

VMware Cloud Web Security Web Proxy Configuration Guide

November 2022

Table of Contents

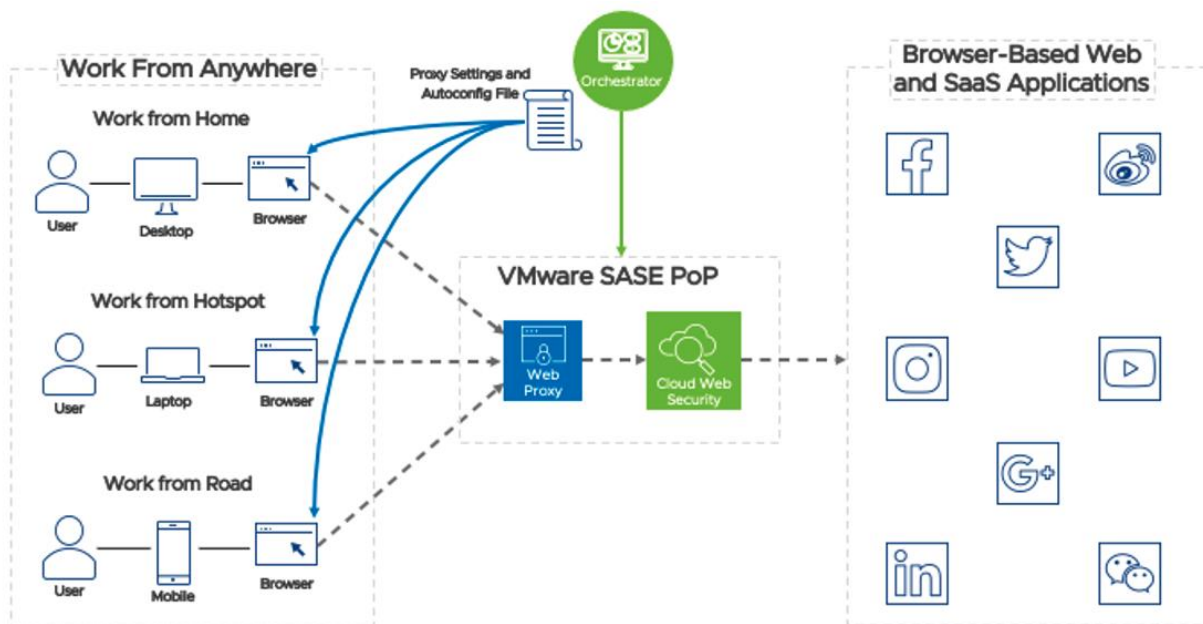
Overview	2
Prerequisites	2
SSL Termination Certificate	2
SAML Provider	5
Enabling SSO	6
Enable Web Proxy	8
PAC Files	11
Default PAC File	11
Custom PAC Files	12
1 PAC File Details	13
2 Proxy and Roaming Configuration	13
3 Default Proxy Bypass	15
4 Bypass Office 365	17
5 Custom Proxy Bypass	17
Host Configuration	18
Manual Proxy Settings	18
Automatic Proxy Settings	23
Troubleshooting	25
Single Sign On is Disabled	25

Overview

The VMware Cloud Web Security (CWS) Web Proxy is designed to enable the standalone consumption of CWS without the need for VMware SD-WAN or VMware Secure Access (SA). Any device with a modern browser that can support a network proxy configuration, either manually or automatically through a proxy auto-config (PAC) file, can have its Web traffic redirected to CWS for security inspection.

The Web Proxy Service is hosted by the VMware SASE PoP and enabled using the VMware Orchestrator. When a user enables the Web Proxy functionality in CWS, several things happen:

- A unique proxy URL is generated for the tenant
- A CWS policy is associated with the Web proxy service
- A default PAC file is generated by the system
- Custom PAC files can be created
- Orchestrator instructs the PoP to listen for proxied connections
- Proxy connections are service chained to CWS for inspection



Prerequisites

SSL Termination Certificate

When a user first connects to the Web Proxy, they are typically going to open their browser and navigate to some Website. And it is highly likely that user will navigate to an HTTPS site. The Web Proxy will need to perform an SSL intercept of this traffic and return a redirect to the

authentication service. While it is possible to instruct the user to accept the security warning it is better to have the VMware Root Certificate installed on the endpoint. The steps required to retrieve the root certificate and install it on a host is shown below.

