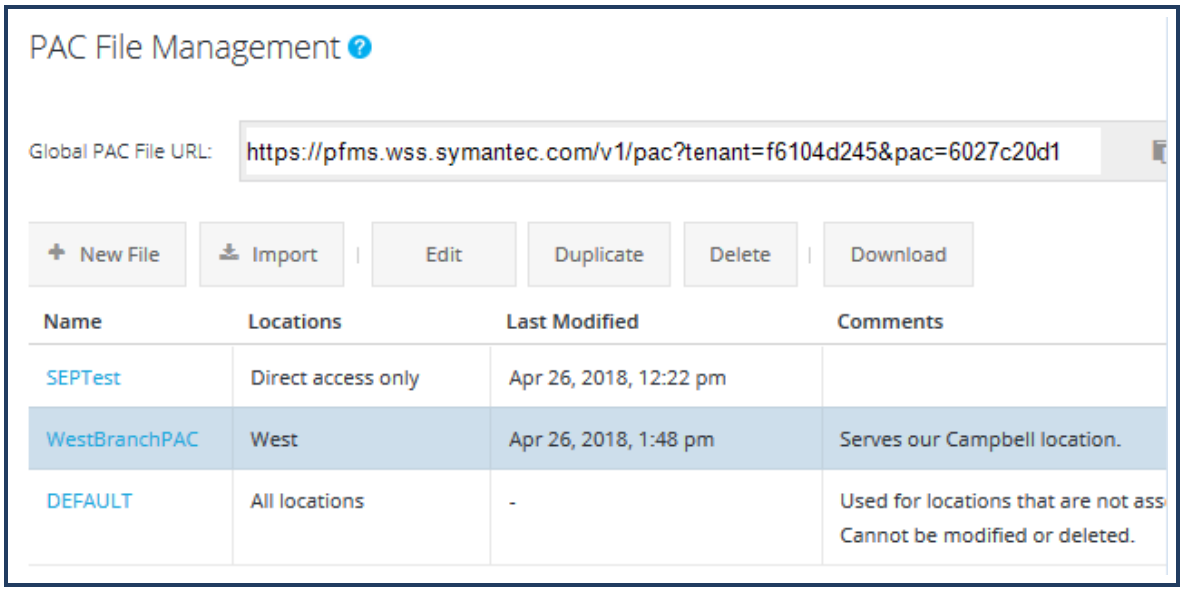


b. Select a **Location** that is to connect through this PAC file. This example selects a previously added Explicit Proxy Location created to test SEP integration.

> **Tip:** You can have more than one location that uses the same PAC file. For more information about the Roaming Endpoints, see "About the Roaming Location" on page 17.

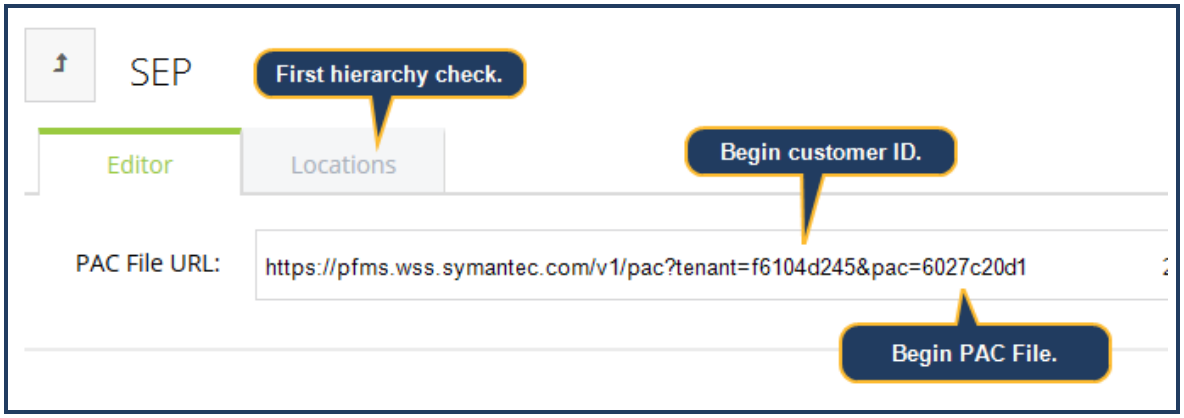
c. Click **Add** and **Save**.

5. Click the **PAC Files** link (or the Up arrow icon next to the PAC file name). The portal now displays the newly-created PAC file.



About PAC File Hierarchy

With the possibility of multiple PAC files, the WSS evaluates and connects according to the following hierarchy.



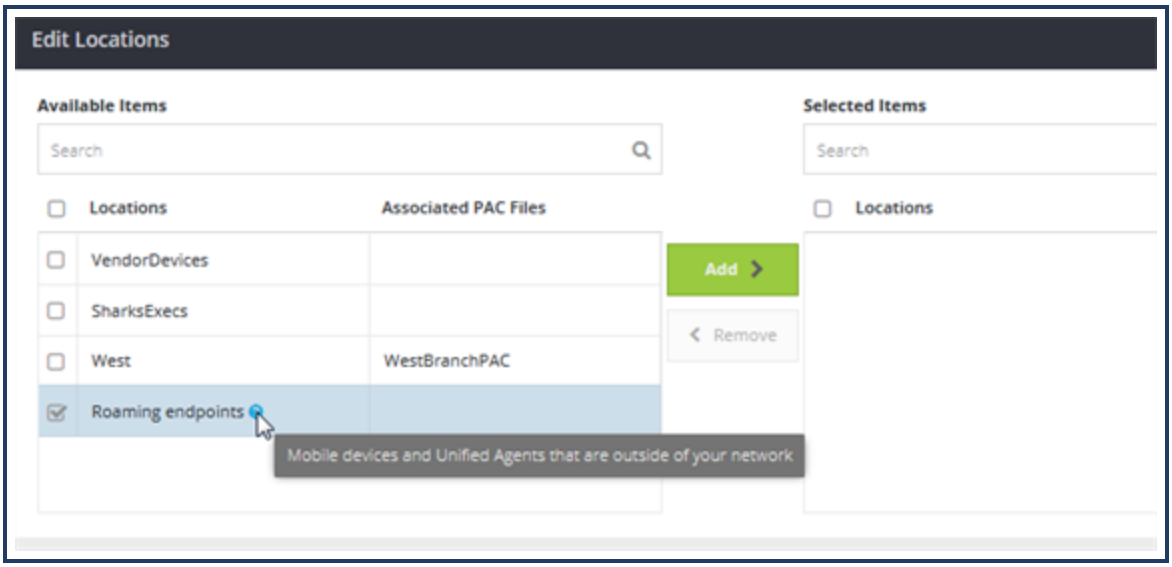
- Full custom PAC File URL–The connection always uses the parameters in this PAC file.
- **Locations**–The WSS checks to see if the Location has an assigned PAC file. If yes, the connection proceeds with those parameters.
- **Default PAC File**–If no Location is assigned to the connection, WSS uses the default PAC file (`http://portal.threatpulse.com:8080/pac`).

> **Note:** The default PAC file behavior is *fail open*. If for some reason the client cannot connect to WSS, it falls back and goes DIRECT.

- If you configure a connection to use the PAC File URL *only* up to the customer ID portion (see screenshot), then WSS follows the Locations/Default hierarchy described in the previous two bullets.

About the Roaming Location

The PFMS provides a Location called Roaming Endpoints. You can create a PAC file that applies to WSS Agents and mobile devices that access the internet when outside of the corporate network. This is available on the **Locations** tab of the PAC File dialog.



After the traffic reaches the WSS, your configured Authentication method is triggered (**Identity > Auth Connector > Roaming Captive Portal** option or **Identity > SAML**).

PAC File Management

Edit

During the creation phase or any time after, you can **Edit** a PAC file to change the parameters. Be advised that this requires a moderate knowledge of network connections.

> **Note:** PAC file edits might experience up to a one minute delay for world-wide propagation.

Duplicate

You can **Duplicate** an existing PAC file and modify it for another purpose. For example, you want to test a configuration update before implementing it.

Import

If you have created PAC files in text files, you can **Import** them for use in WSS.

Troubleshooting

- Verify the browser can download the PAC file.
- Confirm provided PAC file is the correct one for the situation (Location, Roaming).
- Verify issue applies to *all* browsers.
- Confirm if the issue is related to one webserver or several.
- Create three troubleshooting test policies.
    - Public URL with *no* auth required.
    - URL requiring Auth no policy.
    - URL with Auth policy.

Connectivity: Set Browsers to Explicit Proxy

Manually configure web browsers on client systems or a demonstration client to point to the location of the Symantec Proxy Automatic Configuration (PAC), which provides the route to the Web Security Service. See "Connectivity: About Explicit Proxy" on page 8.

> **Tip:** Currently, this is intended for backward compatibility and will be deprecated in a future service update. The best practice is to create a custom PAC file with the PFMS.

Technical Requirements

- Verify that firewall port `8080` is open.

> **Warning:** If you continue to use the default PAC file and for some reason WSS is not accessible–for example, firewall issue on 8080, mis-configured URL, deleted PAC file), fail open occurs and the connection goes direct.

Apple Safari

1. Select **Apple** menu **> System Preferences**.
2. Select the **Internet and Network** tab.
3. Select an option:
   - If you are connected by cable to the network, select **Ethernet**.
   - If you are connected using WiFi, select the **AirPort** option.
4. Click **Advanced**. Enter the address of your PAC file in the **Address** field. For example, `https://portal.threatpulse.com/pac`.
5. Click the **Proxies** tab.
   a. Select **Using a PAC file**.
   b. Enter the Web Security Service PAC file location in the **Address** field: `https://portal.threatpulse.com/pac`.
6. Select **Quit** to exit System Preferences.

Google Chrome

1. In the top-right corner of the browser, select the **wrench** .
2. From the drop-down list, select **Options**. The browser displays the Google Chrome Options dialog.
3. In the **Network** section, click **Change proxy settings.** The browser displays the Internet Properties dialog.
4. Click the **Connections** tab.
5. In the **Local Area Network (LAN) Settings** section, click **LAN settings**. The Local Area Network (LAN) Settings dialog displays.
    a. In the **Automatic configuration** area, select **Use automatic configuration script**.
    b. Enter the Web Security Service PAC file location in the **Address** field: `https://portal.threatpulse.com/pac`.
6. Click **OK** and exit out of all open dialogs.

Microsoft Internet Explorer

1. Select **Tools > Internet Options**.
2. Select the **Connections** tab.
3. If you are using a VPN connection, click **Add** to set up the connection wizard. If you are using a LAN connection, click **LAN settings**
4. LAN settings dialog:
    a. Select **Automatically detect settings** and **Use automatic configuration script**.
    b. Enter the Web Security Service PAC file location in the **Address** field: `https://portal.threatpulse.com/pac`.
5. Click **OK** and exit out of all open dialogs.

Mozilla Firefox

1. Select **Tools > Options**. The browser displays the Options dialog.
2. Select the **Advanced > Network** tab.
3. In the **Connections** area, click **Settings**.
4. Configure **Connection Settings**:
    a. Select **Automatic proxy configuration URL**.
    b. Enter the WSS PAC file location in the **Address** field: `https://portal.threatpulse.com/pac`.
5. Click **OK** and exit out of all open dialogs.

Next Step

- Proceed to "Prevent IP/Subnet From Routing to the Web Security Service" on page 55.

Connectivity: Publish PAC File With WPAD

Enforce the use of a Proxy Automatic Configuration (PAC) file without manual web browser configuration by using the Web Proxy Auto-Discovery (WPAD) protocol. WPAD offers two options to publish the location of the PAC file: Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS). See "Connectivity: About Explicit Proxy" on page 8.

> **Tip:** Currently, this is intended for backward compatibility and will be deprecated in a future service update. Symantec strongly encourages you to create a custom PAC file with the PFMS.

Technical Requirements

- Verify that firewall port `8080` is open.

  > **Warning:** If you continue to use the default PAC file and for some reason the WSS is not accessible–for example, firewall issue on 8080, mis-configured URL, deleted PAC file), fail open occurs and the connection goes direct.

- Example PAC File.

  "Reference: Sample PAC File for Explicit Proxy" on page 63

Procedure

Step 1–Select and perform a publish method.

