VMware Cloud Web Security Configuration Guide

VMware Cloud Web Security

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Cloud Web Security Configuration Guide

1

VMware Cloud Web Security™ is part of the VMware SASE™ solution and is a cloud hosted service that protects users and infrastructure accessing SaaS and Internet applications from a changing landscape of internal and external threats, offers visibility and control, and ensures compliance.

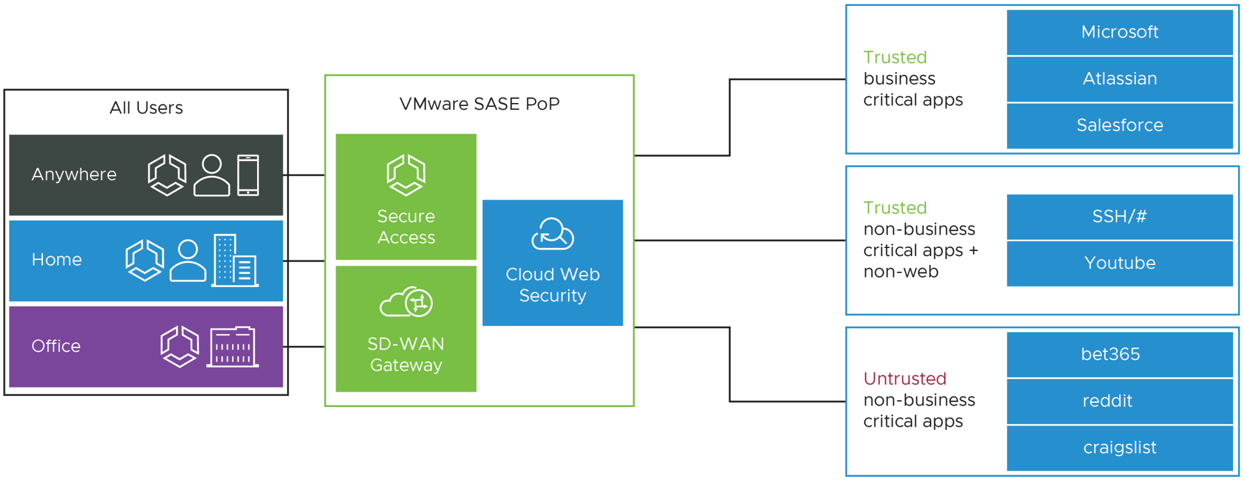
VMware Cloud Web Security™ Configuration Guide provides information about how to create, configure, apply, and monitor security policies for the VMware Cloud Web Security service. The guide provides detailed information about how to use the SSL Inspection, Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), Web Security, and Web Proxy features for the VMware Cloud Web Security service.

Read the following topics next:

- VMware Cloud Web Security Overview
- Prerequisites
- Create a Security Policy
- Clone a Security Policy
- Configuring a Security Policy
- Cloud Web Security Policy and Rule Limits
- Applying a Security Policy

VMware Cloud Web Security Overview

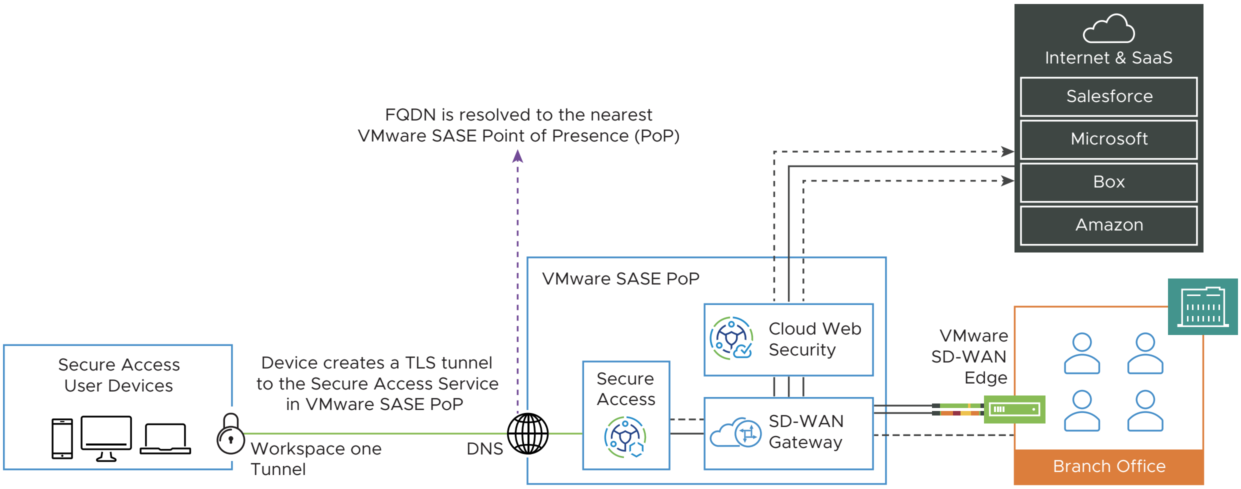
VMware Cloud Web Security™ is a cloud hosted service that protects users and infrastructure accessing SaaS and Internet applications from a changing landscape of internal and external threats, offers visibility and control, and ensures compliance.



VMware Cloud Web Security is delivered through a global network of VMware SASE™ Points-of-Presence (PoP) to ensure that users located anywhere and connecting over any device have a secure, consistent, and optimal access to applications. Cloud Web Security simplifies management of security services and helps IT tighten the security posture while balancing user productivity.

Packet Flow

VMware Cloud Web Security uses Transport Layer Security (TLS) to ensure fully secure communication from a client device to a web server. To learn more about the TLS versions used by Cloud Web Security, see Supported Transport Layer Security (TLS) Versions and Cipher Suites.


Internet & SaaS
Salesforce
Microsoft
Box
Amazon
FQDN is resolved to the nearest VMware SASE Point of Presence (PoP)
VMware SASE PoP
Cloud Web Security
Secure Access
SD-WAN Gateway
VMware SD-WAN Edge
Branch Office
Secure Access User Devices
Device creates a TLS tunnel to the Secure Access Service in VMware SASE PoP
Workspace one Tunnel
DNS

Cloud Web Security provides IT teams the visibility and control they need to maintain a strong security posture while adhering to compliance needs with the following advantages:

- Agile Security Posture - As a cloud hosted service any threat detected anywhere by Cloud Web Security is immediately blocked for all customers taking advantage of the cloud-native properties.
- Secure Seamless Access for Anywhere Workforce - Leveraging a global network of VMware SASE PoP, Cloud Web Security delivers secure and optimal access to users for Internet and SaaS applications.
- Simplified Operations - Cloud Web Security uses a centralized management pane using the VMware SD-WAN Orchestrator for network services and security services simplifying deployment and operations of a distributed workplace.
- Reducing Operational Cost - Cloud Web Security offers cost savings from managing the life cycle and refresh cycle of physical or virtual appliances deployed on-premises.

Cloud Web Security is offered through the global network of VMware SASE PoP that are delivered as a managed service and used by more than 150 Telecommunication Partners and thousands of Value-Added Resellers globally.

Cloud Web Security Release Notes can be found here.