Retrieval from Orchestrator

1. Open a Web browser and navigate to **VMware Cloud Orchestrator**

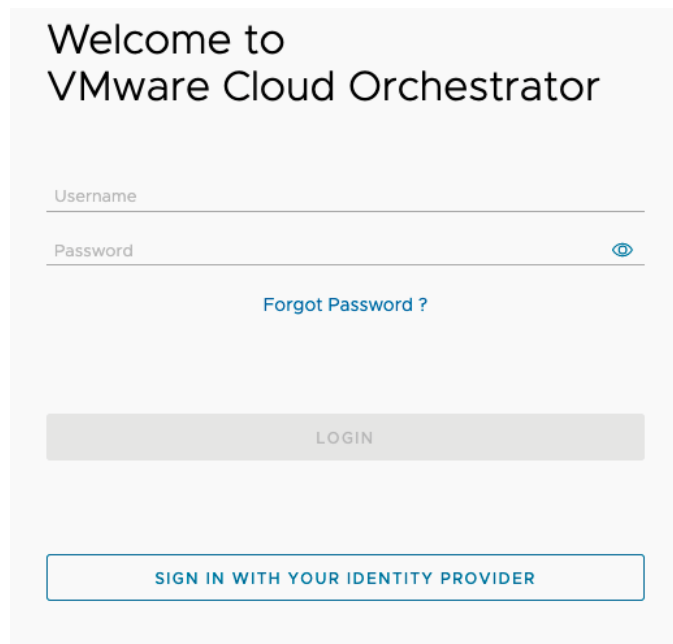


Figure: Orchestrator Login Page

2. From the top navigation bar go to **Enterprise Applications > Cloud Web Security**.

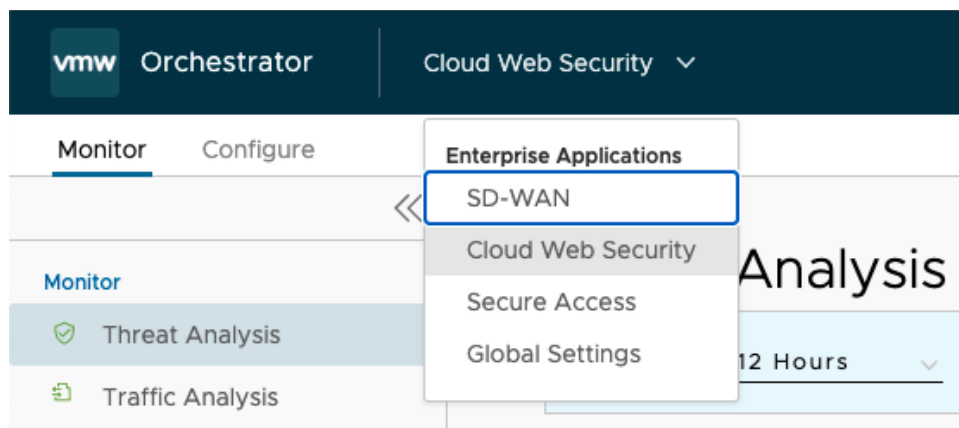


Figure: Orchestrator Enterprise Applications Navigation

3. Click on the **Configure** tab and select **Certificates > SSL Termination**.

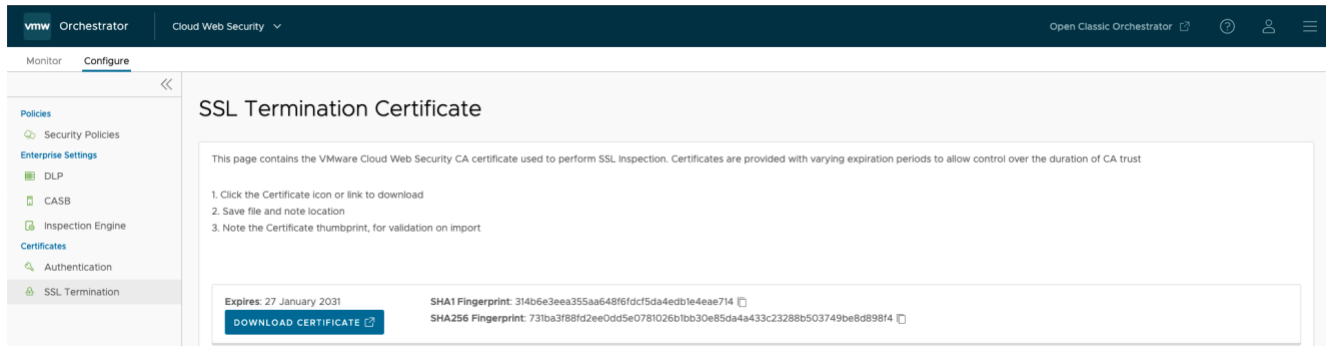


Figure: SSL Termination Certificate

4. Click on **Download Certificate** and save the file to the host machine.

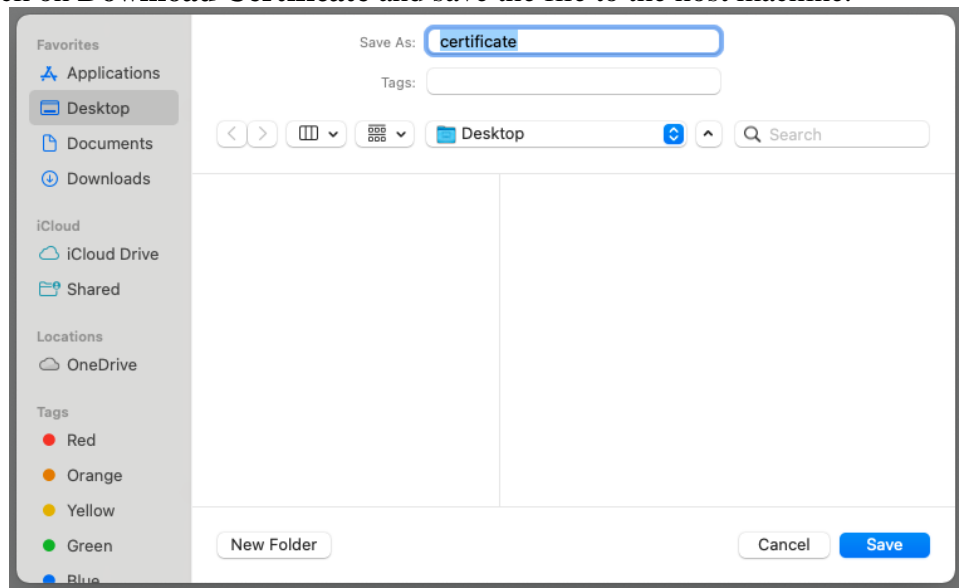


Figure: SSL Termination Certificate

5. (Optional) Use a utility, such as OpenSSL, to verify the downloaded root certificate has not been tampered with during transmission. This is done by computing the certificate fingerprint and comparing against what is shown in Orchestrator. For testing purposes, this step can be optional, but in production environments this should not be skipped.

OpenSSL Commands to Compute Certificate Fingerprint

```
$openssl x509 -noout -fingerprint -sha1 -inform pem -in certificate.cer
```

```
$openssl x509 -noout -fingerprint -sha256 -inform pem -in certificate.cer
```

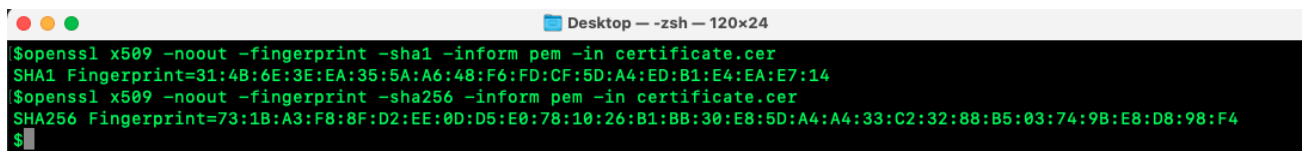


Figure: OpenSSL Commands in Terminal

SSL Termination Certificate

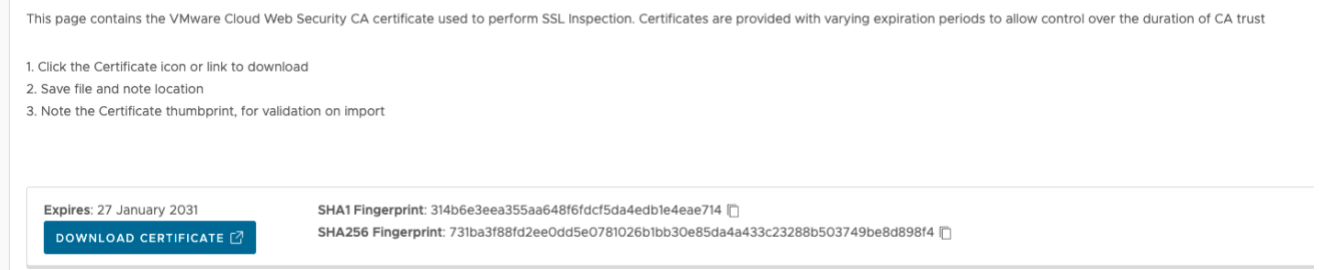


Figure: SSL Termination Certificate SHA1, SHA256 Fingerprints

Installation on Host(s)

The following external links provide instructions on how to install a private root certificate on common endpoint devices:

- [Microsoft Windows](#)
- [Apple OS X](#)
- [Apple iOS](#)
- [Android](#)

Alternatively, a root certificate can be installed at the browser level. This is useful for testing purposes, but not recommended for production use. The following external links provide instructions on how to install a private root certificate on popular Web browsers:

- [Google Chrome](#)
- [Mozilla Firefox](#)

SAML Provider

A SAML provider is necessary to authenticate users to the Cloud Web Security Proxy service. This requirement ensures only authenticated users are connected to Cloud Web Security and provides operational insight into the activity of those using the Web proxy.

Okta Example

The following example is based on using Okta as the identity provider (IdP) for Cloud Web Security. The first screenshot highlights three key pieces of information that are used, after creating a custom application in Okta for Cloud Web Security, to enable the integration.

- **Location** – This is the single sign on (SSO) URL provided by the IdP for the defined SAML application. In this case, that application is Cloud Web Security.
- **EntityID** – The EntityID or “Issuer” is part of the verification process for validating the IdP.

- **Certificate** – This is the x.509 certificate the IdP is used to authenticate and authorize the SAML service.

The following is needed to configure VMware Cloud Web Security

1 Identity Provider Single Sign-On URL:

Location

2 Identity Provider Issuer:

EntityID

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

Certificate

[Download certificate](#)

Figure: Okta Configuration for VMware Integration

Enabling SSO

Integrating the IdP requires you to input the information about into CWS. To do this, navigate to **Cloud Web Security > Certificates > Authentication**. There you must accomplish several tasks:

- **Single Sign On** – Click to **Enabled**
- **SAML Server Internet Accessible** – Select **Yes**
- **SAML 2.0 Endpoint** – Copy & paste the **Location** information from the IdP here
- **Service Identifier (Issuer)** – Copy & paste the **EntityID** information from the IdP here
- **Domain** – Enter your company's domain here (example: vmware.com)
 - Users will authenticate to the service using their email address
 - The user's email domain must match what is configured here

The screenshot shows the VMware Orchestrator interface for configuring Cloud Web Security. The left sidebar contains a navigation menu with sections: Policies (Security Policies), Enterprise Settings (DLP, CASB, Inspection Engine, Corporate Gateways), Certificates (Authentication, SSL Termination), and Access Method (Web Proxy). The main content area is titled 'Single Sign On' and features a toggle switch set to 'Enabled'. Below this, there are several configuration fields: 'SAML Server Internet Accessible?' with radio buttons for 'Yes' (selected) and 'No'; 'SAML Provider' with a dropdown menu showing 'Okta'; 'SAML 2.0 Endpoint' with a red label 'Location' and a red input field; 'Service Identifier (Issuer)' with a red label 'EntityID' and a red input field; 'Domain' with a red label 'Domain' and a red input field; and 'Enable SAML Verbose Debugging' with radio buttons for 'Yes' (selected) and 'No'. At the bottom, there is an 'X.509 Certificate' section showing an expiration date of 'May 24 13:42:51 2032 GMT' and a blue 'EDIT CERTIFICATE' button, with a red label 'Certificate' next to it.

Figure: Configure IdP Information in Cloud Web Security

After you have set these attributes be sure to **Save Changes**. The **Save Changes** button will appear on the bottom right of the screen.



Figure: Save Changes Button

To finish the configuration, you must provide Cloud Web Security with the IdP certificate.