DHCP Method

1. Before retrieving the first page, the web browser sends the local DHCP server a `DHCPINFORM` query.
2. The web browser uses the URL returned from the server to locate the PAC file.
3. If the DHCP server does not return the location of the PAC file, the DNS method is used.

DNS Method

1. Change the name of the PAC file located on the web server from `proxy.pac` to `wpad.dat`.
2. The web browser searches the web server for the PAC file using URLs until the proxy configuration file is found in the domain of the client. The URL format is `http://wpad.x.x.com/wpad.dat`. `WPAD.dat` is the name for the PAC file and `x` is a part of the domain name.

Step 2–Bypass IP Addresses/Subnets

Some IP addresses or subnets do not require WSS processing. For example, you want to exclude test networks. Configure the service to ignore these connections.

See "Prevent IP/Subnet From Routing to the Web Security Service" on page 55.

Step 3–Add an Explicit Proxy Location in the portal.

See Add an Explicit Proxy Location.

Next Step

- Proceed to "Prevent IP/Subnet From Routing to the Web Security Service" on page 55.

Connectivity: About Symantec Endpoint Protection

The Symantec Endpoint Protection (SEP) solution provides security to endpoint devices, such as laptops. SEP is an agent-based approach that uses PAC file based re-direction to protect traditional endpoints. Integrating SEP with the Web Security Service extends the security profile to the network level.

WSS provides four SEP methods. This topic provides conceptual information to help you determine which is the most appropriate for your network, then provides links to topics that provide best practices and recommended values for configuring a VPN tunnel.

- If you need to understand the methods before deciding, continue reading the following concept sections.
- If you know what deployment you require, select a link to the configuration topic.
    - "Connectivity: WSS-SEP with Captive Portal" on page 30
    - "Connectivity: WSS-SEP-WTR With Seamless Identification" on page 36
    - "Connectivity: WSS-SEP-NTR With Seamless Identification" on page 43
    - "Connectivity: WSS-SEP Roaming SAML" on page 47

About the SEP Client Benefits

WSS-SEP occurs through the Proxy Auto Configuration (PAC) File. SEP updates the proxy settings for the operating system and browsers to point to a PAC file URL published by the WSS PFMS. The PAC file contains rules about what proxy actions to take for different URLs. When a client application that supports PAC file sends a web request, the PAC file rules instruct the application whether to proxy the request to WSS or send the request out directly.

Based on the predefined configuration, the WSS proxy redirects, allows, or blocks the traffic.

- SEP focuses on endpoint detection and remediation.
  - Enforces rule-based security on devices, whether remote or behind a corporate firewall.
  - Leverages a policy-based approach to enforce security on your devices.
  - Detects, identifies, blocks, and remediates threats and other security risks on the client device.
- SEP provides tamper-proof settings. It also installs the WSS certificate on the endpoint (if selected by policy). The client-side control, when allowed by a SEP Manager administrator, can help IT to troubleshoot issues.
- Authentication—The Auth Connector is required.

Why Select This Method?

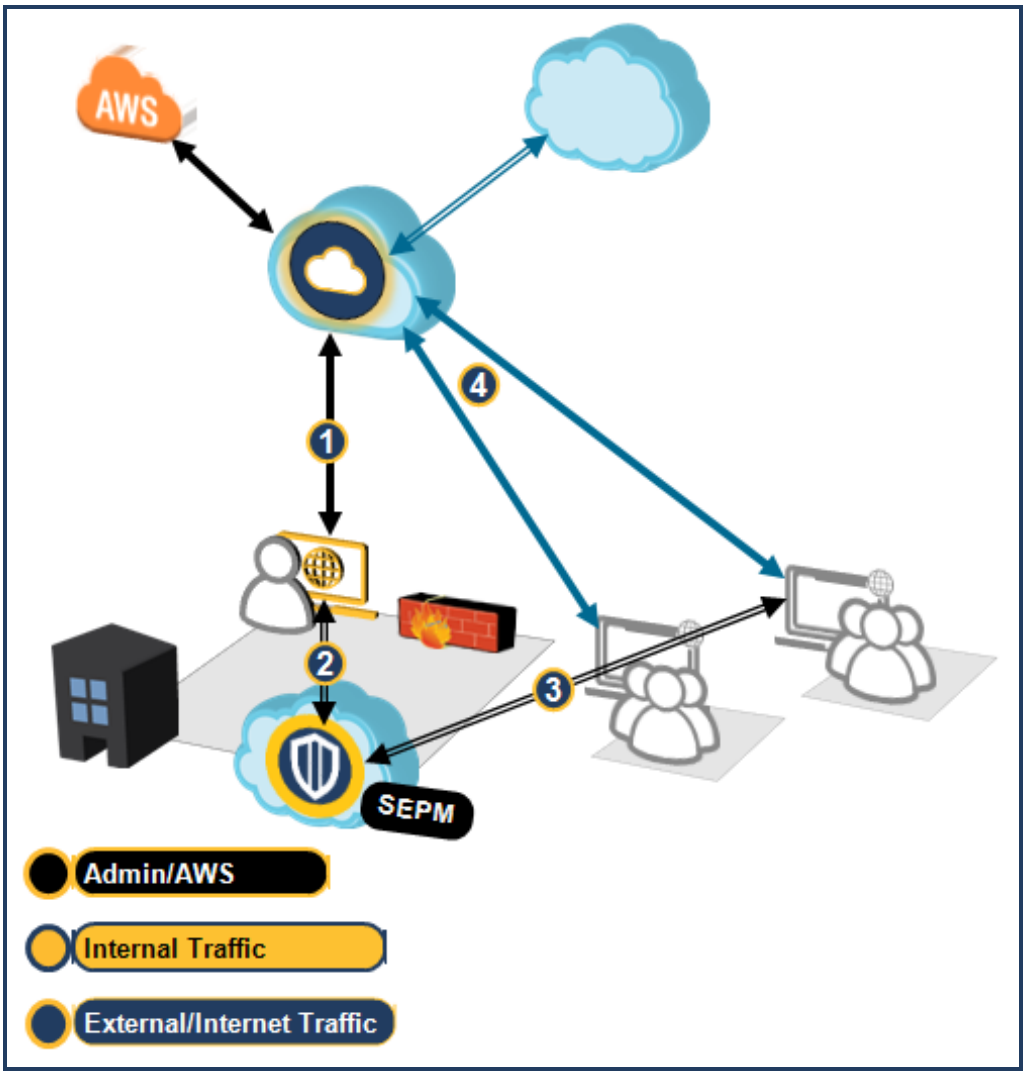
Benefits—

- You already have clients with the SEP solution and you want to extend from just local protection to network protection.
- Your environment has infrastructure and IP address space.
- You do not want to install an agent.

Select another method if—

- Your network egress is not a static IP address or it requires traversing a NAT devices.

Sample WSS-SEP with Captive Portal Topography



1–The Admin uses the WSS portal to create custom a PAC file –possibly providing custom bypassing of specific servers–and associates it with an Explicit Proxy Location.

2–The Admin accesses the SEP Manager and configures Web Traffic Redirection (WTR), which includes adding the generated PAC file.

3–SEP Manager distributes the security policy, including the PAC file URL, to the SEP endpoints. The SEP agent receives the security policy and configures the proxy settings for system and browsers.

4–The PAC file proxies all internet-bound traffic to the nearest WSS for web use and security policy processing.

Why Select This Method?

Benefits–

- Used in conjunction with PFMS, the SEP client can dynamically update the PAC file on the endpoint's browser. This feature also allows you to maintain more than one PAC file; for example, for various locations, groups, and so on.
- Your network egress is not a static IP address or it requires traversing NAT devices.

Select another method if–

- Your network egress is not a static IP address or it requires traversing a NAT devices.

Used in conjunction with the PFMS, the SEP client can dynamically update the PAC file on the endpoint's browser. This feature also allows you to maintain more than one PAC file; for example, for various locations, groups, and so on.

Is this the method you require?

- "Connectivity: WSS-SEP with Captive Portal" on page 30.

About WSS-SEP-WTR/NTR–Web or Network Redirection with Seamless Identification

This method requires an integration token that you generate in your WSS portal. The token is entered into the SEP Manager, which then pushes the integration out to the SEP clients. When the employee logs in to their system, the SEP client initiates a secure connection (with a session key and a pre-shared key (PSK)) to WSS. The SEP client then provides an assertion to WSS. The assertion contains the user identity and other information about the endpoint, such as the OS version. This *seamless identification* means employees do not have to re-login again when accessing the internet through Captive/Roaming Captive Portal. This allows for per-user policy to be applied to traffic and also provides risky client context to WSS for logging and reporting. Seamless Identification also prevents issues related to Cross-Origin-Resource-Sharing (CORS).

If the seamless identification is disabled or fails for any reason, user identity is not automatically provided. Authentication reverts to a backup method configured for that location (Captive Portal if enabled or Roaming Captive Portal).

Connection Methods

- WSS-SEP-WTR–Leverage the WSS PFMS with the SEP Web Traffic Redirection (WTR) option in SEP Manager.
- WSS-SEP-NTR–Embeds and deploys selective WSS Agent technology into SEP. This yields the benefits of the full Network Traffic Redirection (NTR) and captures non-proxy applications. You can select what is captured by the agent. This method is beneficial if SEP clients frequently change from one network to another. The tunnel method provides heightened security by encrypting traffic between the endpoint and the data center.

Authentication Support

- **Auth Connector**–It is possible that client systems can belong to different Active Directory domains or even different forests, which means WSS cannot discern the proper group. Therefore, the Auth Connector is required for group-based policies.
- **SAML**–SEP with Seamless Identification supports Roaming SAML (WSS-SEP-WTR only at this time). Adding a WSS-generated token to the SEP Manager establishes tenancy, which is required for the SAML IdP.

Why Select This Method?

Benefits–

- Securely transfers the logged-in user ID and device information to WSS or SAML IdP, thus Captive Portal is not required.

Is this the method you require?

- "Connectivity: WSS-SEP-WTR With Seamless Identification" on page 36.
- "Connectivity: WSS-SEP-NTR With Seamless Identification" on page 43
- "Connectivity: WSS-SEP Roaming SAML" on page 47.

Connectivity: WSS-SEP with Captive Portal

Redirect traffic from Symantec Endpoint Protection (SEP) clients to the Web Security Service to extend from local to network-level protection.

- See "Connectivity: About Symantec Endpoint Protection" on page 24 for more information about the solution.

Technical Requirements

- Admin access to an WSS account.
- Admin access to SEP Manager.
- SEP client 14.2+ Windows and MAC clients.
- Captive Portal–Employees must log in to the Captive or Roaming Captive Portal. This method requires the on-premises Auth Connector integration.
- You must backup the client proxy settings because the new SEP install erases them (Symantec is investigating this issue). Restore the settings after installing SEP.
- Before installing, verify no listener on `TCP 2968`.
- Firewall rule: Open port `8080`.
- Supported browsers:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Microsoft Internet Explorer 9 through 11
  - Mozilla Firefox
- If you plan to use the PAC File Management Service (PFMS) in conjunction with SEP clients, you must run Norton LiveUpdate on the client to obtain the required certificate.

  https://support.norton.com/sp/en/us/home/current/solutions/kb20080520094501EN_EndUserProfile_en_us

  ISSUE: If you encounter issues with Live Update, download the SSL Intercept cert from the WSS portal and manually install it on the test machine(s).

  - https://portal.threatpulse.com/docs/am/Solutions/ManagePolicy/SSL/ssl_chrome_cert_ta.htm
  - https://portal.threatpulse.com/docs/am/Solutions/ManagePolicy/SSL/ssl_ie_cert_ta.htm

Technical Limitation

- Some browsers do not support proxy settings change in already running sessions. Changing a policy state (enabled/disabled) requires browser restarts.

Best Practice

- Keep SEP clients updated to the latest versions; the updates provide critical fixes and performance enhancements.

Procedure—Enable Web Traffic Redirection on SEP

This procedure is for high-level reference. For greater detail, consult the documentation for your SEP/SEP Manager versions.