Supported Transport Layer Security (TLS) Versions and Cipher Suites

This section covers the versions of Transport Layer Security (TLS) communication used by Cloud Web Security. Cloud Web Security will always use the highest TLS version available for the connection.

This highest TLS version is supported for full end-to-end communication **Client > Cloud Web Security > Web Server** provided the client and server support this TLS version.

For any communication to a web server, the client will begin by trying to negotiate the highest TLS version (1.3), and then when the Cloud Web Security service proxies the connection it will try to honor that version. However, the web server will have the ultimate say on which TLS version is used. In other words, if the web server only supports TLS 1.2, that is the version that would be used for end-to-end communication in that instance.

The following is a list of supported TLS versions and cipher suites used in Cloud Web Security:

Table 1-1. TLS Versions and Cipher Suites Used in Cloud Web Security

TLS Versions/Cipher Suites
(TLS 1.3) AES_256_GCM_SHA384
(TLS 1.3) CHACHA20_POLY1305_SHA256
(TLS 1.3) AES_128_GCM_SHA256
(TLS 1.2) ECDHE-RSA-AES128-GCM-SHA256
(TLS 1.2) ECDHE-RSA-AES256-GCM-SHA384

Table 1-1. TLS Versions and Cipher Suites Used in Cloud Web Security (continued)

TLS Versions/Cipher Suites
(TLS 1.2) ECDHE-RSA-AES128-SHA256
(TLS 1.2) ECDHE-RSA-AES256-SHA384
(TLS 1.2) AES128-GCM-SHA25
(TLS 1.2) AES256-GCM-SHA384
(TLS 1.2) AES128-SHA256
(TLS 1.2) AES256-SHA256
(TLS 1.0, 1.1) AES128-SHA
(TLS 1.0, 1.1) AES256-SHA
(TLS 1.0, 1.1) ECDHE-RSA-AES128-SHA
(TLS 1.0, 1.1) ECDHE-RSA-AES256-SHA

Prerequisites

For a customer deployment to use Cloud Web Security, the following conditions need to be met:

- A customer Enterprise must be hosted by a VMware Cloud Orchestrator using Release 4.5.0 or later. The Orchestrator version may be viewed at the bottom of any browser page.
- The Orchestrator must always have internet connectivity.
- A VMware SD-WAN Edge is not required to use Cloud Web Security when using Web Proxy. However, if using Cloud Web Security through an Edge, the Edge must use release 4.5.0 or later.
- The customer deployment must be using a SD-WAN Gateway Pool that includes at least one VMware SD-WAN Gateway using Release 4.5.0 or later. This information is viewable by an Operator or Partner User. A Customer would need to confirm this their supporting Partner or, lacking one, a Technical Support Engineer.
- The SD-WAN Gateway must also be configured to have a Cloud Web Security Role. For steps, see Configuring a SD-WAN Gateway for a Cloud Web Security Role.

Configuring a SD-WAN Gateway for a Cloud Web Security Role

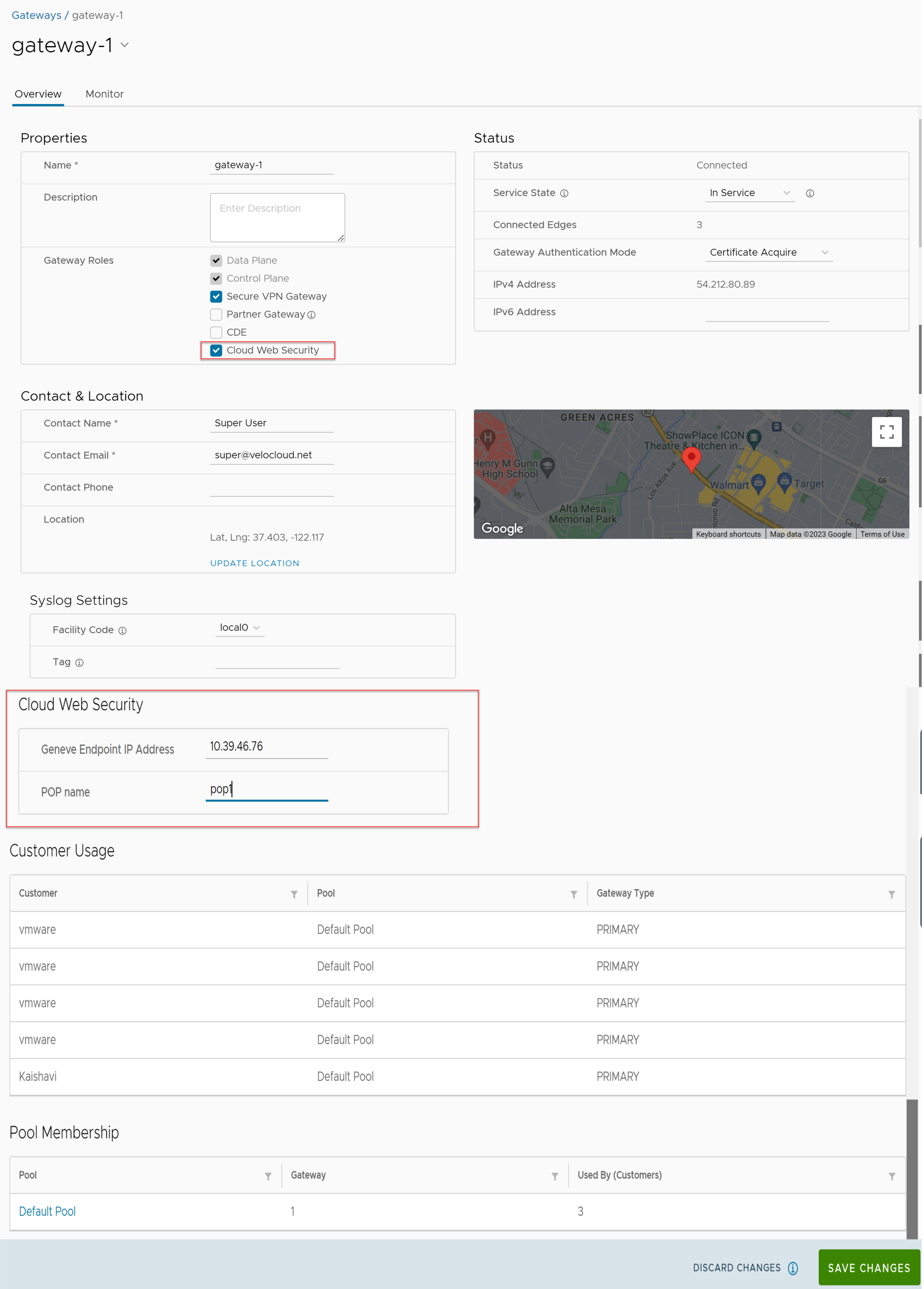
Only an Operator User with either a Superuser or Standard role can configure a SD-WAN Gateway for a Cloud Web Security role.

Users can configure a Gateway for a Cloud Web Security role in the New Orchestrator UI portal.

Procedure

1 In the Operator portal, click the **Gateway Management** tab and go to **Gateways** in the left navigation pane.

2 The **Gateways** page displays the list of available Gateways. Click the link to a Gateway for which users want to configure the Cloud Web Security role. The details of the selected Gateway are displayed in the **Configure Gateways** page.