- **Edit Certificate** – Copy & paste the **Certificate** information from the IdP here
 - When you click this button, a modal will pop-up
 - Click the **Show Certificate** drop box to reveal where you will paste in the certificate
 - When done click **Save**

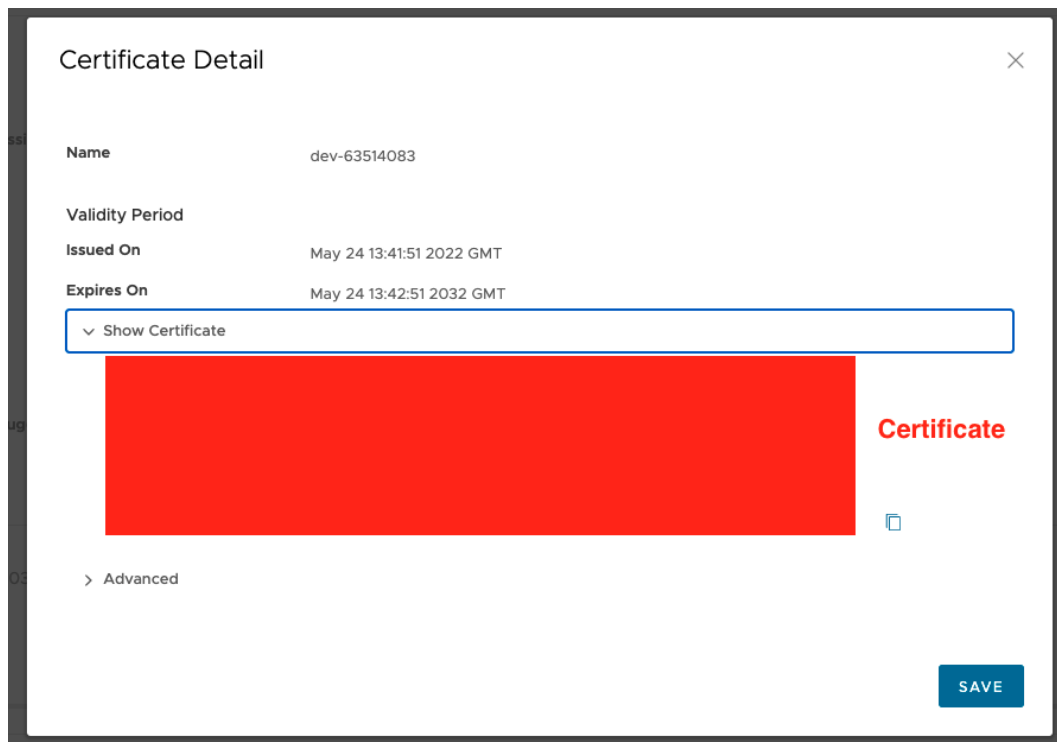
A screenshot of a 'Certificate Detail' form. The form has a title bar with a close button (X). It contains several fields: 'Name' with value 'dev-63514083', 'Validity Period' with a sub-label 'Issued On' and value 'May 24 13:41:51 2022 GMT', and 'Expires On' with value 'May 24 13:42:51 2032 GMT'. Below these is a dropdown menu labeled 'Show Certificate'. A large red rectangular area represents the certificate content. To the right of this area is the word 'Certificate' in red and a small icon. At the bottom left is a link '> Advanced' and at the bottom right is a blue 'SAVE' button.

Figure: Insert IdP Certificate in Cloud Web Security

After you have set these attributes be sure to **Save Changes**. The **Save Changes** button will appear on the bottom right of the screen.



Figure: Save Changes Button

Enable Web Proxy

The Web Proxy configuration pane is accessed by navigating to **Cloud Web Security > Access Method > Web Proxy**. From this page you can activate the Web Proxy service, associate a Cloud Web Security Policy, and generate a PAC file. Configuration steps are documented below.

From the **Web Proxy Configuration** page, you must first enable the web proxy service. This is done by clicking the toggle button beside **Enable Web Proxy**. This will change the setting from **Inactive** to **Active**. Finally, click **Save**.

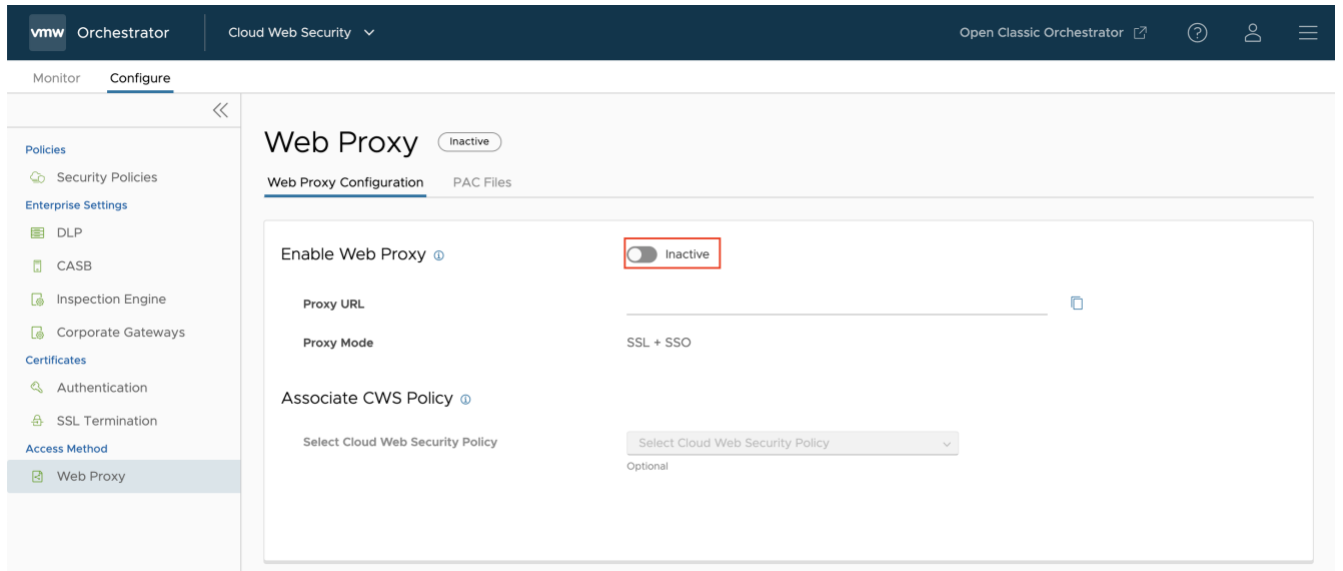


Figure: Web Proxy Inactive

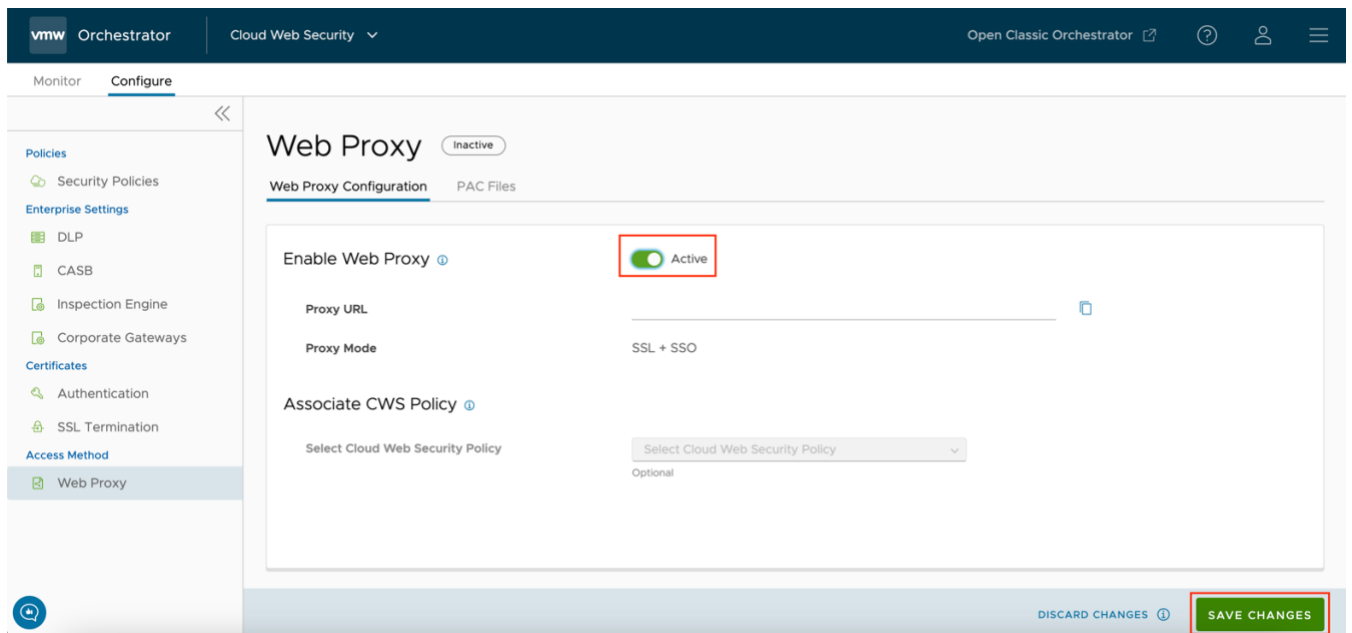


Figure: Web Proxy Activation

Once the service has been activated you will receive a notification and see several fields change on the **Web Proxy Configuration** page.