Prerequisite Step—Obtain a PAC File URL

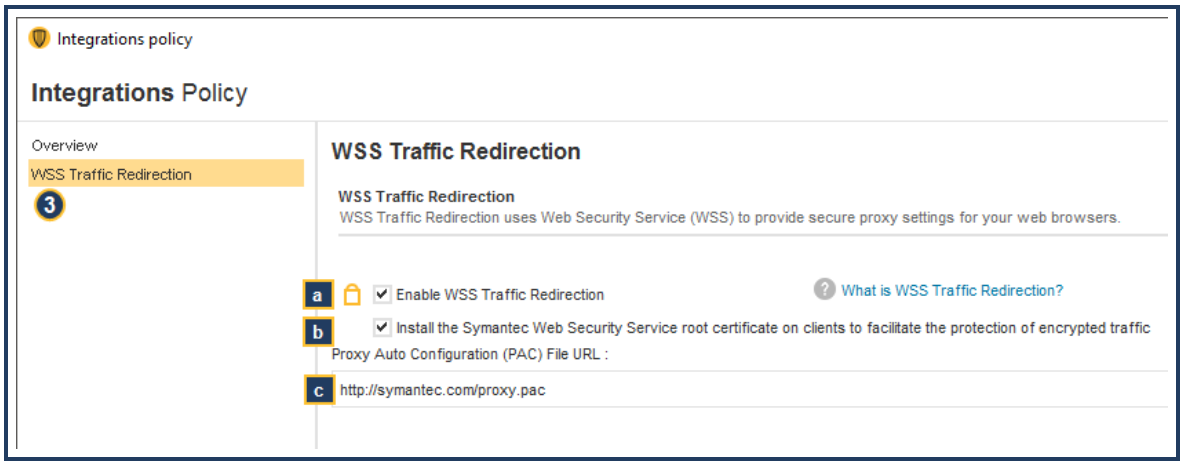
WSS-SEP requires a PAC File URL, which instructs the browsers on machines where to download the PAC File. Use the PAC File Management Service to create one for use with SEP connections. See "Connectivity: PAC File Management Service (EP)" on page 12.

Step 1—Obtain and Distribute the SEP Client

- If you already have a supported SEP client, proceed to **Step 2**.
- Consult the welcome letter you receive from Symantec regarding how to access the SEP Manager.
- SEP Client Downloads—https://knowledge.broadcom.com/external/article?legacyId=TECH103088.

Step 2—Enable WSS Traffic Redirection in the SEP Manager

1. Log in to the Symantec Endpoint Protection Manager.
2. Select **Policies > Integrations**.
3. Click **Add an Integrations Policy**. The SEP Manager displays the Integrations Policy dialog.
4. Select **WSS Traffic Redirection**.



a. Select **Enable WSS Traffic Redirection**.

b. Select **Install the...root certificate...**.

c. In the **PAC Auto Configuration (PAC) File URL** field, enter the URL obtained from the WSS.

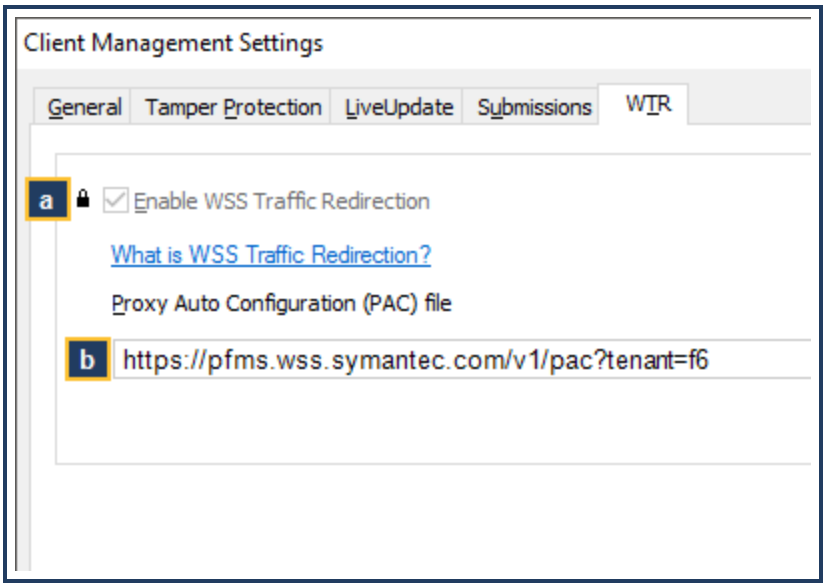
   Example format: `https://pfms.wss.symantec.com/v1/pac?tenant=f6104d245&pac=6027c20d1`.

d. Click **OK**.

> **Tip:** If you click **Mixed Control** under **Client User Interface Control Settings** and then click **Customize**, no option exists in the client user interface settings to configure WSS Traffic Redirection.

Verify WTR on the SEP Client

1. Access the SEP client on a system that is receiving this configuration.
2. Select the **WTR** tab.



a. **Enable WSS Traffic Redirection** is enabled.

b. **PAC file URL** is the same.

PAC File Management in SEP

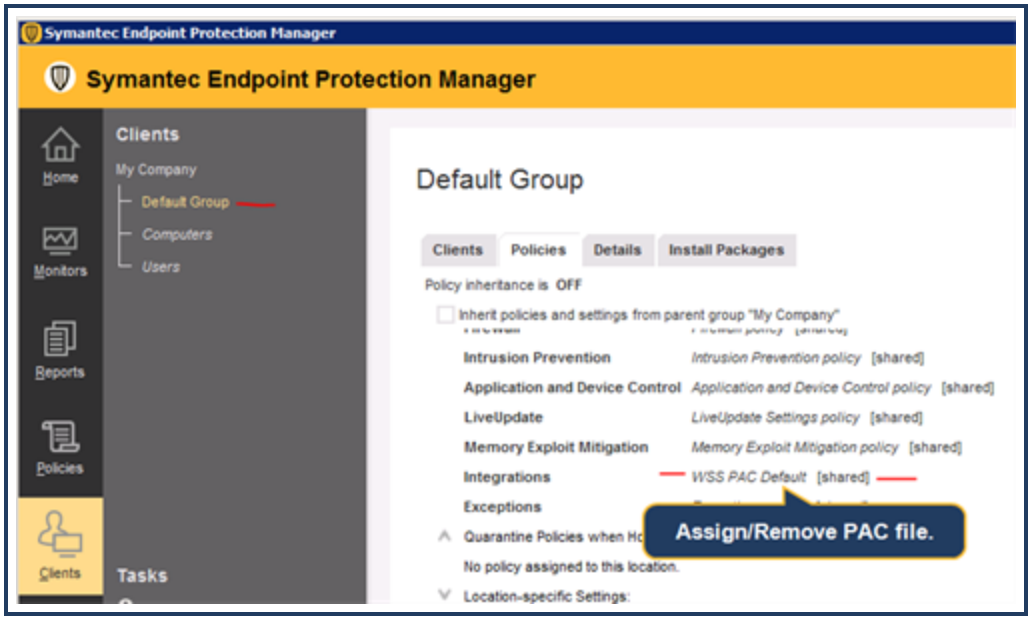
The SEP Manager provides additional admin options and options to further refine how users connect through the PAC files.

Assign a PAC File to Specific Assets

The SEP Manager allows you to select specific groups, client systems, and users. For IE and Chrome, the PAC files are then managed and inserted into the browsers (check the respective browser PAC settings).

1. In the SEP Manager, select **Clients**. There are three sub-categories: **Default Group**, **Computers**, and **Users**.
2. Each group contains a series of tabs.
    - **Clients**–Specify the user systems in the group.

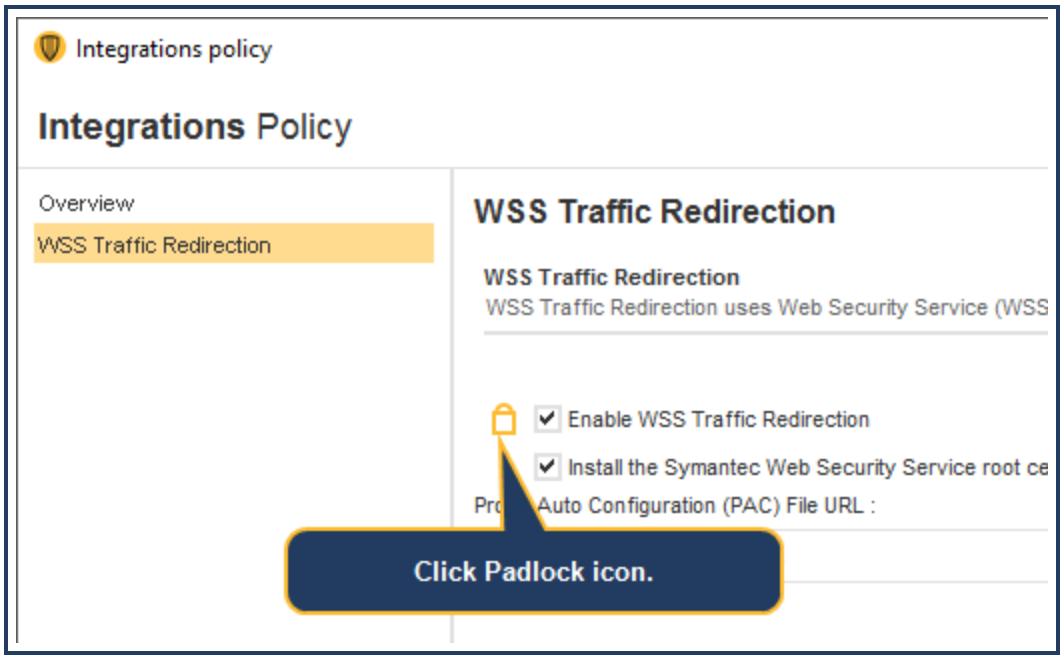
- **Policies**–Assign or remove the WSS PAC file.



Give Users the Ability to Turn the Service On or Off

Allow specific users and SEP groups the ability to turn the service on and off. For example, a specific consulting group requires the ability to turn off these settings; however, a help desk employee cannot turn off these settings.

On the integration policy created in **Step 3** (**Policy > Integrations**), the interface displays a gold padlock icon.



The gold padlock icon enables or disables the end user ability to turn on or off the WSS redirection settings. By default, the policy is locked, which means users cannot disable the service. Click the padlock (which switches to an unlocked icon) to allow users to disable connection to the service on their systems.

You can review all enable/disable activities on the **Monitors > Logs** SEP Manager page.

Take Policy Offline

You can disable the policy for all clients assigned Integrations Policy. Perhaps you have a need to troubleshoot some policy and don't want employee productivity to be impacted.

1. On the integration policy screen, click **Overview**.
2. Clear the **Enable** this policy option.

The next time SEP connects to the management server, it receives the instruction. If you change policy and re-enable it, the same occurs. Upon the next management server connection, the client receives the policy.

Connectivity: WSS-SEP-WTR With Seamless Identification

Redirect traffic from Symantec Endpoint Protection (SEP) clients to the Web Security Service to extend from local to network-level protection. This topic provides the information for a fixed-location that uses SEP Web Traffic Redirection (WTR), which requires a PAC File.

- See "Connectivity: About Symantec Endpoint Protection" on page 24 for more information about the solution.

Technical Requirements

- SEP 14.2+ is required for this feature.
- Requires an Explicit Proxy Location defined in **Connectivity > PAC Files**. The examples in this procedure use a location named **PAC-SA**.
- Authentication method–

  The Seamless Identification feature securely transfers the logged-in user ID and device information to WSS, thus Captive Portal is not required. However, you can enable Captive Portal or Roaming Captive Portal for backup authentication method should it become disabled or fail for any reason. This method supplies only the individual user information. To perform group-based policy, the Auth Connector is still required.
- Verify that your WSS portal is *not* configured to bypass `client-id.wss.symantec.com` or any domains that could contain `client-id.wss.symantec.com`.
- If you plan to use the PAC File Management Service (PFMS) in conjunction with SEP clients, you must run Norton LiveUpdate on the client to obtain the required certificate.

  https://support.norton.com/sp/en/us/home/current/solutions/kb20080520094501EN_EndUserProfile_en_us

  ISSUE: If you encounter issues with Live Update, download the SSL Intercept cert from the WSS portal and manually install it on the test machine(s).