Properties

Name *	gateway-1
Description	Enter Description
Gateway Roles	☑ Data Plane ☑ Control Plane ☑ Secure VPN Gateway ☐ Partner Gateway ☐ CDE ☑ Cloud Web Security

Status

Status	Connected
Service State	In Service
Connected Edges	3
Gateway Authentication Mode	Certificate Acquire
IPv4 Address	54.212.80.89
IPv6 Address	

Contact & Location

Contact Name *	Super User
Contact Email *	super@velocloud.net
Contact Phone	
Location	Lat, Lng: 37.403, -122.117 UPDATE LOCATION

Syslog Settings

Facility Code	local0
Tag	

Cloud Web Security

Geneve Endpoint IP Address	10.39.46.76
POP name	pop1

Customer Usage

Customer	Pool	Gateway Type
vmware	Default Pool	PRIMARY
vmware	Default Pool	PRIMARY
vmware	Default Pool	PRIMARY
vmware	Default Pool	PRIMARY
Kaishavi	Default Pool	PRIMARY

Pool Membership

Pool	Gateway	Used By (Customers)
Default Pool	1	3

3 In the **Properties** section, under **Gateway Roles**, select the **Cloud Web Security** check box.

4 In the **Cloud Web Security** section, enter the Geneve endpoint IP address and Points-of-Presence (PoP) name for the Cloud Web Security Gateway role.

5 Click **Save Changes**.

For more details, see the *Manage Gateways* section in the *VMware SD-WAN Operator Guide* published at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

What to do next

- Create a Security Policy

Create a Security Policy

To use VMware Cloud Web Security, a user must first create, configure a Security Policy, and then apply the policy.

Security policies are created and edited on the New UI of the VMware SD-WAN Orchestrator.

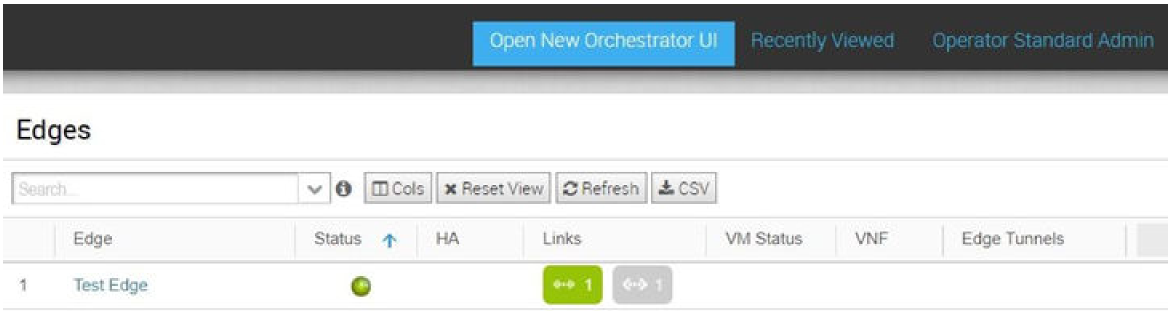
Prerequisites

To create a Cloud Web Security (CWS) policy, a user must have one of the following roles:

- An Operator with a superuser or standard roles.
- A Partner user with a superuser or standard role.
- A Customer user with a superuser, standard, or security administrator role.

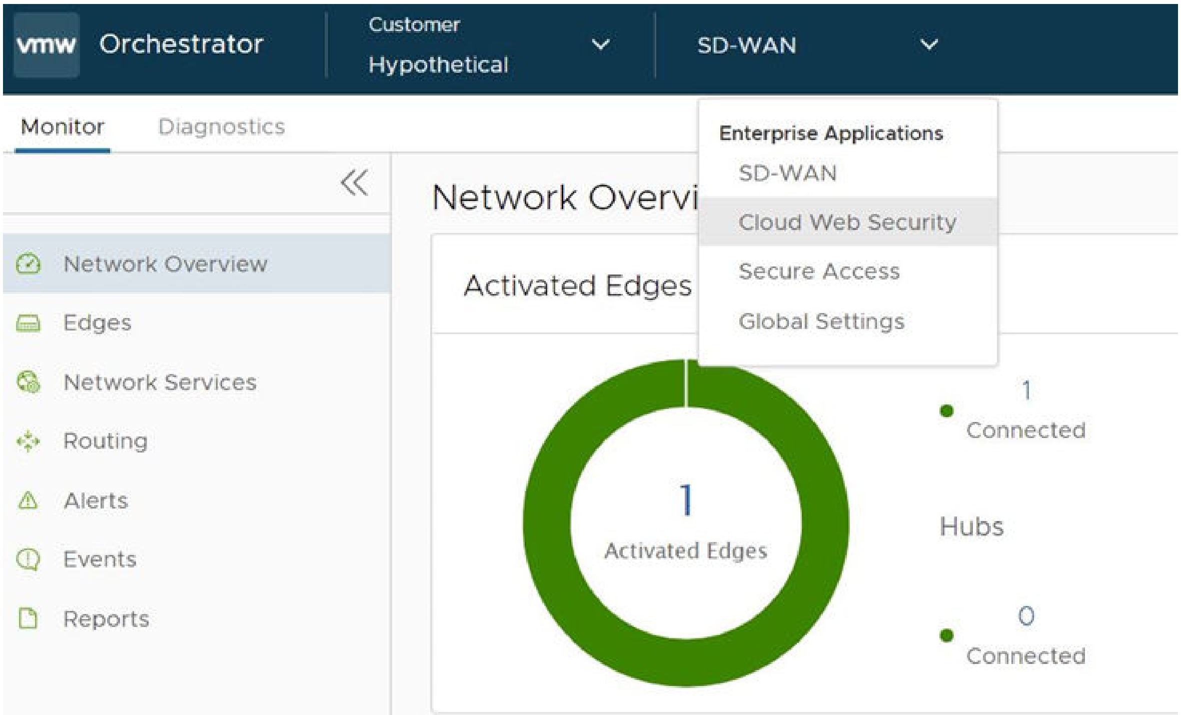
Procedure

1 In the Orchestrator portal, if not using Orchestrator version 5.1.0 or later, click the **Open New Orchestrator UI** option available at the top of the Window.