- **Proxy URL** – This is an autogenerated URL that comprises a unique user identifier (UUID) followed by `cwsproxy.gsm.vmware-test.net` and the port number 3129. For manual proxy configuration on a host, this will be the URL and port you will need to supply to the system.
- **Proxy Mode** – There is only one available proxy mode for Cloud Web Security. This mode requires the use of SSL and SSO to connect to the proxy service.

- **Select Cloud Web Security Policy** – Upon activation of the Web Proxy service no security policy is set. Although the Web Proxy is useable in this state it does not offer any security. If you have not defined a Cloud Web Security Policy do so. It will be selectable from the drop-down menu and applied to all Web Proxy users.

The screenshot shows the 'Web Proxy' configuration page. At the top, there's a 'Web Proxy' header with an 'Active' status indicator. Below this are two tabs: 'Web Proxy Configuration' (selected) and 'PAC Files'. The main configuration area includes a toggle for 'Enable Web Proxy' which is turned on. Below the toggle are fields for 'Proxy URL' (containing 'b56c24e978bf64af.cwsproxy.gsm.vmware-test.net:3129') and 'Proxy Mode' (set to 'SSL + SSO'). There is also a section for 'Associate CWS Policy' with a dropdown menu labeled 'Select Cloud Web Security Policy' and a red arrow pointing to it. At the bottom, a green success message states: 'Web Proxy enabled successfully. You can now use the proxy URL to configure your PAC file.' with a red arrow pointing to it.

Figure: Web Proxy Activation

Associate CWS Policy

This screenshot shows the 'Select Cloud Web Security Policy' dropdown menu. A red arrow points to the selected option, 'web-proxy-users'. Below the policy name, it shows 'Created: May 17, 2022' and 'Status: Unused'.

Figure: Associate Policy for Proxy Users

After your Cloud Web Security Policy is associated you will be prompted to **Save** the configuration.

Web Proxy Active

Web Proxy Configuration PAC Files

Enable Web Proxy Active

Proxy URL b56c24e978bf64af.cwsproxy.gsm.vmware-test.net:3129

Proxy Mode SSL + SSO

Associate CWS Policy web-proxy-users

Select Cloud Web Security Policy Optional

Web Proxy enabled successfully. You can now use the proxy URL to configure your PAC file.

[DISCARD CHANGES](#) [SAVE CHANGES](#)

Figure: Saving a Complete Web Proxy Configuration

At this point you are now ready to begin securing remote users with the Cloud Web Security Web Proxy

PAC Files

CWS provides a default PAC file when the Web Proxy Configuration is enabled. You are also able to create custom PAC file(s) based on your organization's exact needs and desired behavior when connecting to the service. You can find the PAC Files settings by navigating to **Cloud Web Security > Access Method > Web Proxy > PAC Files**.

Web Proxy Active

Web Proxy Configuration PAC Files

Q Search

+ NEW PAC EDIT CLONE PREVIEW DOWNLOAD DELETE

	Name	Description	Created	PAC File URL	Download File / Copy URL
<input type="checkbox"/>	Default		2 July 2022	https://cwsproxy.gsm.vmware.com/eba19fce416223f0/wpad.dat	Download / Copy
<input checked="" type="checkbox"/>	Cloud Authentication Only		15 July 2022	https://cwsproxy.gsm.vmware.com/eba19fce416223f0/cloud-auth-only.dat	Download / Copy

Figure: PAC Files Configuration

Default PAC File

You are not able to edit the default PAC File's configuration, but you can view it to see if it is right for your requirements.

Simply click the **Check Box** by the line of the Default PAC File and select **PREVIEW** to see its contents in Orchestrator.

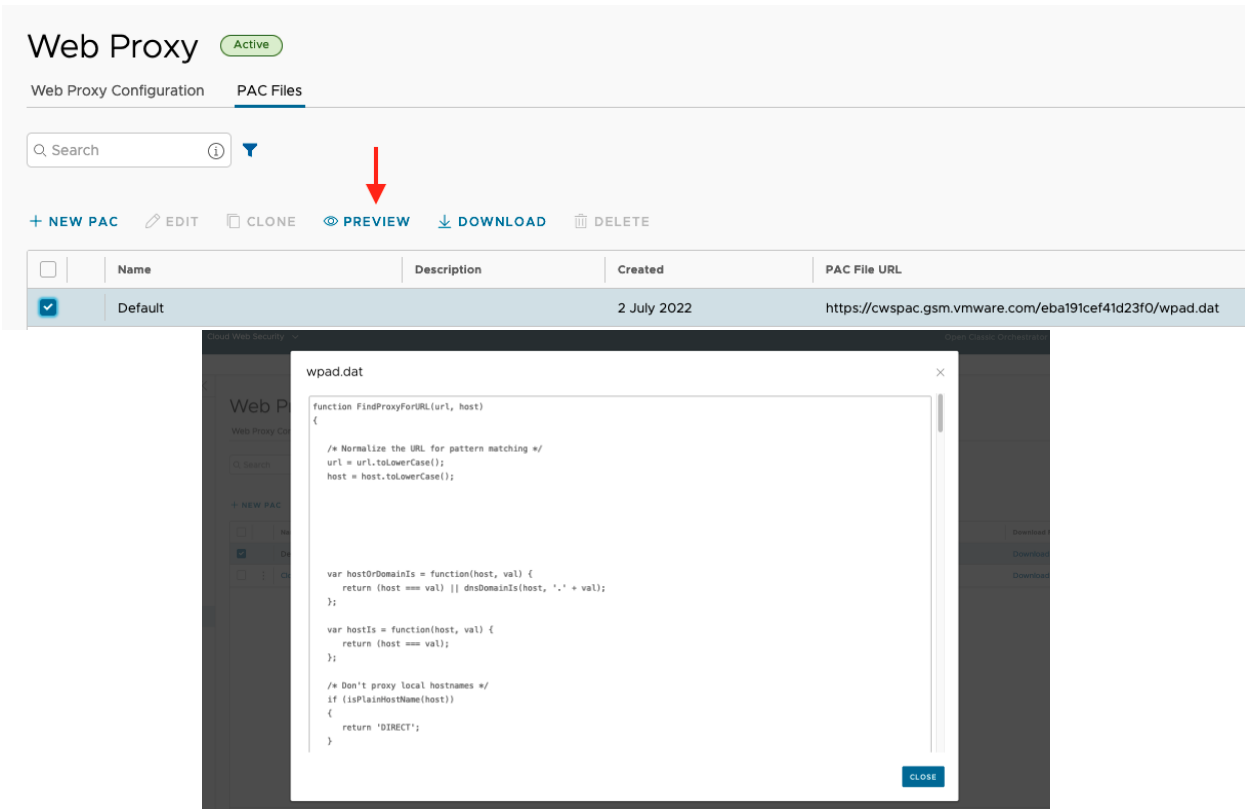


Figure: Default PAC File Details

While you do not need to concern yourself with creating the exact syntax, as the built-in wizard will guide you through PAC file configuration, it is useful to understand the directives in the file.

For example, if a matching block instructs the client to send the traffic **DIRECT** that means any traffic to those destinations will not go through the proxy. This is useful for several reasons. And traffic that is meant to go to the proxy will have the **PROXY** directive in its return statement. It could also have both **PROXY** followed by **DIRECT**. This means that if the proxy is unavailable, that traffic would still be permitted to go to the Internet.

Custom PAC Files

To launch the PAC file creation wizard simply click + **NEW PAC** on the PAC Files configuration page and follow the steps in the wizard.