  - https://portal.threatpulse.com/docs/am/Solutions/ManagePolicy/SSL/ssl_chrome_cert_ta.htm
  - https://portal.threatpulse.com/docs/am/Solutions/ManagePolicy/SSL/ssl_ie_cert_ta.htm
- Supported browsers:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Microsoft Internet Explorer 9 through 11
  - Mozilla Firefox

Technical Limitations

- WSS-SEP does not support remote logins if:
  - The client is not in the domain tied with the Auth Connector;
  - And policies based on groups exist in the policy editor.

Best Practice

- Keep SEP clients updated to the latest versions, which provide critical fixes and performance enhancements.

Procedure—Enable Web Traffic Redirection and Seamless Identification on SEP

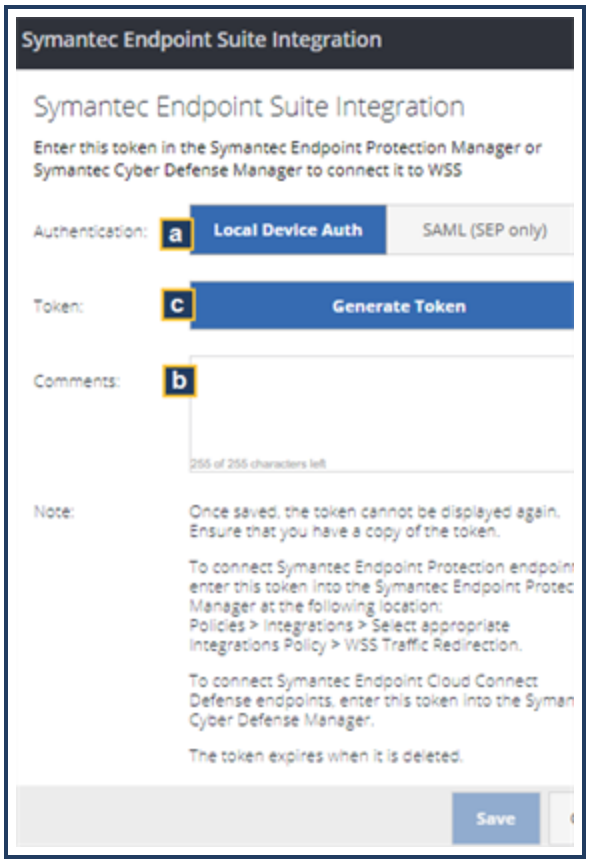
Step 1—Obtain and Distribute the SEP Client (SEP 14.2+)

- If you already have a supported SEP Client, proceed to **Step 2**.
- Consult the welcome letter you receive from Symantec regarding how to access the SEP Manager.
- SEP Client Downloads—https://knowledge.broadcom.com/external/article?legacyId=TECH103088.

Step 2—Obtain an Integration Token

For SEP clients to securely forward user ID and client-context information to the WSS, you must generate an integration token to be entered in SEP Manager.

1. In the WSS portal, navigate to **Connectivity > Symantec Endpoint Protection**.
2. Click **New Token**.



a. Verify that **Local Device Authentication** is selected.

b. (Optional) Enter a **Comment** to reference the purpose of this token.

c. Click **Generate Token**. WSS generates the randomized token.

d. **Copy** or record the token.

e. Click **Save**.

Step 3–Obtain a PAC URL

1. In the WSS portal, navigate to **Connectivity > PAC Files**.
2. Click **New File**. The portal switches to the PAC File Editor.

a. **Name** the PAC file.

b. (Optional) **Describe** the purpose of this PAC file.

c. **Include WSS Bypass** adds any IP addresses or domains that were previously added to the portal bypass lists. You can click the expander to view those entries; however, you cannot edit those entries here.

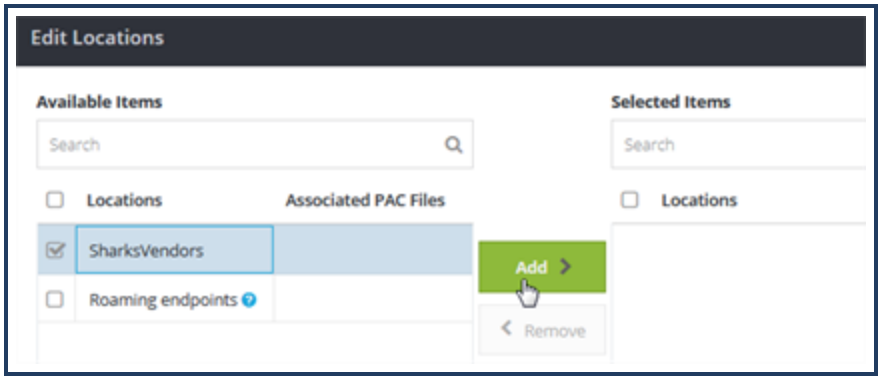
d. **Include Office 365 Bypass** adds all of the currently known Microsoft Office web application domains.

3. Click **Save**.

The portal generates an explicit PAC File URL. Copy this URL (click the Copy icon at the right-side of the field), as it is required during the SEP integration step.

4. Continuing with the example, click the **Locations** tab.

> **Tip:** You can have more than one location that uses the same PAC file.



a. Select a **Location** that is to connect through this PAC file. This example selects a previously added Explicit Proxy Location (named **PAC-SA**) created to test SEP integration.

> **Tip:** The **Roaming Endpoints** option applies the PAC file to all remote client (non-corporate network) connections.

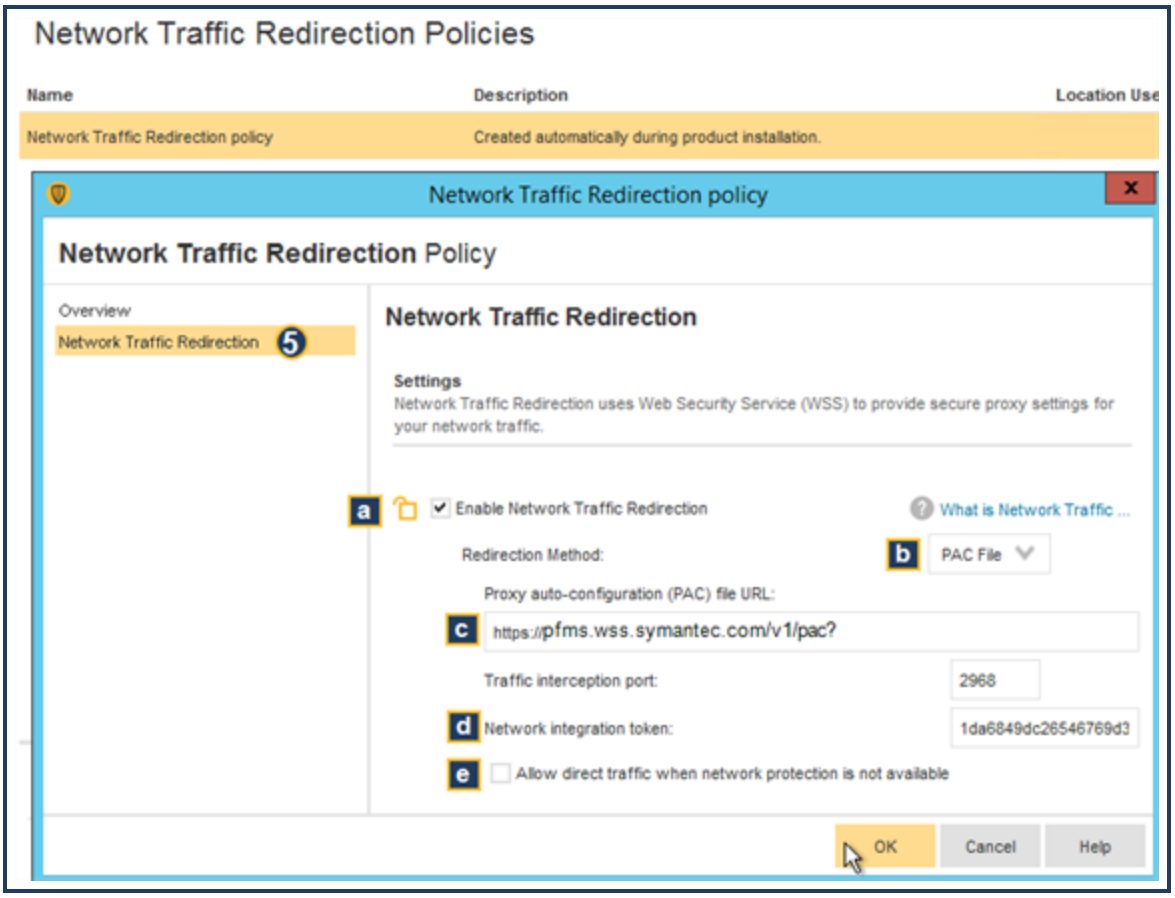
b. Click **Add** and **Save**.

5. Click the **PAC Files** link (or the Up arrow icon next to the PAC file name). The portal now displays the newly-created PAC file.

Step 4–Configure WTR in the SEP Manager

In the Symantec Endpoint Protection Manager, configure WSS Traffic Redirection (WTR).

1. Log in to the Symantec Endpoint Protection Manager.
2. Select **Policies > Network Traffic Redirection**.
3. Double-click **Network Traffic Redirection policy**. The SEP Manager displays the Network Traffic Redirection dialog.
4. On the **Overview** tab, verify that **Enable This Policy** is selected.
5. Select **Network Traffic Redirection**.



a. Select **Enable WSS Traffic Redirection**.

> **Tip:** The gold padlock icon enables or disables the end user ability to turn on or off the WSS Redirection settings. By default, the policy is locked, which means users cannot disable the service. Click the padlock (which switches to an unlocked icon) to allow users to disable connection to the service on their systems. You can review all enable/disable activities on the **Monitors > Logs** SEP Manager page.

b. From the **Redirection Method** drop-down, select **PAC File**.

c. In the **Proxy auto-configuration (PAC) file URL** field, enter the URL obtained from the WSS (in **Sub-Step 3.3** above).

   Example format: `https://pfms.wss.symantec.com/v1/pac?tenant=f6104d245&pac=6027c20d1.....`

d. In the **Network Integration Token** field, enter the token that you created in **Step 2**.

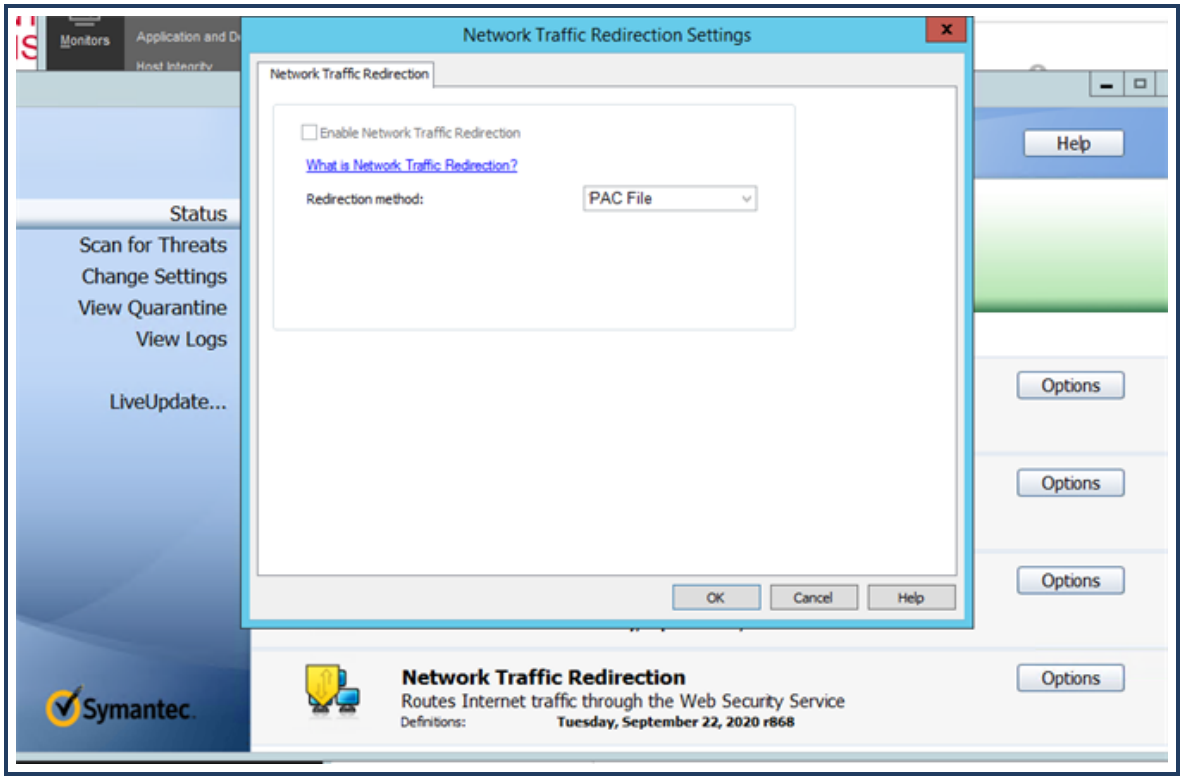
e. (Optional) Select **Allow direct traffic when network protection is not available** to allow the request to go continue should the PFMS not be reachable. This option lowers security.

f. Click **OK**.