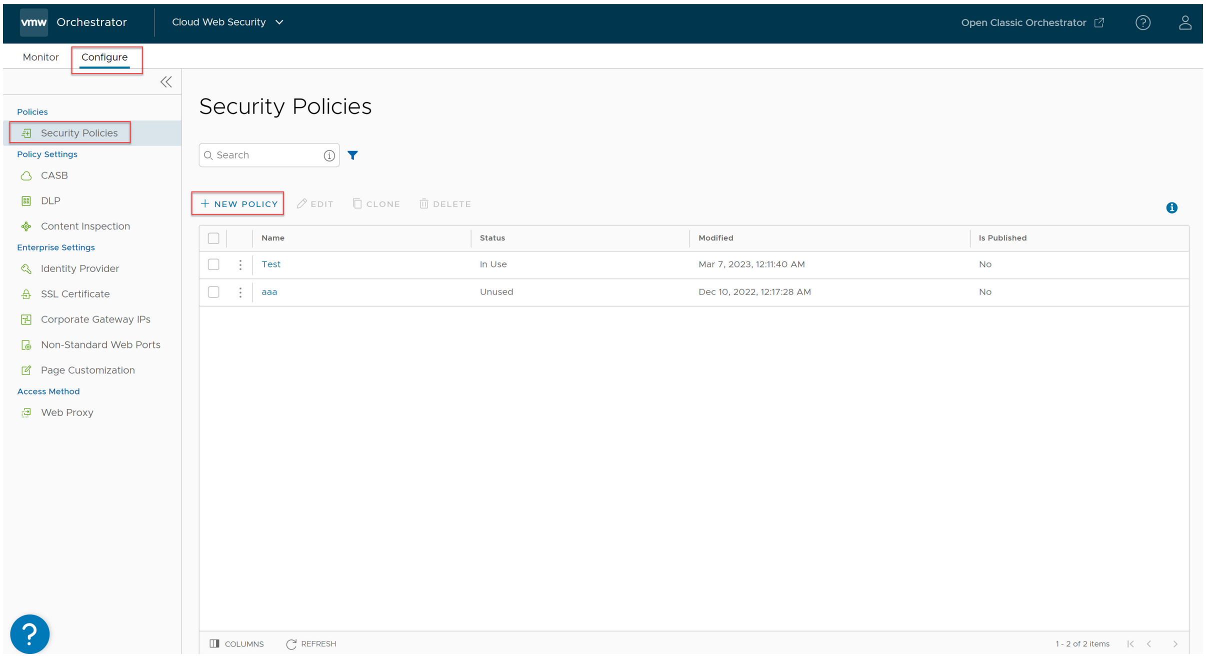
	Edge	Status	HA	Links	VM Status	VNF	Edge Tunnels
1	Test Edge	●		1 1			

2 Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab.



3 From the **SD-WAN** drop-down menu, select **Cloud Web Security**.

The **Cloud Web Security** page appears.

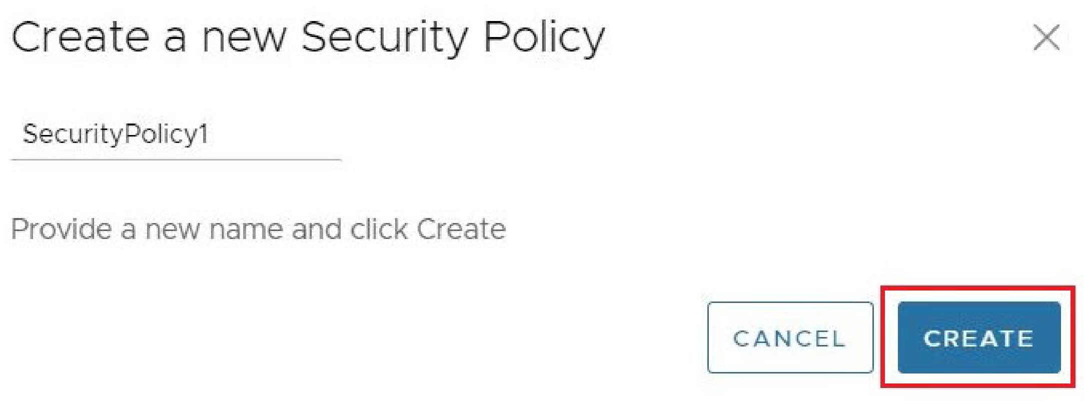


Name	Status	Modified	Is Published
Test	In Use	Mar 7, 2023, 12:11:40 AM	No
aaa	Unused	Dec 10, 2022, 12:17:28 AM	No

On the **Cloud Web Security** page, user can view, create, clone, and edit Cloud Web Security policies, and monitor the application of Cloud Web Security policies.

4 To create a new Security Policy, click the **Configure** > **Policies** > **Security Policies**. On the **Security Policies** page, click **NEW POLICY**.

The **Create a new Security Policy** pop-up window appears.



Create a new Security Policy

SecurityPolicy1

Provide a new name and click Create

5 In the textbox, enter the name for the Security Policy and click **CREATE**.

Note The policy name must be a continuous text string with no spaces. For example, **Security Policy 1** will return an error while **SecurityPolicy1** will be accepted.

Results

A Security Policy is created and appears in the **Security Policies** page.

What to do next

- Configuring a Security Policy

Clone a Security Policy

A VMware Cloud Web Security user may want to have a back-up of a production **Security Policy**. Instead of manually configuring a brand new **Security Policy** that matches the production security policy, users can clone the production policy and make the clone the backup.

A Security Policy is cloned on the New UI of the VMware SD-WAN Orchestrator.

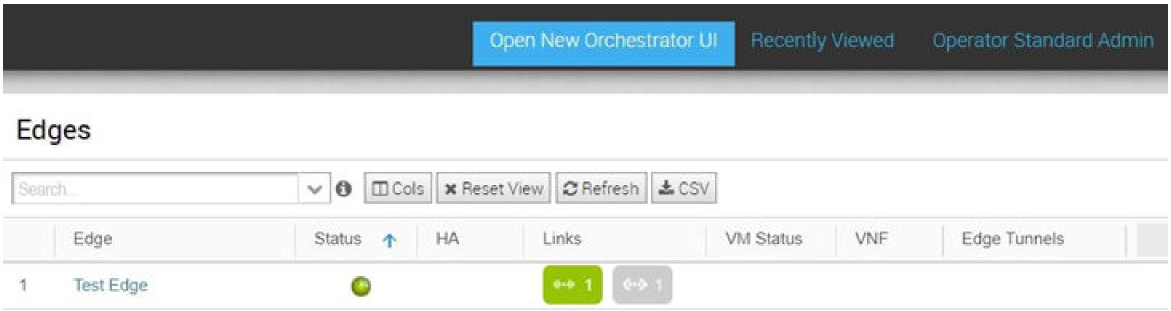
Prerequisites

To clone a Cloud Web Security (CWS) policy, a user must have one of the following roles:

- An Operator with a superuser or standard roles.
- A Partner user with a superuser or standard role.
- A Customer user with a superuser, standard, or security administrator role.