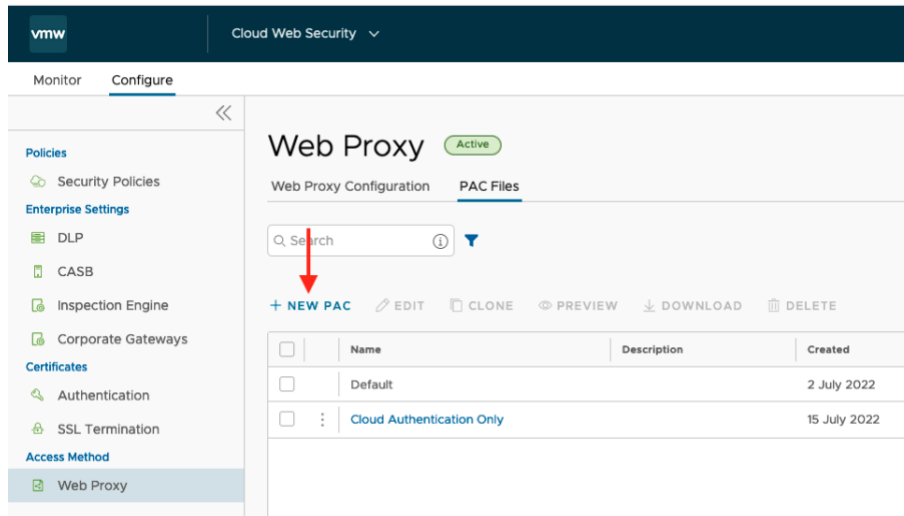


Figure: Launch New PAC File Wizard

1 PAC File Details

Fill in the details and click **NEXT** to proceed to the next step.

- **Name** (required): A useful reference for this PAC file.
- **Description** (optional): Any additional information you would like to leave for other administrators.
- **File Name** (required): The filename that VMware will host for your organization. This file name must end in '.dat' to be accepted. A warning will appear if the file name is not correctly formatted.

New/Edit PAC File

1 PAC File Details
2 Proxy and Roaming Configura...
3 Default Proxy Bypass
4 Bypass Office 365
5 Custom Proxy Bypass

PAC File Details

Define a PAC file to configure the rules to identify traffic to be forwarded to the CWS web proxy server.

PAC File Details

Name

Cloud Authentication Only

Description

Description

Optional

File Name

cloud-auth-only.dat

CANCEL

NEXT

Figure: PAC File Details

2 Proxy and Roaming Configuration

This section gives you the flexibility to determine how your remote clients connect to the proxy service when using this PAC file.

Options include determining if clients should or should not be allowed to the Internet if the proxy is inaccessible. Or, if the client is behind a corporate network should it use the corporate network's Internet access or be redirected to an on-premises proxy server.

- **Proxy Inaccessible:** Connect Direct or Block Access

New/Edit PAC File

1 PAC File Details

2 Proxy and Roaming Configuration

3 Default Proxy Bypass

4 Bypass Office 365

5 Custom Proxy Bypass

Proxy and Roaming Configuration

Settings to (a) Configure action based on proxy accessibility (b) Configure action based on user location inside or outside the corporate network.

PAC File Details

Proxy Inaccessible

Connect Direct

Block Access

Detect when within the corporate network

CANCEL BACK NEXT

Figure: Proxy and Roaming Configuration

- **Detect when within the corporate network:** Toggle on or off
 - **Internal Server Name:** The name of an internal server to be resolved. This server should only be resolvable on the private network.
 - **IP Address:** The expected internal IP that the server's name should resolve to.
 - **If the hostname is successfully resolved:**
 - **Connect Direct** – Instruct the client to send outbound Web traffic from a browser using the private network
 - **Custom Proxies** – Instruct the client to send outbound Web traffic to an on-premises web proxy accessible through the private network

New/Edit PAC File

- 1 PAC File Details
- 2 Proxy and Roaming Configura...
- 3 Default Proxy Bypass
- 4 Bypass Office 365
- 5 Custom Proxy Bypass

Proxy and Roaming Configuration

Settings to (a) Configure action based on proxy accessibility (b) Configure action based on user location inside or outside the corporate network.

PAC File Details

Proxy Inaccessible ⓘ Connect Direct

Detect when within the corporate network ⓘ ☒

Internal Server Name

IP Address

Ex: test.vmware.com

Ex: 1.2.3.4

If the hostname is successfully resolved

- ✓ Connect Direct
- Custom Proxies

CANCEL BACK NEXT

Figure: Detect when within the corporate network

New/Edit PAC File

- 1 PAC File Details
- 2 Proxy and Roaming Configura...
- 3 Default Proxy Bypass
- 4 Bypass Office 365
- 5 Custom Proxy Bypass

Proxy and Roaming Configuration

Settings to (a) Configure action based on proxy accessibility (b) Configure action based on user location inside or outside the corporate network.

PAC File Details

Proxy Inaccessible ⓘ Connect Direct

Detect when within the corporate network ⓘ ☒

Internal Server Name

IP Address

Ex: test.vmware.com

Ex: 1.2.3.4

If the hostname is successfully resolved

- Custom Proxies

IP Address

Custom Proxies as eg: domain.vmware.com:4343

CANCEL BACK NEXT

Figure: Custom Proxies

3 Default Proxy Bypass

This section contains smart defaults to enable easy bypasses of domains and subnet/IPs that should not be sent to the Web proxy. However, your organization may desire to send Netflix traffic to the Web proxy as part of your security posture. You can simply toggle on or off the domains that should be allowed or bypassed from proxy. The subnet/IP entries in this section are fixed since these are all non-routable IPs that will otherwise fail to reach a destination when sent to the Internet.