Step 5–(Optional) Verify the SEP Client Settings

On a test system with SEP client installed with Admin rights, you can review the settings.

1. Access the SEP client application.
2. On the **Status** page, click **Options** for **Network Traffic Redirection**.



- **Enable WSS Traffic Redirection**–This client has the feature enabled.
- **Redirection Method** is **PAC File**.

Additional Support

- Refer to the Symantec SEP documentation.

Connectivity: WSS-SEP-NTR With Seamless Identification

Redirect traffic from Symantec Endpoint Protection (SEP) clients to the Web Security Service to extend from local to network-level protection. This topic provides the information required for enabling Network Traffic Redirection (NTR) in SEP Manager.

- See "Connectivity: About Symantec Endpoint Protection" on page 24 for more information about the solution.

Technical Requirements

- SEP 14.3-RU1 is required for this feature.
- Authentication method–

  The Seamless Identification feature securely transfers the logged-in user ID and device information to WSS, thus Captive Portal is not required. However, you can enable Captive Portal or Roaming Captive Portal for backup authentication method should Seamless Identification become disabled or fail for any reason. This method supplies only the individual user information. To perform group-based policy, the Auth Connector is still required.
- Verify that your WSS portal is *not* configured to bypass `client-id.wss.symantec.com` or any domains that could contain `client-id.wss.symantec.com`.

Technical Limitation

- WSS-SEP does not support remote logins if:
  - The client is not in the domain tied with the Auth Connector;
  - And policies based on groups exist in the policy editor.

Best Practice

- Keep SEP clients updated to the latest versions, which provide critical fixes and performance enhancements.

Procedure–Enable Web Traffic Redirection and Seamless Identification on SEP

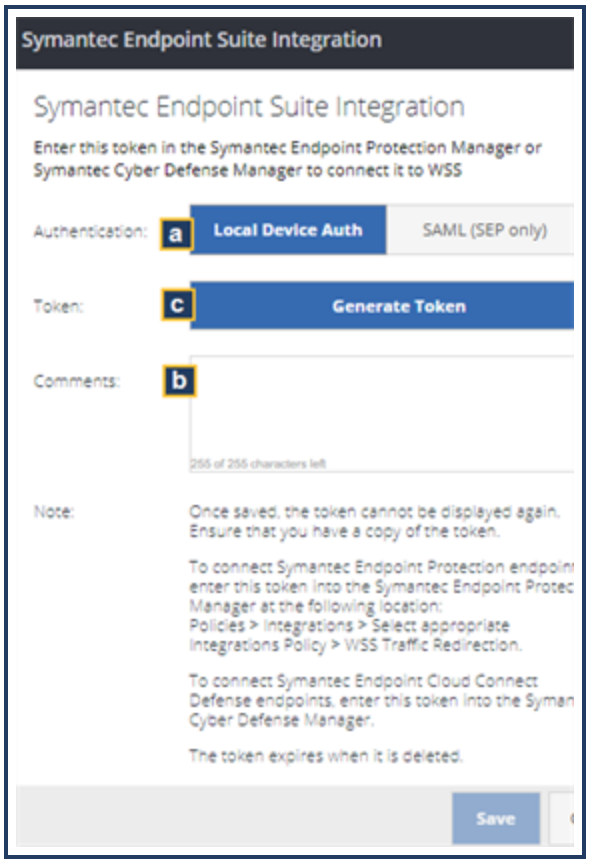
Step 1–Obtain and distribute the SEP client (SEP 14.3-RU1).

- If you already have a supported SEP Client, proceed to **Step 2**.
- Consult the welcome letter you received from Symantec regarding how to access the SEP Manager.
- SEP Client Downloads–https://knowledge.broadcom.com/external/article?legacyId=TECH103088.

Step 2–Obtain an Integration Token.

For SEP clients to securely forward user ID and client-context information to WSS, you must generate an integration token to be entered in SEP Manager.

1. In the WSS portal, navigate to **Connectivity > Symantec Endpoint Protection**.
2. Click **New Token**.



a. Verify that **Local Device Authentication** is selected.

b. (Optional) Enter a **Comment** to reference the purpose of this token.

c. Click **Generate Token**. The WSS generates the randomized token.

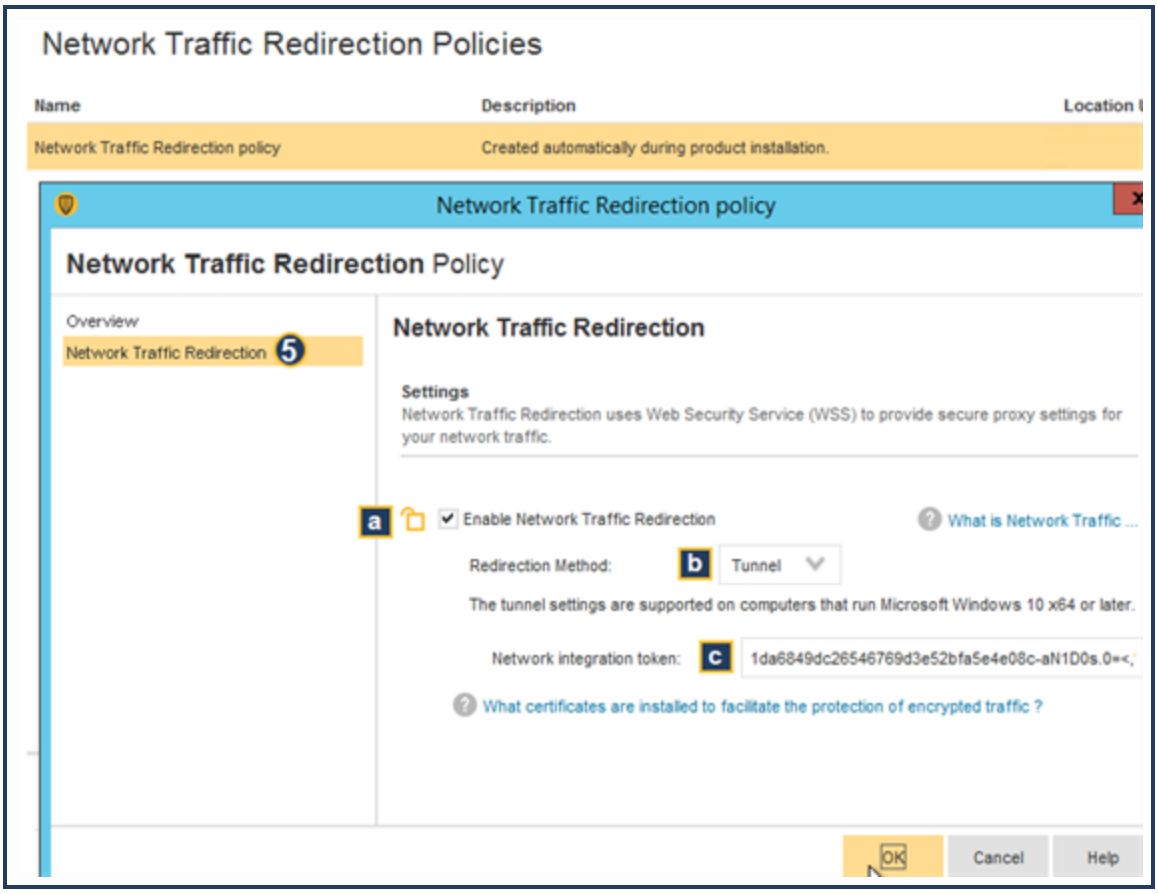
d. **Copy** or record the token.

e. Click **Save**.

Step 3–Configure NTR in the SEP Manager.

In the Symantec Endpoint Protection Manager, configure WSS Network Traffic Redirection (NTR).

1. Log in to the Symantec Endpoint Protection Manager.
2. Select **Policies > Network Traffic Redirection**.
3. Double-click **Network Traffic Redirection policy**. The SEP Manager displays the Network Traffic Redirection dialog.
4. On the **Overview** tab, verify that **Enable This Policy** is selected.
5. Select **Network Traffic Redirection**.



a. Select **Enable Network Traffic Redirection**.

> **Tip:** The gold padlock icon enables or disables the end user ability to turn the WSS Redirection settings on or off. By default, the policy is locked, which means users cannot disable the service. Click the padlock (which switches to an unlocked icon) to allow users to disable the connection to the service on their systems. You can review all enable/disable activities on the **Monitors > Logs** SEP Manager page.

b. From the **Redirection Method** drop-down, select **Tunnel**.

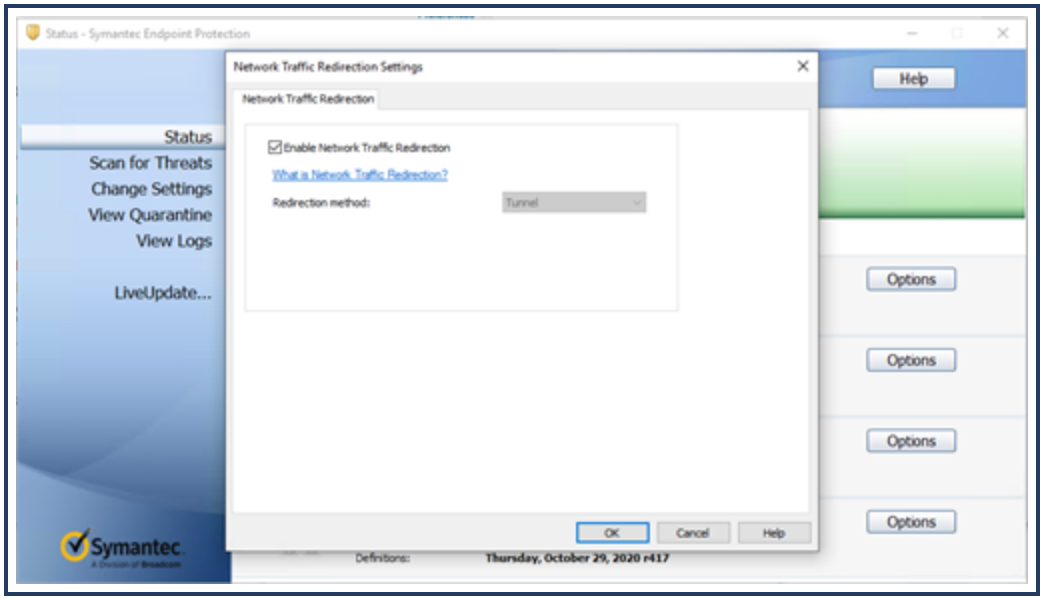
c. In the **Network Integration Token** field, enter the token that you created in **Step 2**.

d. Click **OK**.

Step 4–(Optional) Verify the SEP client Settings.

On a test system with a SEP client installed with Admin rights, you can review the settings.

1. Access the SEP client application.
2. On the **Status** page, click **Options** for **Network Traffic Redirection**.



   - **Enable WSS Traffic Redirection**–This client has the feature enabled.
   - **Redirection Method** is **Tunnel**.

Additional Support

- Refer to the Symantec SEP documentation.