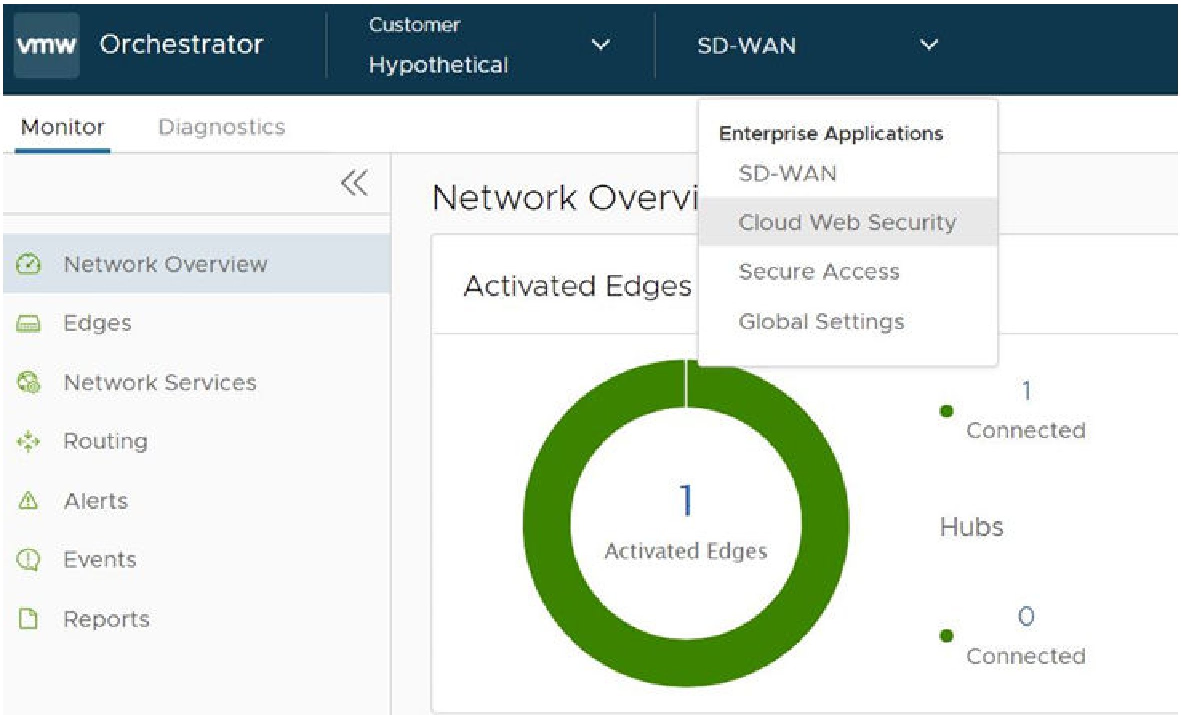
Procedure

1 In the Orchestrator portal, if not using Orchestrator version 5.1.0 or later, click the **Open New Orchestrator UI** option available at the top of the Window.



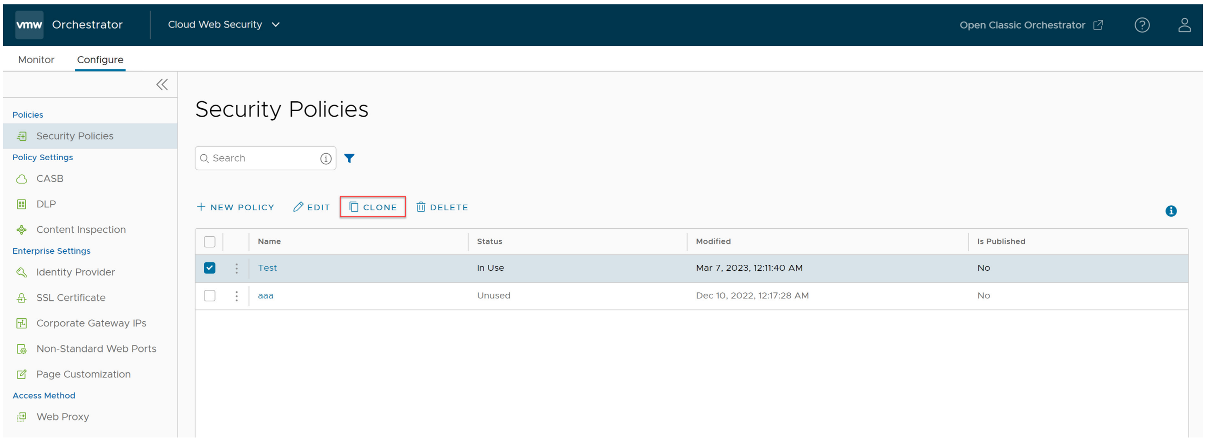
	Edge	Status	HA	Links	VM Status	VNF	Edge Tunnels
1	Test Edge	●		1 1			

2 Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab.



3 From the **SD-WAN** drop-down menu, select **Cloud Web Security**.

The **Cloud Web Security** page appears.



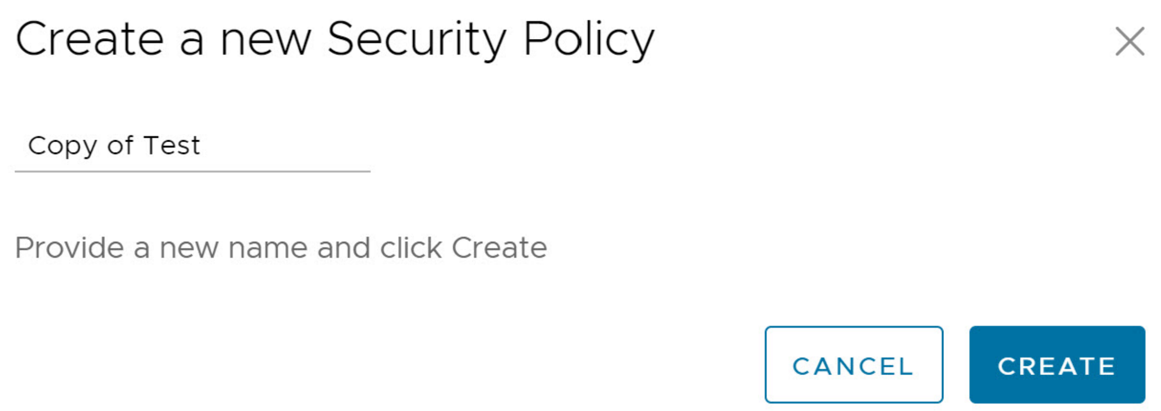
Security Policies

☐	Name	Status	Modified	Is Published
☑	Test	In Use	Mar 7, 2023, 12:11:40 AM	No
☐	aaa	Unused	Dec 10, 2022, 12:17:28 AM	No

On the **Cloud Web Security** page, user can view, create, clone, and edit Cloud Web Security policies.

4 To clone an existing Security Policy, click the **Configure > Policies > Security Policies**. On the **Security Policies** page, click **CLONE**.

The **Create a new Security Policy** pop-up window appears.



Create a new Security Policy

Copy of Test

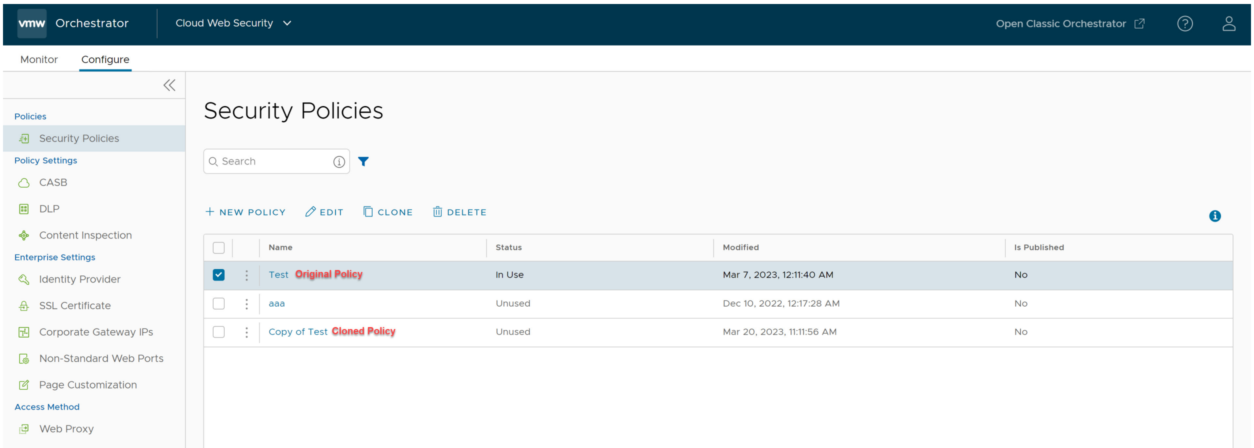
Provide a new name and click Create

5 In the textbox, there will be a default name for this cloned Security Policy. For example, if cloning a security policy with name "Test", the default name will show as **Copy of Test**. Users may either accept this name or edit the name to something they prefer (for example, **SecurityPolicy2**). Once the Security Policy name is correct, click **CREATE**.