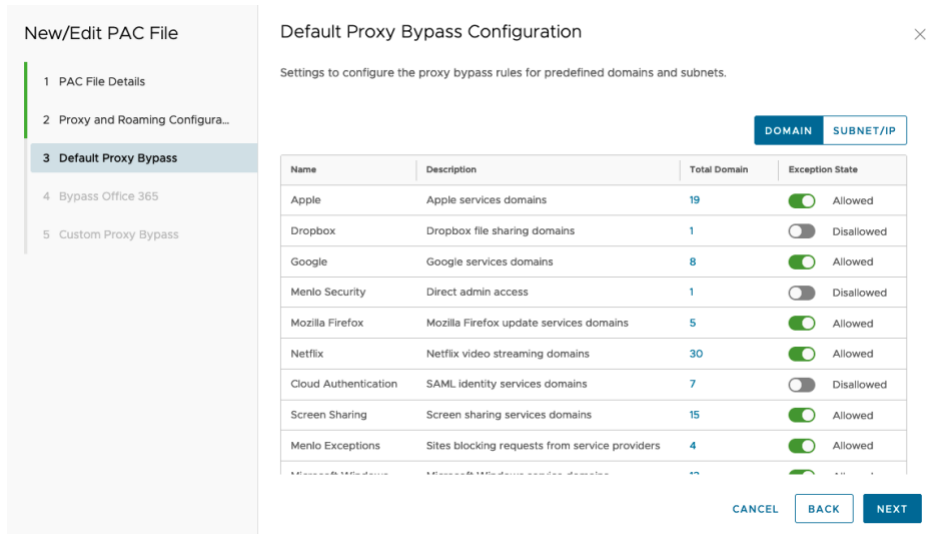


Figure: Toggle Allowed/Disallowed Domains

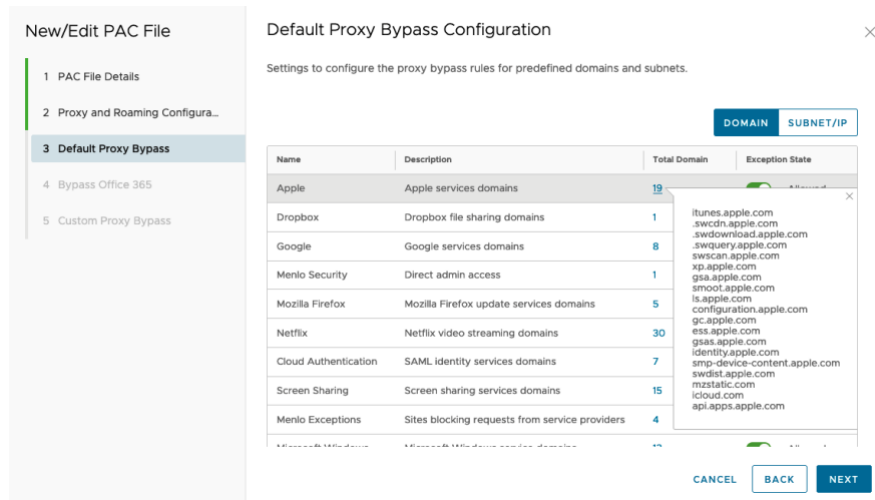


Figure: View Domains Associated to an App

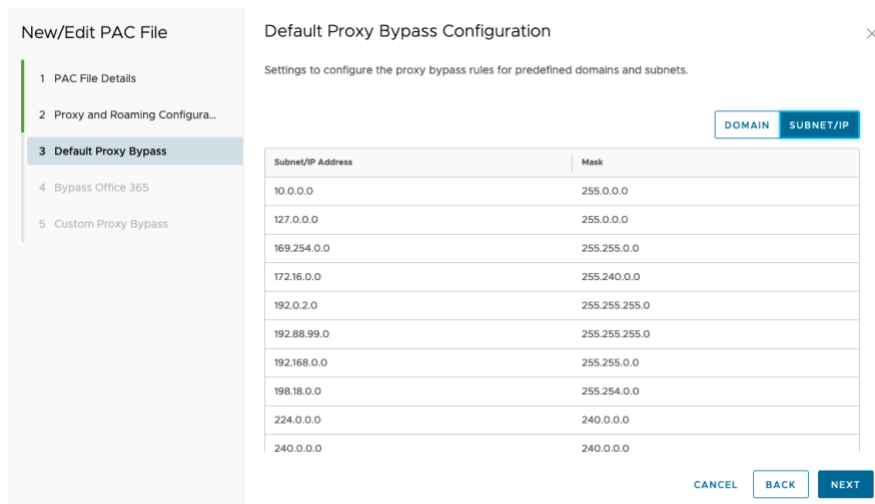


Figure: View Subnets Excluded from Proxy

4 Bypass Office 365

Microsoft Connectivity Principles recommend bypassing their endpoints from Web Proxy or SSL Inspection services. Microsoft encourages their customers to access their services direct over the Internet. This section allows for easy bypass of Microsoft 365 domains. Additionally, you can include your organization's specific tenants in this configuration pane.

- **Bypass Office 365:** Allowed simply means these domains will be added to the PAC file to be bypassed.
- **Tenants:** Gives you the option to specific your company specific subdomains provided by Microsoft.

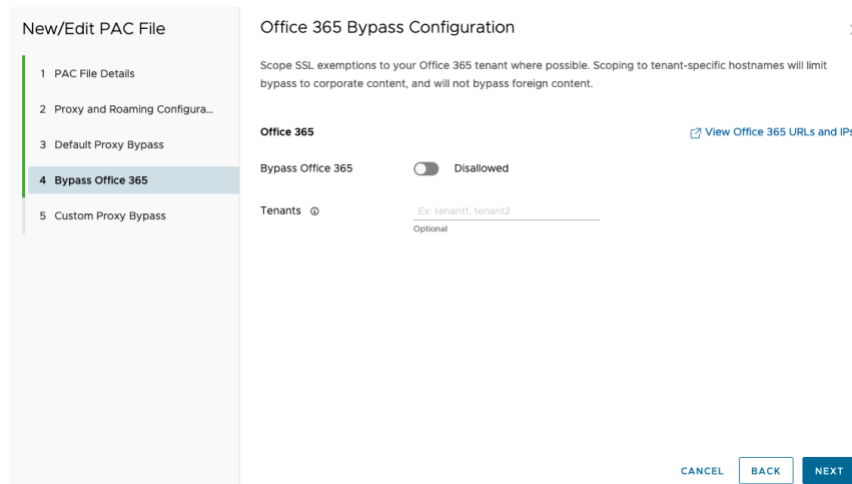


Figure: Microsoft 365 Easy Bypass Setting

5 Custom Proxy Bypass

At this point you are given full flexibility to dictate which domain(s) and subnet/IP(s) will be exempted from being sent to the Web proxy.

- **DOMAIN**
 - **+ ADD RULE:** This will create a rule entry in the table for you. Here you can enter a valid domain. Click '+ ADD RULE' each time you need to add a new entry.
 - **DELETE:** This provides the mechanism to remove a domain that was entered incorrectly or no longer to be bypassed when updating the configuration.

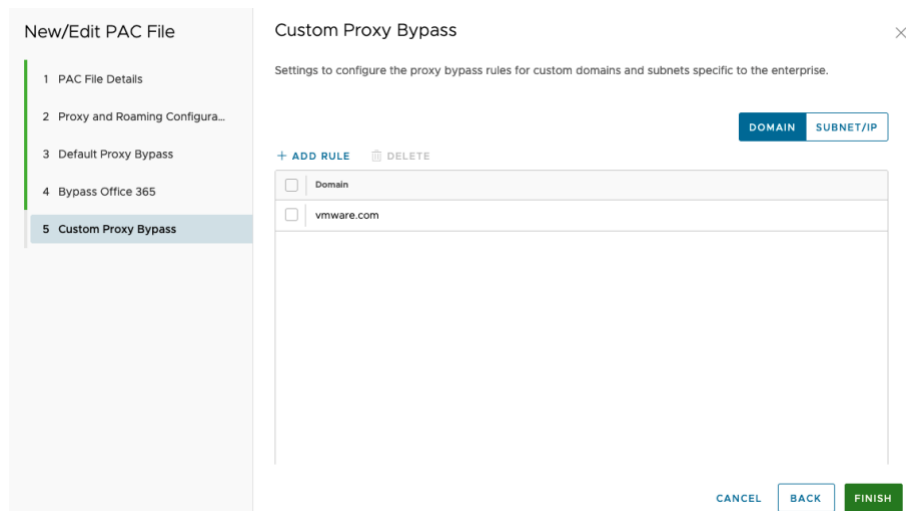


Figure: Add Domain(s) to Custom Proxy Bypass Option

- **SUBNET/IP**
 - **+ ADD RULE:** Like domain, this provides an entry row for the IP information. Here you will need to provide either the network address (subnet) or the IP address (host) and the appropriate subnet mask value.
 - **DELETE:** Like domain, this is used to remove erroneous entries or update existing configuration files.

When done click **FINISH** to create your PAC file and begin using it.

Host Configuration

A host can be configured with manual or automatic proxy settings. The distribution of these configurations will most likely be performed with Microsoft Group Policy Objects (GPO) or Mobile Device Management (MDM) platforms like Workspace ONE. However, it is necessary to understand provisioning methodologies to ensure the correct configuration is added on all devices.

Manual Proxy Settings

A host can be configured manually or automatically. The manual configuration requires the administrator to specify the proxy URL and port that Web browser traffic should be redirected towards. Additionally, manual entry of domains and endpoints pass might be required to ensure correct operations. The automatic method relies on the availability of a PAC file the system can reference to download its proxy settings.

Ubuntu

The following is a simple example highlighting the manual and configuration on an Ubuntu Desktop host. The general concepts shown here apply to Windows, macOS, Android, and iOS devices. Links to product specific documentation are provided in those sections.

Click on the **Show Applications** button and select **Settings**.

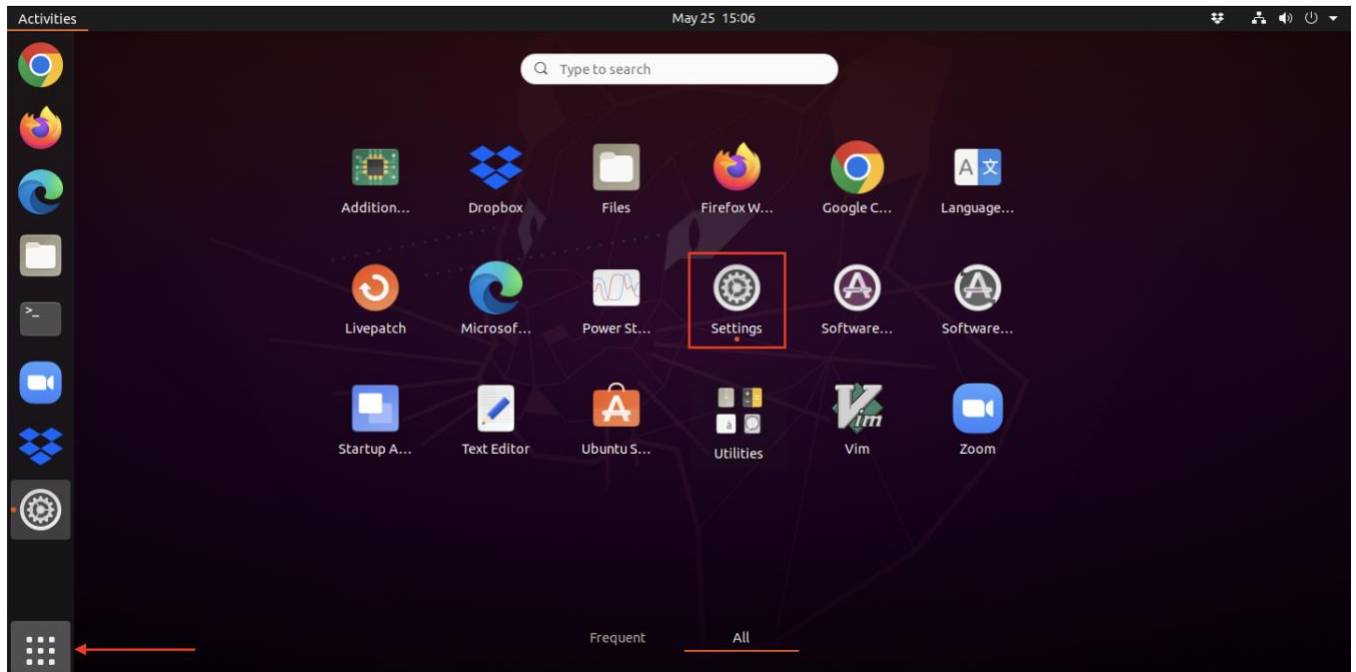


Figure: Navigating to Ubuntu Desktop Settings

Once in the **Settings** pane click on **Network** if not already there. Here you can click the **Cog Wheel** to turn proxy settings on manually, automatically, or off.