Connectivity: WSS-SEP Roaming SAML

Redirect traffic from Symantec Endpoint Protection (SEP) clients to the Web Security Service to extend from protection to SAML-authenticated clients when not connecting through a corporate network. The Seamless Identification feature securely transfers the logged-in user ID and device information to the cloud-based or on-premises SAML Identity Provider (IdP). This method is a solution for roaming SEP clients because the SAML realm must receive the tenancy before authentication occurs; that is, client-to-IdP traffic cannot route through WSS.

- See "Connectivity: About Symantec Endpoint Protection" on page 24 for more information about the solution.

Technical Requirements

- SEP 14.2+ is required for this feature.
- Authentication method.
  - Your environment has a functioning SAML/IdP solution.
  - Allow `saml.threatpulse.net:8443`.
  - **IdP NOTE**–As the client to SAML IdP traffic cannot route through WSS because, you must add an entry to the PAC file to make the IdP traffic go direct.
    - The default SAML method is Cookie. CORS-issues are mitigated because the procedure includes generating and providing an integration token, which is included in the HTTP header.
- The IdP must have an internet-facing IP address.
- For traffic bypass best practices, consult the following KB article.
  - https://knowledge.broadcom.com/external/article?legacyId=TECH252765
- If you plan to use the PAC File Management Service (PFMS) in conjunction with SEP clients, you must run Norton LiveUpdate on the client to obtain the required certificate.

  https://support.norton.com/sp/en/us/home/current/solutions/kb20080520094501EN_EndUserProfile_en_us

  ISSUE: If you encounter issues with Live Update, download the SSL Intercept cert from the WSS portal and manually install it on the test machine(s).
  - http://portal.threatpulse.com/docs/sol/Solutions/ManagePolicy/SSL/ssl_chrome_cert_ta.htm
  - http://portal.threatpulse.com/docs/sol/Solutions/ManagePolicy/SSL/ssl_ie_cert_ta.htm
- Supported browsers:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge

- Microsoft Internet Explorer 9 through 11
- Mozilla Firefox

Technical Limitations

- Some browsers do not support proxy settings change in already running sessions. Changing a policy state (enabled/disabled) requires browser restarts.

Best Practice

- Keep SEP clients updated to the latest versions, which provide critical fixes and performance enhancements.

Procedure–Enable Web Traffic Redirection and Seamless Identification on SEP

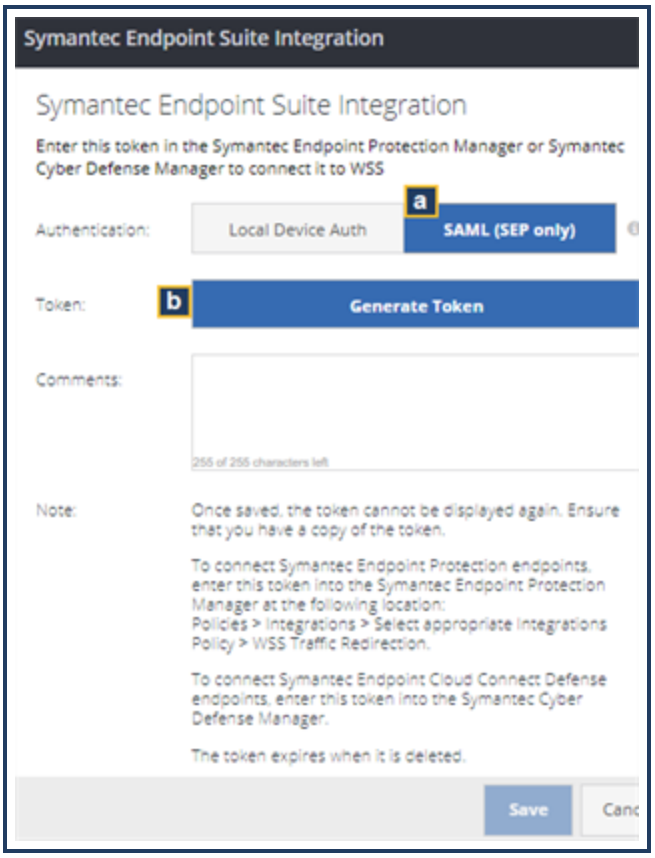
Step 1–Obtain and Distribute the SEP Client (SEP 14.2+)

- If you already have a supported SEP Client, proceed to **Step 2**.
- Consult the welcome letter you receive from Symantec regarding how to access the SEP Manager.
- SEP Client Downloads– https://knowledge.broadcom.com/external/article?legacyId=TECH103088.

Step 2–Obtain an Integration Token

For SEP clients to securely forward user ID and client-context information to the WSS, you must generate an integration token to be entered in SEP Manager.

1. In the WSS portal, navigate to **Connectivity > Symantec Endpoint Protection**.
2. Click **New Token**.



a. For **Authentication**, select **SAML (SEP only)**.

b. Click **Generate Token**. WSS generates the randomized token.

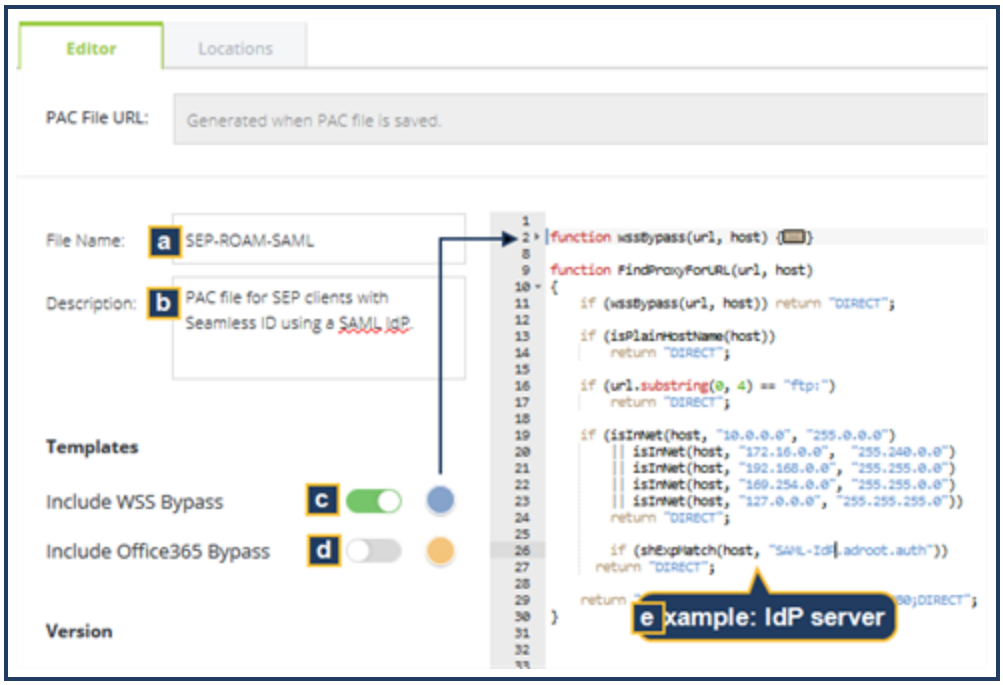
c. **Copy** the token to a local text file or email if another admin is to configure SEP Manager. (Click the copy icon at the end of the field.)

> **Tip:** Enter **Comments** to help future admins understand the token's role when viewed in the portal.

d. Click **Save**.

Step 3–Obtain a PAC URL

1. In the WSS portal, navigate to **Connectivity > PAC Files**.
2. Click **New File**. The portal switches to the PAC File Editor.



a. **Name** the PAC file.

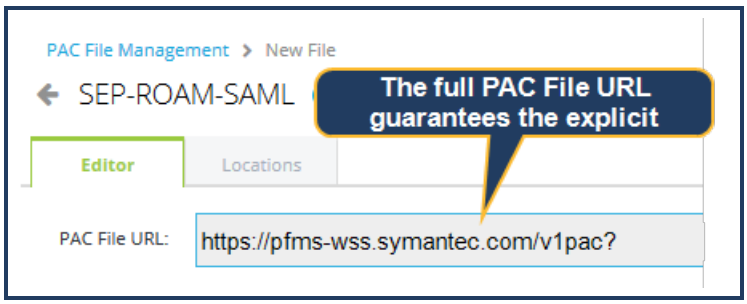
b. (Optional) **Describe** the purpose of this PAC file.

c. **Include WSS Bypass** adds any IP addresses or domains that were previously added to the portal bypass lists. You can click the expander to view those entries; however, you cannot edit those entries here.

d. **Include Office 365 Bypass** adds all of the currently known Microsoft Office web application domains.

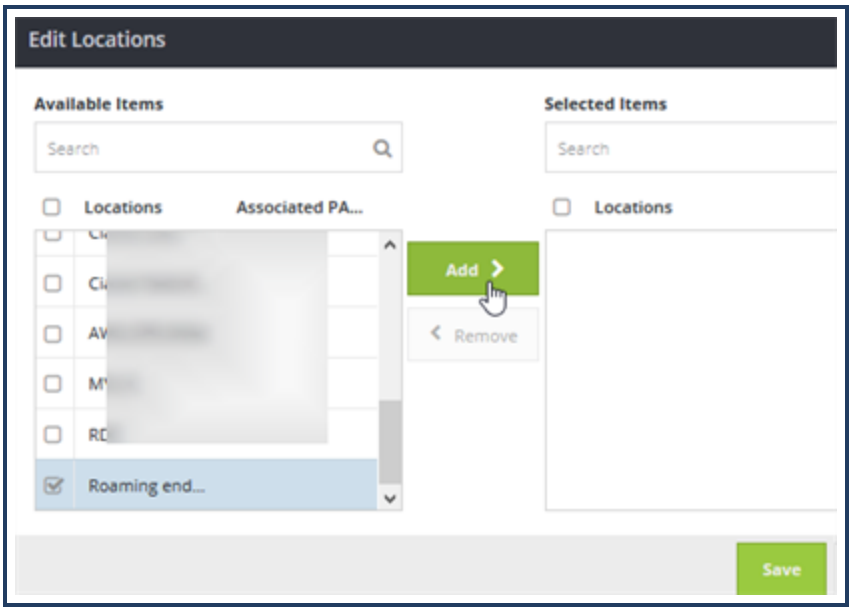
e. Add an entry to bypass the SAML IdP server.

3. Click **Save**.



The portal generates an explicit PAC File URL. Copy this URL (click the **Copy icon** at the right-side of the field), as it is required during the SEP Manager integration step.

4. Continuing with the example, click the **Locations** tab.



a. Select **Roaming Endpoints** and click **Add**.

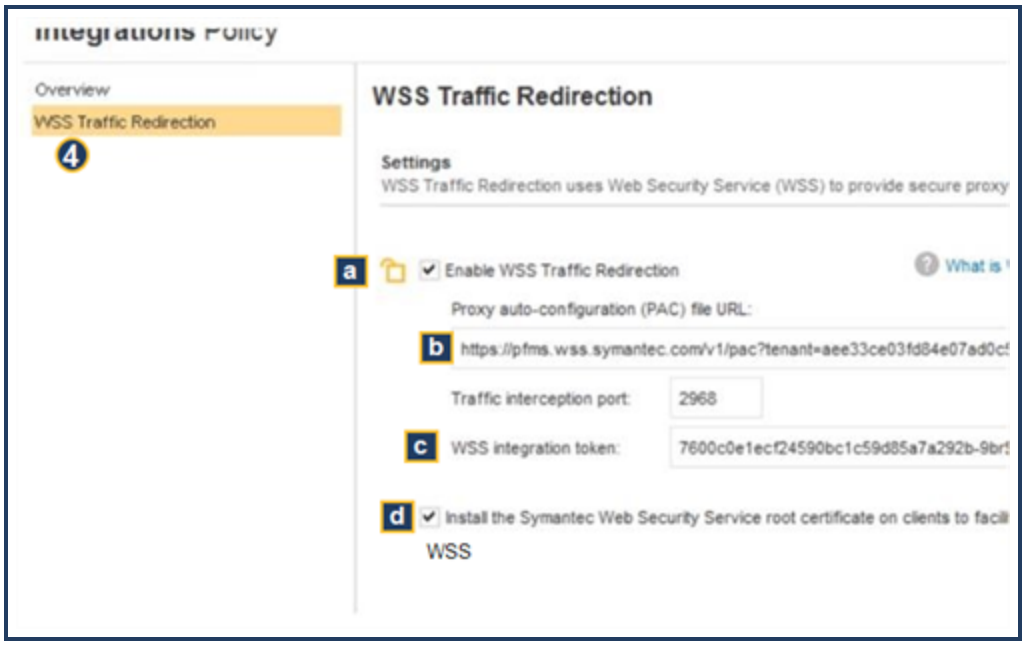
b. Click **Save**.