Note The policy name must be a continuous text string with no spaces. For example, **Security Policy 2** will return an error while **SecurityPolicy2** will be accepted.

Results

A new backup Security Policy is then created and appears in the **Security Policies** page.



Security Policies

☐	Name	Status	Modified	Is Published
☑	Test **Original Policy**	In Use	Mar 7, 2023, 12:11:40 AM	No
☐	aaa	Unused	Dec 10, 2022, 12:17:28 AM	No
☐	Copy of Test **Cloned Policy**	Unused	Mar 20, 2023, 11:11:56 AM	No

Note The clone feature is not limited to the Security Policy itself. Instead of cloning the entire policy, if a user only wants to clone a set of rules within the policy, users can clone the SSL Inspection, CASB, DLP, or Web Security rules as needed.

What to do next

- Configuring a Security Policy

Configuring a Security Policy

This section describes how to configure a Security Policy for VMware Cloud Web Security.

Before you begin:

To configure a Security Policy, users must have first created a Security Policy. For specific instructions on how to create a Security Policy, see Create a Security Policy.

About this Task:

In this section, users will learn how configure the Security Policy that was created in the section titled, Create a Security Policy. When creating a Security Policy, the following are the rule categories that users can configure: Secure sockets layer (SSL) Inspection, Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Web Security, and Web Application.

When creating a Web Security policy rule, users can configure: URL Filtering, Geo-Based Filtering, Content Filtering, and Content Inspection.

Note By configuring any of these categories, users are overriding default rules.

Tip Best Practice: Blocking or Disabling the QUIC Protocol

Google developed the QUIC (Quick UDP Internet Connections) protocol to increase the performance of HTTPS and HTTP (TCP 443 and TCP 80) connections. Chrome browsers have had experimental support for it since 2014, and it is also used in Chromium (for example, Microsoft Edge, Opera, and Brave) and Android devices.

QUIC connections do not require TCP handshakes. However, SSL inspection requires TCP session information and Cloud Web Security performs SSL Inspection by default (unless a bypass rule is explicitly configured to prevent it) and thus Cloud Web Security cannot examine QUIC sessions where SSL Inspection is being done. In such instances where QUIC is activated and SSL Inspection is being performed, this can result in a policy not being applied during a user session.

To ensure that Cloud Web Security policies are consistently applied, it is recommended that the QUIC protocol is either blocked or deactivated on the browser.

To block QUIC, configure your browser or firewall to block UDP 443 and UDP 80 as these are the ports the QUIC protocol uses. When the QUIC protocol is blocked, QUIC has a failsafe to fall back to TCP. This activates SSL inspection without negatively impacting the user experience.

To deactivate QUIC on a Chromium browser, please check the documentation for the respective browser.

To deactivate QUIC on a Chrome browser:

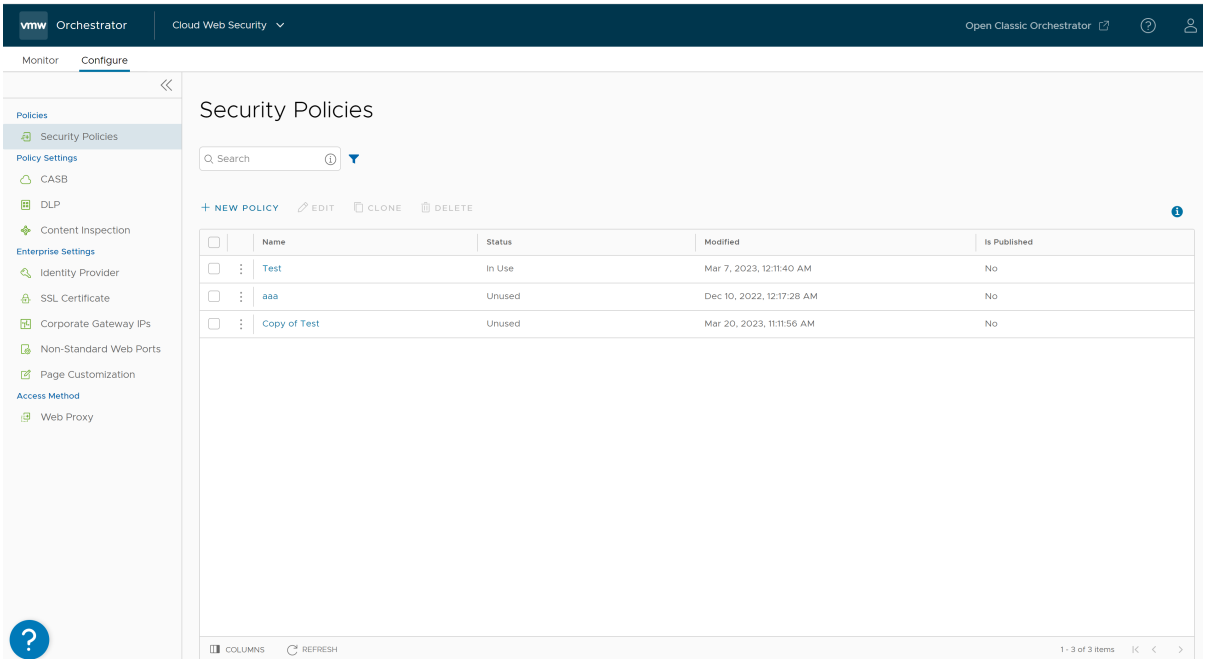
1. Open Chrome
2. In the address bar type: chrome://flags
3. In the search bar, type "quic".
4. Click the drop-down and select Disabled.
5. When Default is selected, Chrome will attempt to use QUIC.
6. When prompted, click Relaunch Now to restart Chrome and apply your changes.

For a recorded demonstration of disabling QUIC on Chrome, watch Blocking QUIC to Enable SSL Inspection.

Procedure:

To configure a Security Policy:

1. In the Security Policies page of the new UI of the VMware SD-WAN Orchestrator, click the Security Policy name for the policy to be configured.