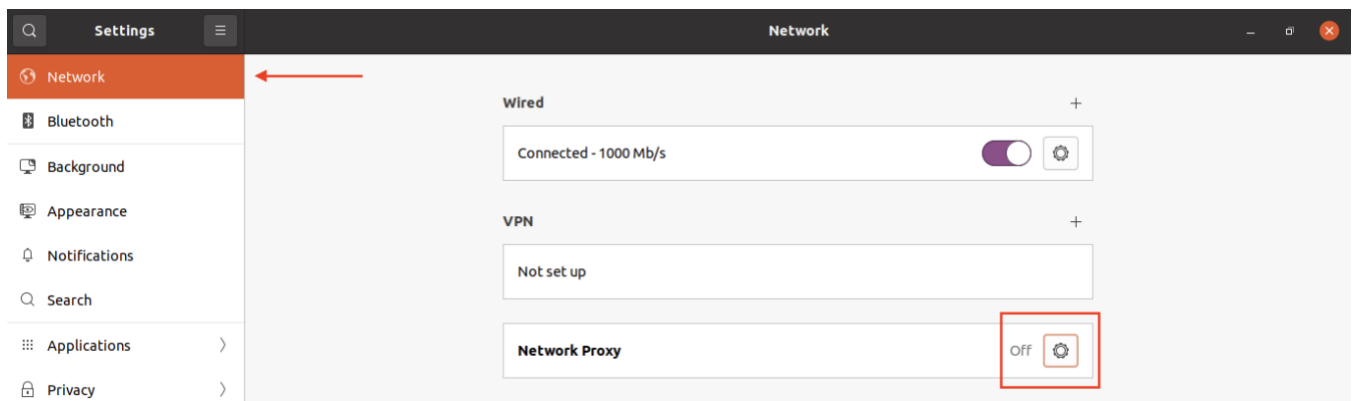


Figure: Network Proxy Settings

For manual configuration, you will need to retrieve the URL + Port information from Cloud Web Security. Return to **Cloud Web Security > Configure > Access Methods > Web Proxy > Web Proxy Configuration** and highlight and copy the URL.

Web Proxy

Active

Web Proxy Configuration

PAC Files

Enable Web Proxy ⓘ ☒ Active

Proxy URL **b56c24e978bf64af.cwsproxy.gsm.vmware-test.net:3129** ⓘ

Proxy Mode SSL + SSO

Associate CWS Policy ⓘ

Select Cloud Web Security Policy **web-proxy-users** ⓘ

Optional

Figure: Copy Proxy URL

Then **paste** the URL into the **HTTP Proxy** and **HTTPS Proxy** field. Next, set the port to **3129** for both rows. You can copy and paste this from Cloud Web Security or type it in manually. **Please be aware that for SSO to work** you will need to bypass the domains associated with your identity provider. The example below shows three domains related to Okta. Additional IdP domains are provided below. If you do not see your IdP please consult their product documentation to determine which domains will need to be exempted from the proxy.

- Okta
 - *okta.com, *oktapreview.com, *oktacdn.com
- Workspace ONE Access
 - *vidmpreview.com
- Azure Active Directory
 - login.microsoftonline.com
 - sts.windows.net
 - microsoftonline-p.com
 - msauth.net
 - msftauth.net

When finished click the **X** icon in the upper right-hand corner to apply the settings.

The screenshot shows a 'Network Proxy' configuration window. At the top, there are three radio buttons: 'Automatic', 'Manual' (which is selected and highlighted with a red border), and 'Disabled'. Below these, there are five rows of proxy settings. Each row has a label on the left, a text input field in the middle, and a port input field on the right. The 'HTTP Proxy' and 'HTTPS Proxy' rows have the same values: the URL '5ff35c0827f238af.cwsj' and the port '3129'. The 'FTP Proxy' and 'Socks Host' rows are empty, with the port set to '0'. The 'Ignore Hosts' row contains the text '*okta.com, *oktapreview.com, *oktacdn.c'. The port input fields have minus and plus buttons for adjustment.

Proxy Type	Proxy URL	Port
HTTP Proxy	5ff35c0827f238af.cwsj	3129
HTTPS Proxy	5ff35c0827f238af.cwsj	3129
FTP Proxy		0
Socks Host		0
Ignore Hosts	*okta.com, *oktapreview.com, *oktacdn.c	

Figure: Paste Proxy URL and Enter 3129 Port Number

At this point you should be able to launch your Web browser and see the Cloud Web Security login page. Please note that if you see a warning page stating that “**Your connection is not private**” it is likely you have not installed the [SSL Termination Certificate](#). You can either follow the steps to install the certificate or accept the warning and proceed to the Cloud Web Security login page.

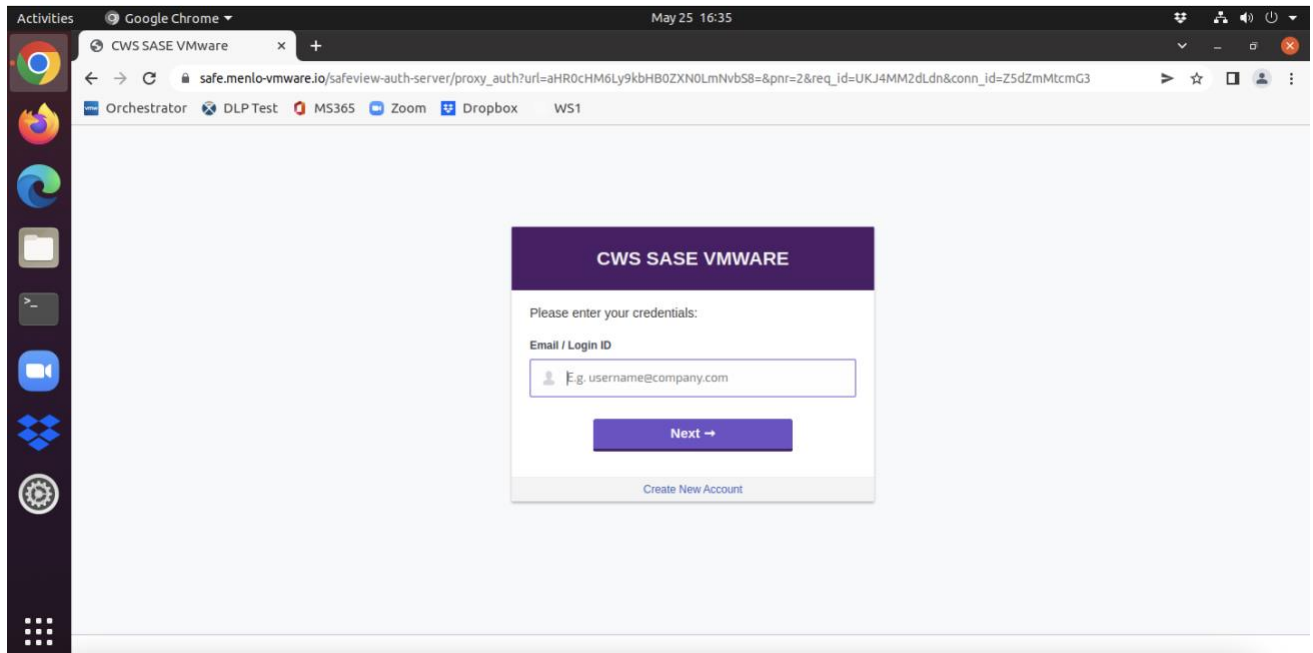


Figure: Cloud Web Security Proxy Login Page

At this point you will need to:

- Enter a valid email address configured in your IdP and click **Next**
- When redirected to your IdP's sign on page, enter your credentials and authenticate
- Begin validating Internet connectivity and Cloud Web Security Policy