5. Click the **PAC Files** link (or the Up arrow icon next to the PAC file name). The portal now displays the newly-created PAC file.

Step 4—Configure WTR in the SEP Manager

In the Symantec Endpoint Protection Manager, configure WSS Traffic Redirection (WTR).

1. Log in to the Symantec Endpoint Protection Manager.
2. Select **Policies > Integrations**.
3. Click **Add an Integrations Policy**. The SEP Manager displays the Integrations Policy dialog.
4. On the **Overview** tab, verify that **Enable This Policy** is selected.
5. Select **WSS Traffic Redirection**.



a. Select **Enable WSS Traffic Redirection**.

b. In the **PAC Auto Configuration (PAC) File URL** field, enter the URL obtained from the WSS (in **Sub-Step 3.3** above; screenshot example format is not valid).

   Example format: `https://pfms.wss.symantec.com/v1/pac?tenant=f6104d245&pac=6027c20d1.....`.

c. In the **WSS Integration Token** field, enter the token that you created in **Step 2**.

d. Select **Install the...root certificate...**.

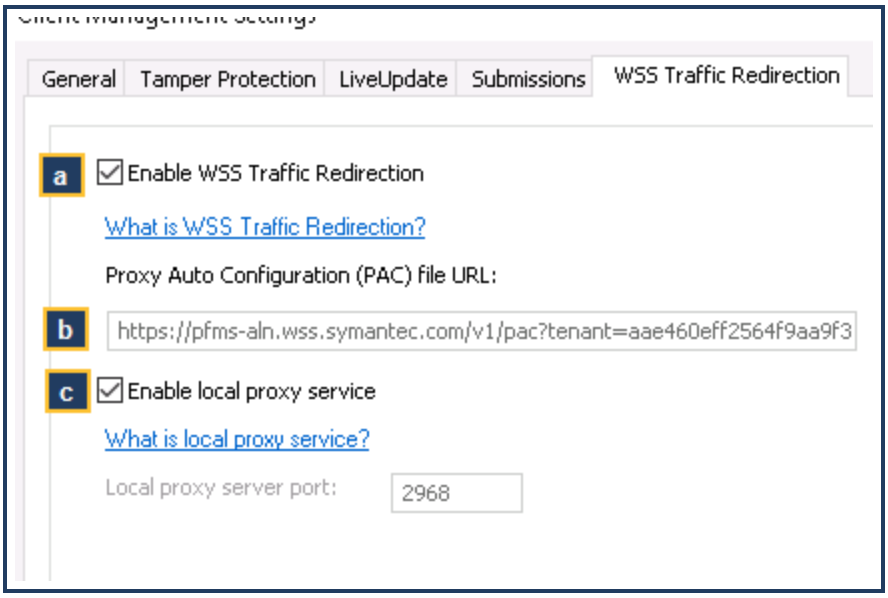
e. Click **OK**.

> **Tip:** The gold padlock icon enables or disables the end user ability to turn on or off the WSS Redirection settings. By default, the policy is locked, which means users cannot disable the service. Click the padlock (which switches to an unlocked icon) to allow users to disable connection to the service on their systems. You can review all enable/disable activities on the **Monitors > Logs** SEP Manager page.

Step 5–(Optional) Verify the SEP Client Settings

On a test system with SEP client installed with Admin rights, you can review the settings.

1. Access the SEP client application.
2. In the **Client Management** row, click **Configure Settings**.
3. Select the **WSS Traffic Redirection** tab.



a. **Enable WSS Traffic Redirection**–This client has the feature enabled.

b. The **PAC URL** is the same as in **Sub-Step 3.3** above.

c. **Enable Local Proxy Service**.

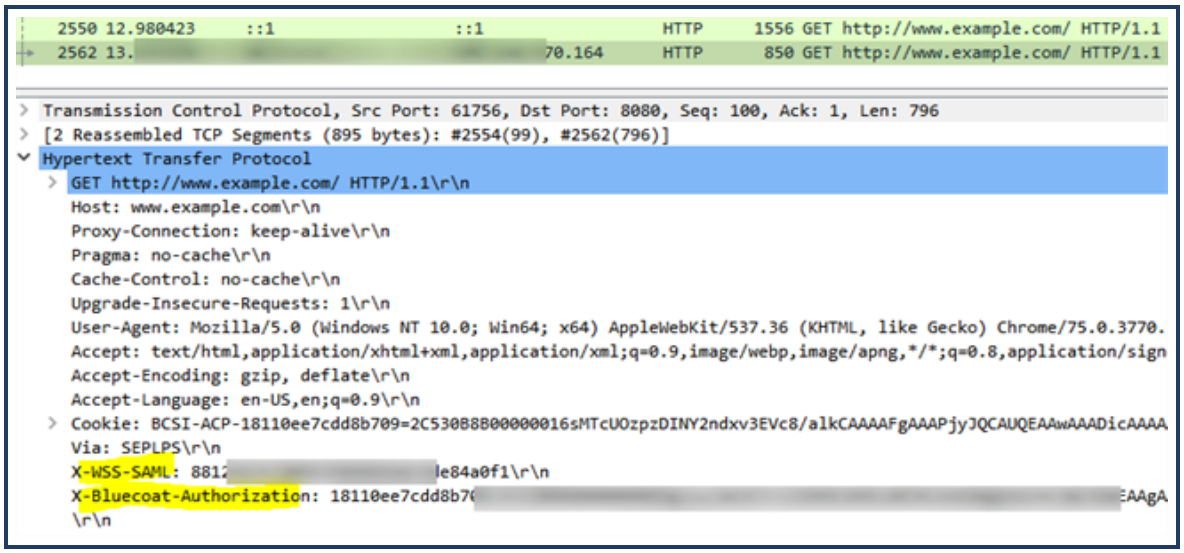
- **Disabled**–All web browser traffic uses the Symantec WSS PAC file URL. This option might be used during troubleshooting scenarios.
- **Enabled**–The recommended setting. All web browser traffic visits a locally cached PAC file.

> **Tip:** In any **Browser Settings** dialog, the PAC File displays the local proxy URL; not the WSS-generated PAC File URL.

d. Click **OK**.

Step 6–Verify Authentication/Troubleshoot

To verify configuration, use a client to connect. The SEP agent redirects to the SAML service (`saml.threatpulse.net:8443`), followed by the IdP server to authenticate. After authentication and the assertion is correctly validated by WSS, all subsequent requests include additional headers that WSS requires.



Additional Support

- Refer to the Symantec SEP documentation.

Prevent IP/Subnet From Routing to the Web Security Service

IMPORTANT–This topic only applies to locations that use the Explicit Proxy and WSS Agent Web Security Serviceconnectivity methods. All other access methods ignore any bypass domain configurations.

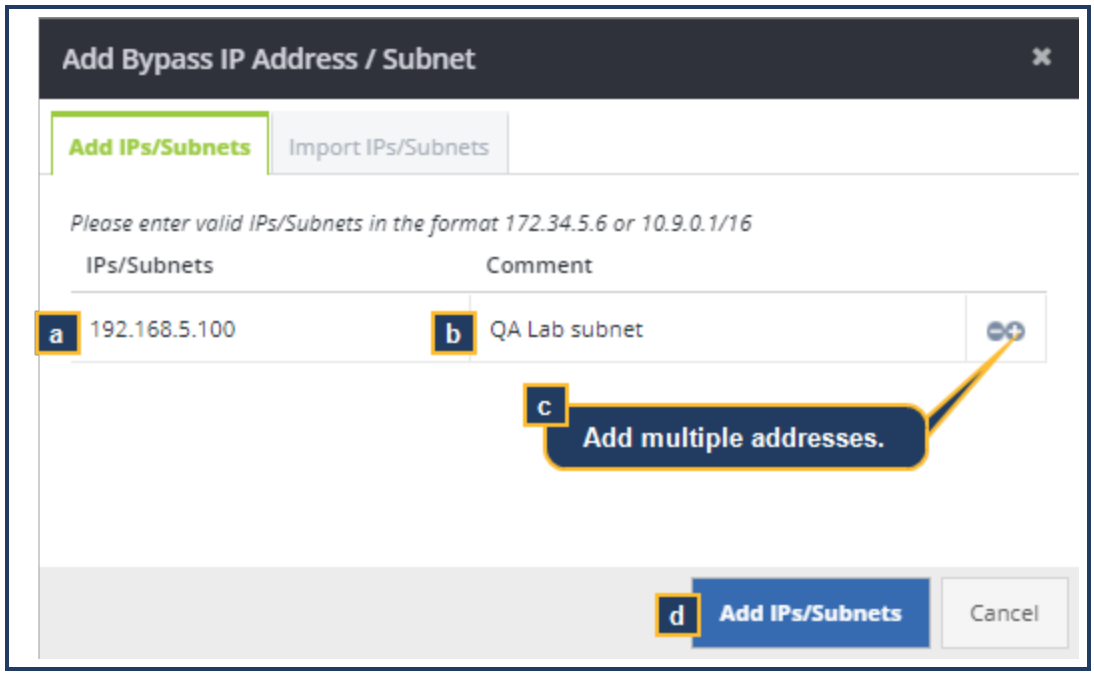
Some IP addresses or subnets do not require WSS processing. For example, you want to exclude test networks. Configure the service to ignore these connections.

Notes

- WSS allows an unlimited number of bypassed IP addresses/subnets.
- Each time that a WSS Agent reconnects to WSS (for example, a user who takes a laptop off campus and connects through a non-corporate network), the client checks against any updates to the list.

Procedure–Manually Add IP Addresses

1. Navigate to the **Policy > Bypassed Traffic > Bypassed IPs/Subnets** tab.
2. Click **Add**. The service displays a dialog.



a. Enter an **IP/Subnet**.

b. (Optional) Enter a **Comment**.

c. (Optional) Click the **+** icon to add another row for another entry.

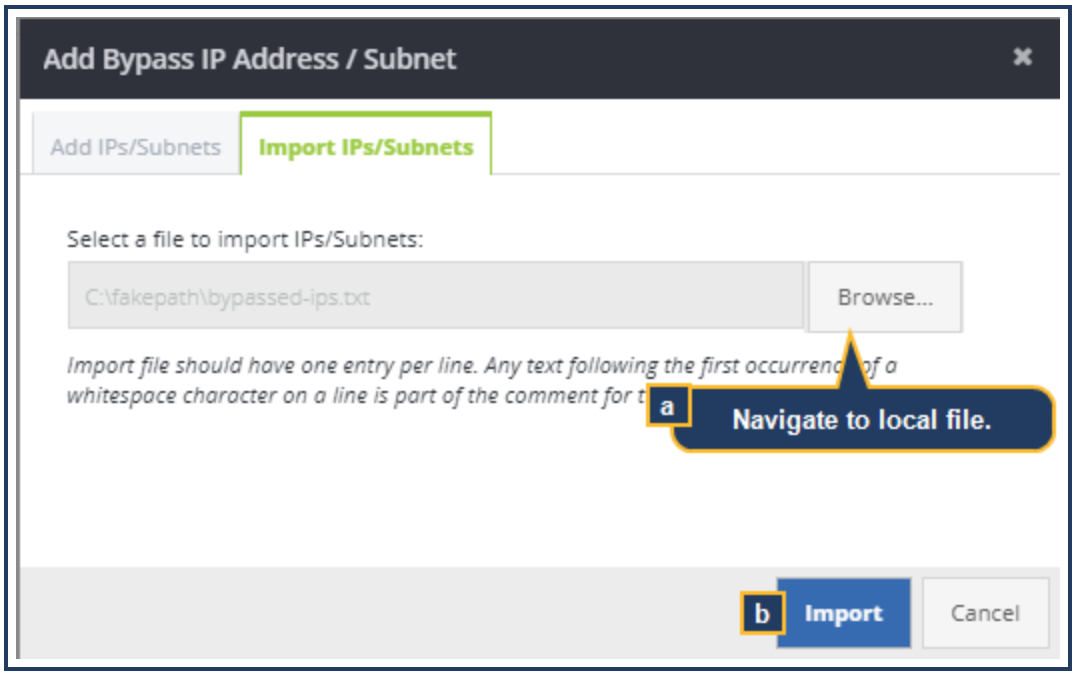
d. Click **Add IPs/Subnets**.