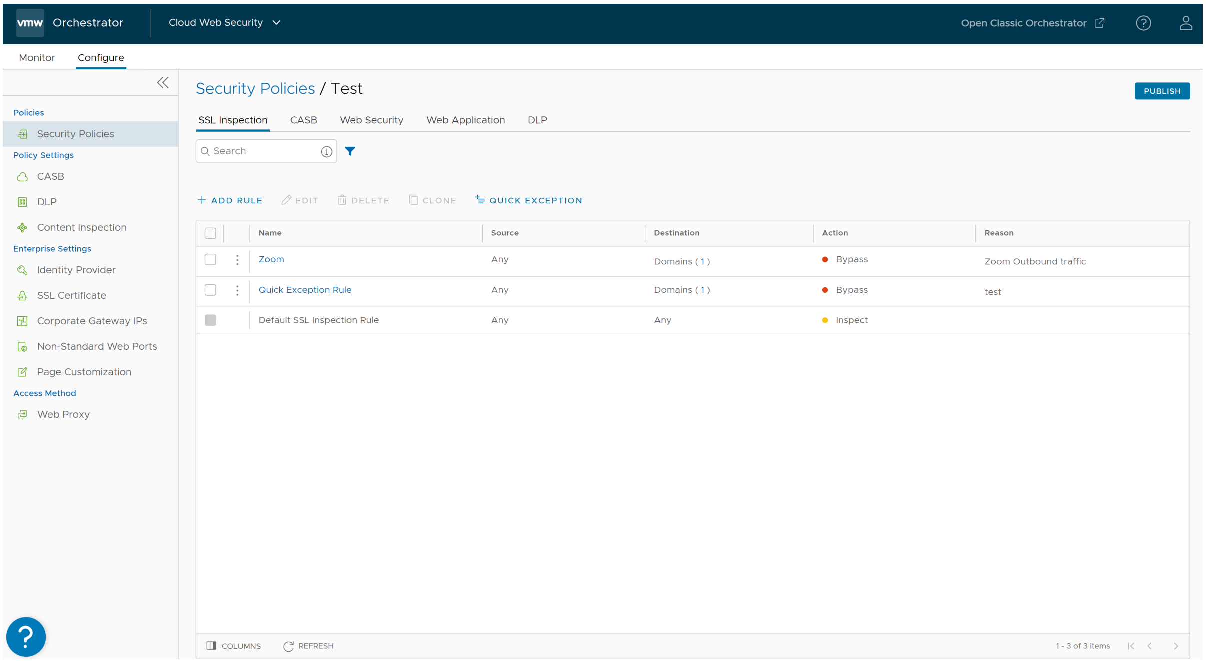


Name	Status	Modified	Is Published
Test	In Use	Mar 7, 2023, 12:11:40 AM	No
aaa	Unused	Dec 10, 2022, 12:17:28 AM	No
Copy of Test	Unused	Mar 20, 2023, 11:11:56 AM	No

The **Security Policies** screen for the selected policy appears.

2 From the selected Security Policy page, users can configure rules from the following rule categories: SSL Inspection, Cloud Access Security Broker (CASB), Web Security, Web Application, and Data Loss Prevention (DLP).

Important By default, a Security Policy has “allow all” and “decrypt all” rules. By configuring any of the five rule categories listed above, users are overriding default rules and creating a policy comprised of their own rules.



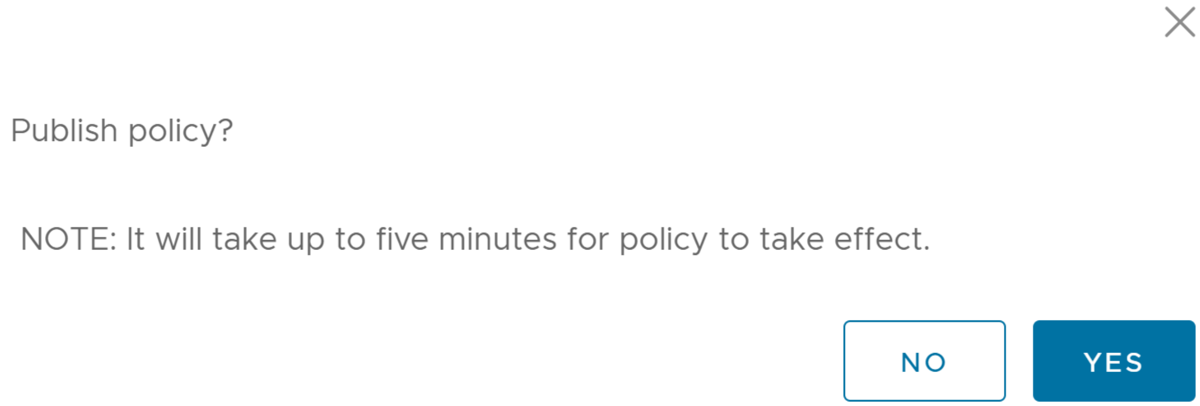
Name	Source	Destination	Action	Reason
Zoom	Any	Domains (1)	● Bypass	Zoom Outbound traffic
Quick Exception Rule	Any	Domains (1)	● Bypass	test
Default SSL Inspection Rule	Any	Any	● Inspect	

For a complete description of how to configure rules for each category, see:

- Configure SSL Inspection Rules
- Configure Cloud Access Security Broker Rules
- Configure Web Security Rules
- Configure Non-Browser Web Application Rules
- Configure Data Loss Prevention Rules

3 After configuring the Security Policy, click the **Publish** button to publish the Security Policy.

4 Click the **Yes** button in the **Publish Policy** pop up dialog to publish the policy.



Publish policy?

NOTE: It will take up to five minutes for policy to take effect.

A green banner appears on the top of the screen indicating that the Security Policy is being published.

Note A Security Policy can be published at any time in the configuration process and be republished whenever users reconfigure it.

What to do next:

- Applying a Security Policy

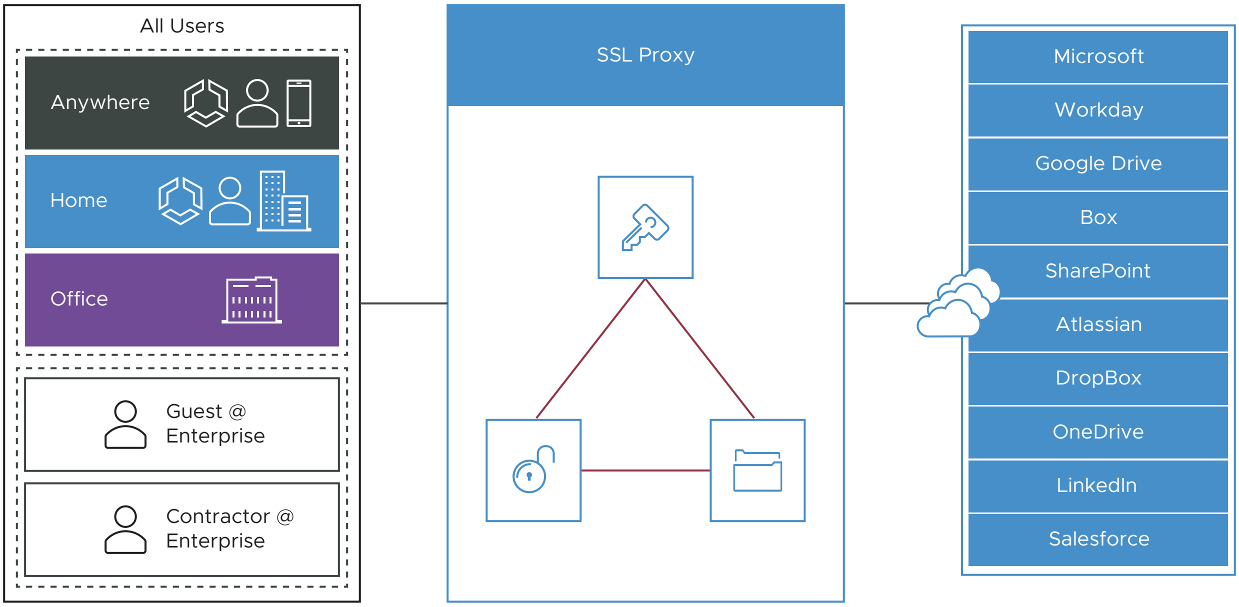
Configure SSL Inspection Rules

Describes in detail how to configure a Secure Sockets Layer (SSL) Inspection rule for a selected Security Policy.