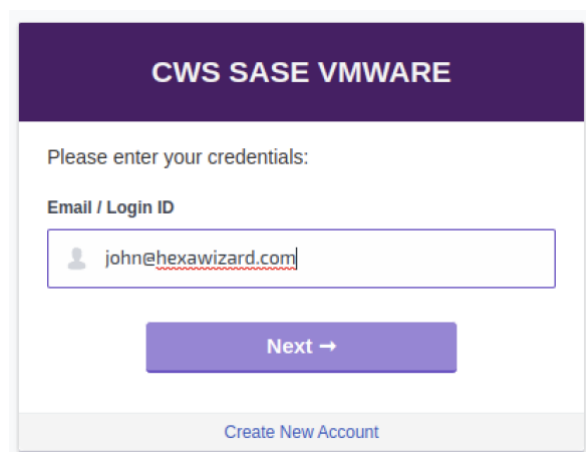




Figure: Enter Valid Username

Connecting to 



Sign In

Username

Password

☐ Keep me signed in

Sign in

[Forgot password?](#)

[Help](#)

Figure: Authenticate to the IdP

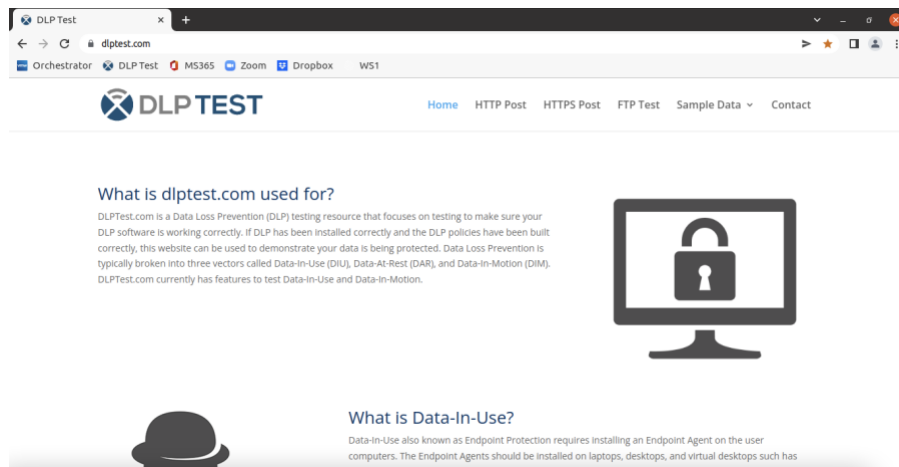


Figure: Begin Browsing

Automatic Proxy Settings

Once you are satisfied with the manual proxy configuration, convert the host to use the Web Proxy Auto-discovery (WPAD) file. The WPAD file is a more robust set of instructions that are downloaded and automatically set on the host.

You will need to return to **Cloud Web Security > Configure > Access Methods > Web Proxy > PAC Files**. From here, you can use the **Copy** button beside any PAC file that is present in the system.

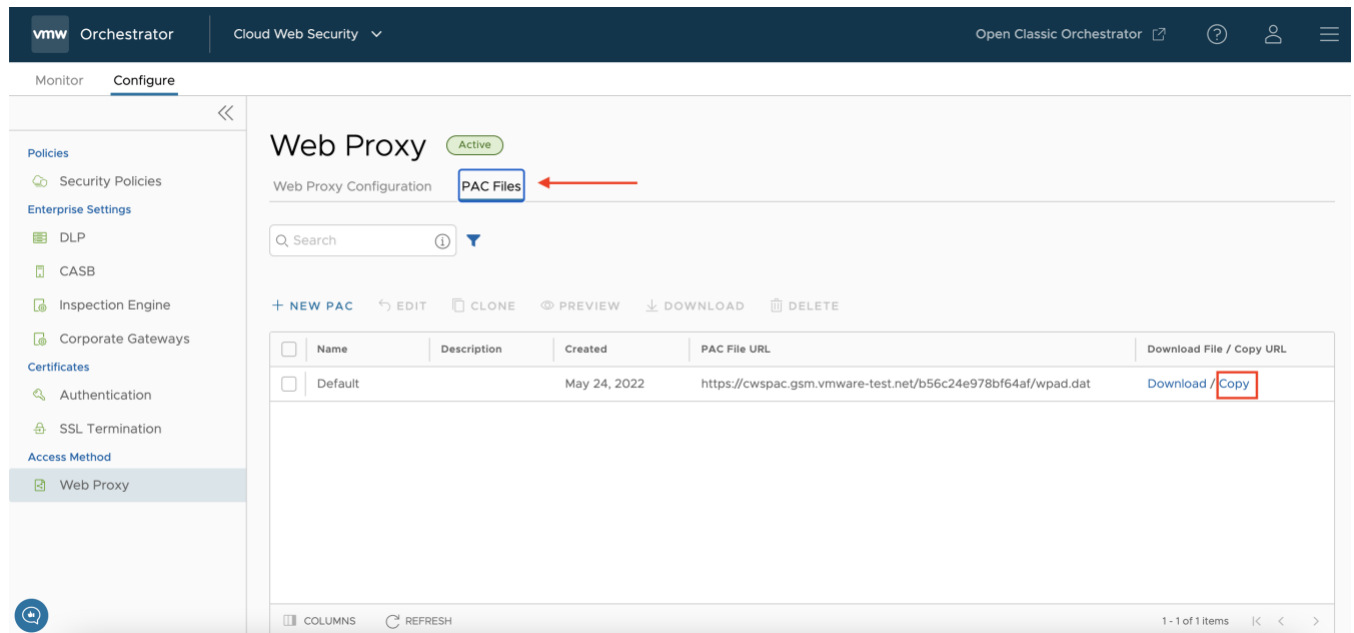


Figure: Copy WPAD URL

Now, return to the host and change the proxy settings to **Automatic** and paste the copied URL into the field. Click **X** to close the dialog box and apply the settings.



Figure: Provide Configuration URL for Automatic Settings

Windows

Consult the product documentation to see how to configure these settings on a Windows system [here](#).

macOS

Consult the product documentation to see how to configure these settings on a macOS system [here](#).

Android

Consult the product documentation to see how to configure these settings on an Android system [here](#). The included reference is for a Google Pixel phone. You may need to search for your specific model if the options are not the same.

iOS

Consult this how to guide to see how to configure these settings on an iOS system [here](#).

Troubleshooting

Single Sign On is Disabled

As stated in the pre-requisite checklist, SSO must be enabled before you are able to setup the Web Proxy. If you see the message bar stating, you need to “Enable SSO” please refer to the prerequisites in this document.

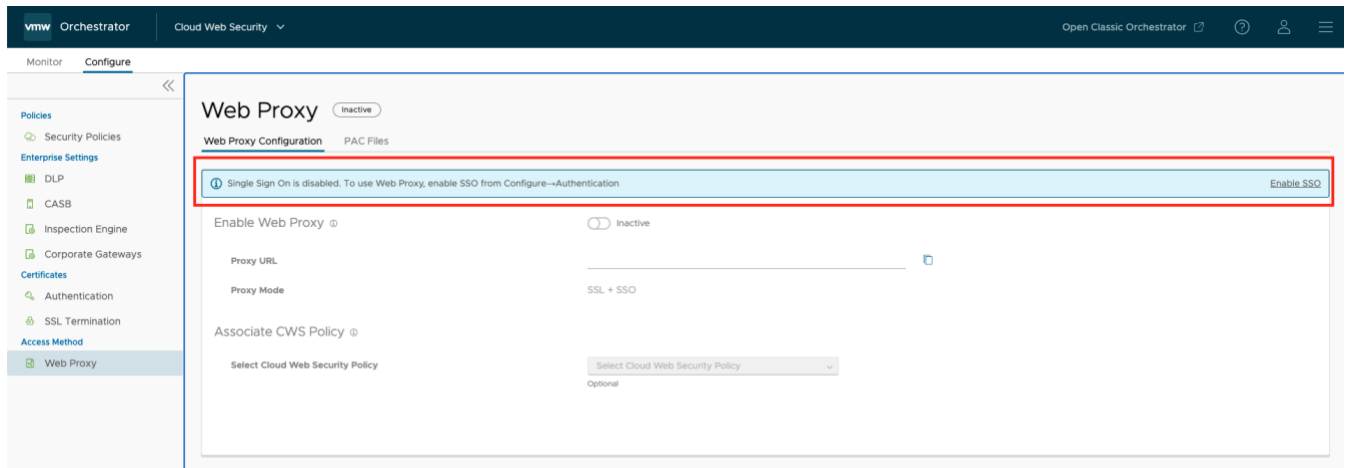


Figure: Enable SSO