The new entries display in the tab view. You can edit or delete any entry from here.

Import IP Address Entries From a Saved List

This procedure assumes that you have already created an accessible list (text file) of IP addresses to be bypassed. Each entry in the file must be on its own line.

1. Navigate to the **Policy > Bypassed Traffic > Bypassed IPs/Subnets** tab.
2. Click **Add**. The service displays the Add Bypass IP Address/Subnet dialog.
3. Click **Import IPs/Subnets**.



a. Click **Browse**. The service displays the File Upload dialog. Navigate to the file location and **Open** it.

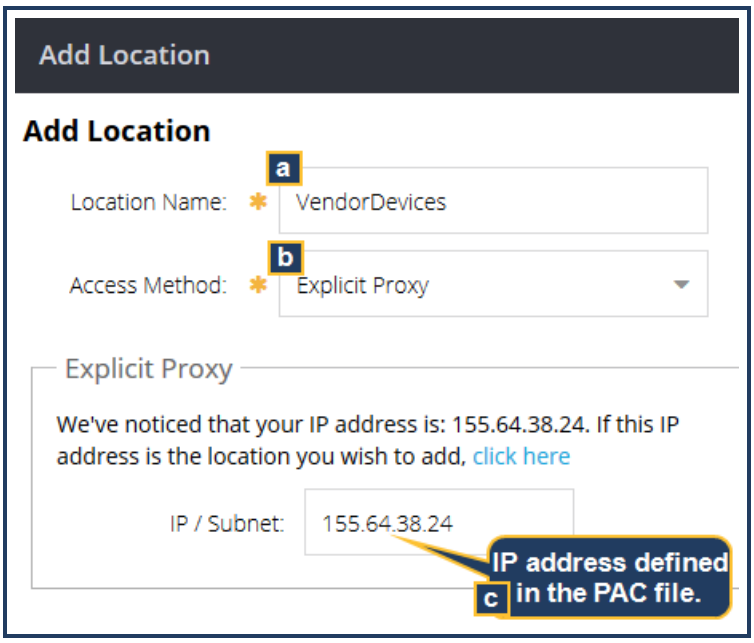
b. Click **Import**.

All of the new entries display in the tab view. You can edit or delete any entry from here.

Add an Explicit Proxy Location

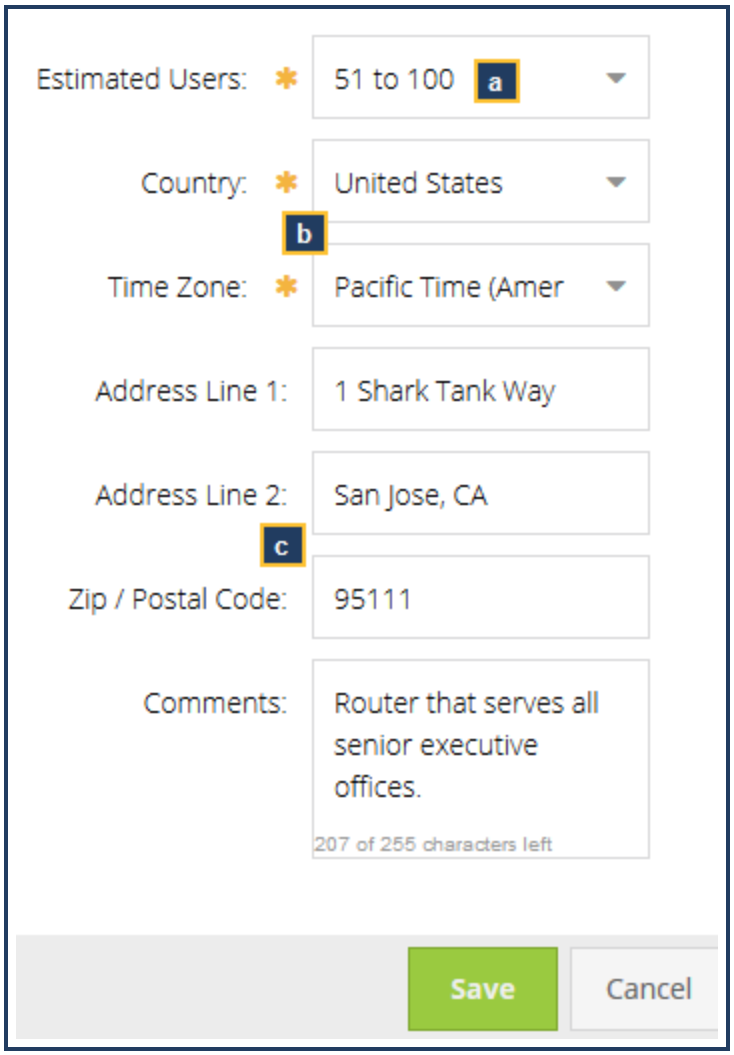
When configuring Explicit Proxy as the connectivity method, each gateway IP address defined in a PAC file requires an equivalent Symantec WSS location configuration.

1. Navigate to **Connectivity > Locations**.
2. Click **Add Location**.
3. Complete the **Location** dialog.



   a. **Name** the location. For example, use the fixed geographical location or organization name.
   b. Select **Explicit Proxy** as the **Access Method**.
   c. Enter the **IP/Subnet** that forwards web traffic to the WSS.

4. Enter resource and location information.



a. Select the **Estimated User** range that will be sending web requests through this gateway interface. Symantec uses this information to ensure proper resources.

b. Select a **Country** and **Time Zone**.

c. Fill out location information and enter comments (optional).

5. Click **Save**.

- The Firewall/VPN connectivity method supports Captive Portal.

Reference: Required Locations, Ports, and Protocols

Most Symantec Web Security Service connectivity and authentication methods require communication through specific ports, protocols, and locations. If you have firewall rules in place, use this reference to verify the ports and services that must be opened to allow connectivity.

Symantec Resource

`support.broadcom.com`	Provides knowledge base articles and support information.

Connectivity Methods

Method	Port(s)	Protocol	Resolves To

WSS portal access URL.
 	
IP addresses for administration of your WSS policy and configuration.
	443		`portal.threatpulse.com`
			
			`35.245.151.224`
			`34.82.146.64`
			
			Partner Portal Functionality
			
			`35.245.151.231`
			`34.82.146.71`

Firewall/VPN (IPsec)	UDP 500 (ISAKMP) UDP4500 if firewall is behind a NAT.	IPsec/ESP	
Proxy Forwarding	TCP 8080/8443 TCP 8084*	HTTP/HTTPS	`proxy.threatpulse.net` * Use when the forwarding host is configured for local SSL interception.

Method	Port(s)	Protocol	Resolves To
Explicit Proxy SEP PAC File Management System or Default PAC file	TCP 443 Default PAC file: TCP 8080		■ Firewall rules to allow PFMS access: ◦ By hostname: `pfms.wss.symantec.com` ◦ By IP Address: `34.120.17.44` The following addresses were used before November 7, 2020. They are acceptable for backup and failover until Symantec announces their decommissioned status. ◦ `35.155.165.94` ◦ `35.162.233.131` ◦ `52.21.20.251` ◦ `52.54.167.220` ◦ `199.247.42.187` ◦ `199.19.250.187` ■ The default PAC file directs browser traffic to `proxy.threatpulse.net`.

Explicit Over IPsec (Trans-Proxy)
 	
In this deployment method, all traffic is transmitted from your network to WSS. Two scenarios are common:
■ On-premises ProxySG appliance.
Explicit browser settings direct traffic to the proxy, which forwards that traffic to WSS through a configured IPsec tunnel.
■ Explicit settings in the browser pointed to `ep.threatpulse.net`.
Direct all firewall traffic destined for `ep.threatpulse.net` to WSS through your configured IPsec tunnel.
	UDP 500 (ISAKMP)
	
	UDP4500 if firewall is behind a NAT.
			`ep.threatpulse.net` resolves to `199.19.250.205`
			
			`ep-all.threatpulse.net` returns the following.
			
			`199.19.248.205`
			`199.19.250.205`
			`199.19.250.206`
			`199.19.250.207`
			`199.19.250.208`
			`199.19.250.209`
			`199.19.250.210`
			`199.19.250.211`
			`199.19.250.212`
			`199.19.250.213`
			`199.19.250.214`
			
			`ep-roundrobin.threatpulse.net` returns all IPs in a round-robin fashion; each two-minute Time-To-Live (TTL) period returns a different address.

Method	Port(s)	Protocol	Resolves To

WSS Agent	TCP/UDP 443	SSL	`ctc.threatpulse.com`
			`130.211.30.2`
			TCP port `443` for CTC requests and configuration.
			
			`portal.threatpulse.com`
			
			TCP port `443` for downloading updates.

Unified Agent	TCP/UDP 443
	
	Port 80
		TCP, SSL	`ctc.threatpulse.com`
			`130.211.30.2`
			TCP port `443` for CTC requests and configuration.
			
			`portal.threatpulse.com`
			
			TCP port `443` for downloading updates.
			
			TCP/UDP port `443` to `client.threatpulse.net` (DNS fallback)
			
			Port `80` for captive network information and updates.

Mobile (SEP-Mobile iOS/Android app)	UDP 500 (ISAKMP)
	
	UDP 4500 (NAT-T)
		IPSec/ESP	`mobility.threatpulse.com`
			
			`35.245.151.228`
			`34.82.146.68`

Universal Policy Enforcement (UPE)/Hybrid Policy			On-Premises Policy Management (`sgapi.threatpulse.com` and `sgapi.es.bluecoat.com`)
			
			`35.245.151.229`
			
			`34.82.146.69`
			
			If connectivity to WSS is behind stringent firewall rules, adjust the rules to allow traffic to pass to these IP addresses on port `443`.

Authentication

Auth Method	Port(s)	Protocol	Resolves To

Auth Connector	TCP 443	SSL	`auth.threatpulse.com`:
			
			`35.245.151.226`
			`34.82.146.65`
			
			`portal.threatpulse.com`:
			
			Tip: Additional Required Information: Reference: Authentication IP Addresses.

Auth Method	Port(s)	Protocol	Resolves To
Auth Connector to Active Directory	TCP 139, 445	SMB	
	TCP 389	LDAP	
	TCP 3268	ADSI LDAP	
	TCP 135	Location Services	
	TCP 88	Kerberos	
	49152-65535	TCP	Open when Auth Connector is installed on a new Windows Server 2012 Member rather than a Domain Controller.
AC-Logon App	TCP 80		Port `80` from all clients to the server.
SAML	TCP 8443 (over VPN)	Explicit and IPSec	`saml.threatpulse.net`
Roaming Captive Portal	TCP 8080		

Reference: Sample PAC File for Explicit Proxy

The following is sample text that makes up a Proxy Automatic Configuration (PAC) file from which Web browsers receive routing instructions. The PAC file redirects all non-internal traffic to the Symantec Web Security Service.

```
function FindProxyForURL(url, host) {
// If URL has no dots in host name, send traffic direct.
     if (isPlainHostName(host)) return "DIRECT";
// If specific URL needs to bypass proxy, send traffic direct.
     if (shExpMatch(url,"*bluecoat.com*") ||
     shExpMatch(url,"*cacheflow.com*"))
     return "DIRECT";
// If IP address is internal send direct.
     if (isInNet(host, "10.0.0.0", "255.0.0.0") ||
         isInNet(host, "172.16.0.0", "255.240.0.0") ||
         isInNet(host, "192.168.0.0", "255.255.0.0") ||
         isInNet(host, "216.52.23.0", "255.255.255.0") ||
         isInNet(host, "127.0.0.0", "255.255.255.0") ||
         isInNet(host, "192.41.79.240", "255.255.255.255"))
   return "DIRECT";
// All other traffic uses below proxies, in fail-over order.
       return "PROXY proxy.threatpulse.net:8080; DIRECT"; return "PROXY 199.19.250.164:8080; DIRECT"; }
```