Before you begin

To configure a Security Policy, users must have first created a Security Policy. For specific instructions on how to create a Security Policy, see Create a Security Policy.

SSL Inspection Category



Because 90 percent of Internet traffic is encrypted, there is a need to decrypt the traffic to inspect what is inside.

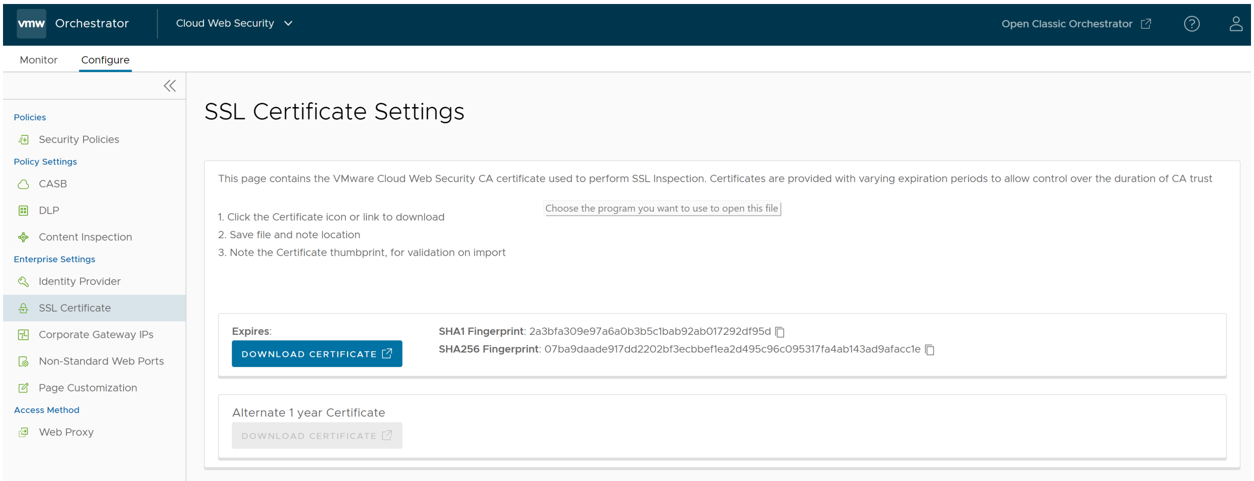
Note By default, all traffic is SSL decrypted and then inspected, forming the basis for stronger security.

However, some traffic does not like having a “man in the middle” for its traffic in the way that the SSL Inspection works. This includes traffic using certificate pinning, Mutual TLS (mTLS) and some using WebSockets. To ensure Cloud Web Security does not break these kinds of traffic, users can configure exceptions to this default SSL Inspection rule, which would allow the traffic to bypass SSL Inspection.

Tip For a list of domains that will need a bypass rule, see Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended.

Note When an SSL Bypass rule is enforced, the connection is not yet decrypted. Internal connection data, such as user identity or file content, cannot be enforced. Category and domain rules are applied, but block policies applying to users, groups, and files are not applied in conjunction with this SSL Bypass policy. As a result, URL filtering is supported when also using an SSL Bypass rule but applying user specific rules is not supported.

The SSL Root CA certificate can be downloaded by clicking on **SSL Certificate** on the left side of the **Cloud Web Security** > **Configure** > **Enterprise Settings** menu.



SSL Certificate Settings

This page contains the VMware Cloud Web Security CA certificate used to perform SSL Inspection. Certificates are provided with varying expiration periods to allow control over the duration of CA trust

Choose the program you want to use to open this file

1. Click the Certificate icon or link to download
2. Save file and note location
3. Note the Certificate thumbprint, for validation on import

Expires:

SHA1 Fingerprint: 2a3bfa309e97a6a0b3b5c1bab92ab017292df95d

SHA256 Fingerprint: 07ba9daade917dd2202bf3ecbbef1ea2d495c96c095317fa4ab143ad9afacc1e

Alternate 1 year Certificate

The **SSL Certificate Settings** page contains a downloadable VMware Cloud Web Security CA certificate used to perform SSL Inspection. To download the CA certificate:

1 Click the Certificate icon or link to download.

2 Save file and note location.

3 Note the Certificate thumbprint, for validation on import.

Configure an SSL Inspection Rule

If users want to make an exception to the default rule and does not want VMware Cloud Web Security to decrypt SSL encrypted packets, users can configure an SSL Inspection rule using one of the following two methods:

- Manual SSL Bypass
- Easy SSL Inspection Bypass/Quick Exceptions

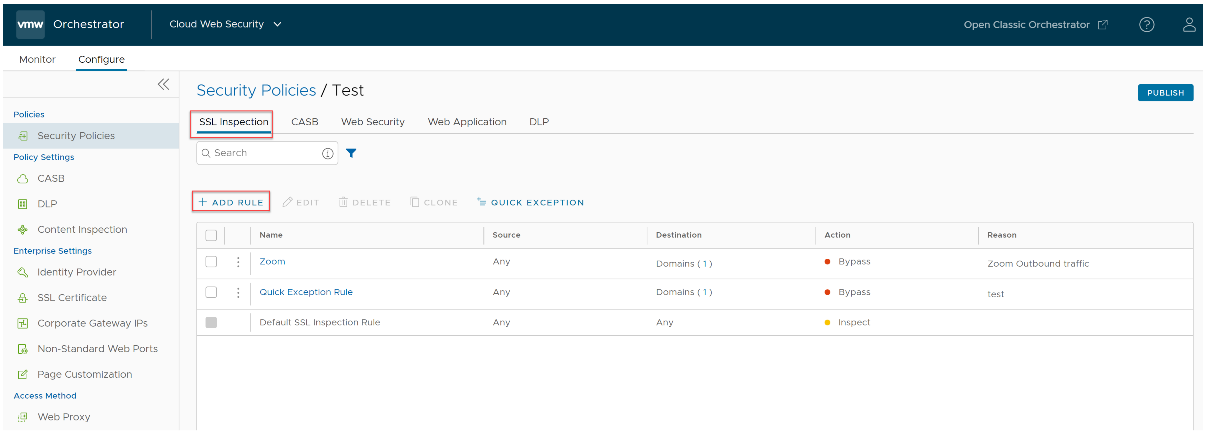
Manual SSL Bypass

User can manually configure an SSL Inspection rule based on either source, destination, or destination categories by performing the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

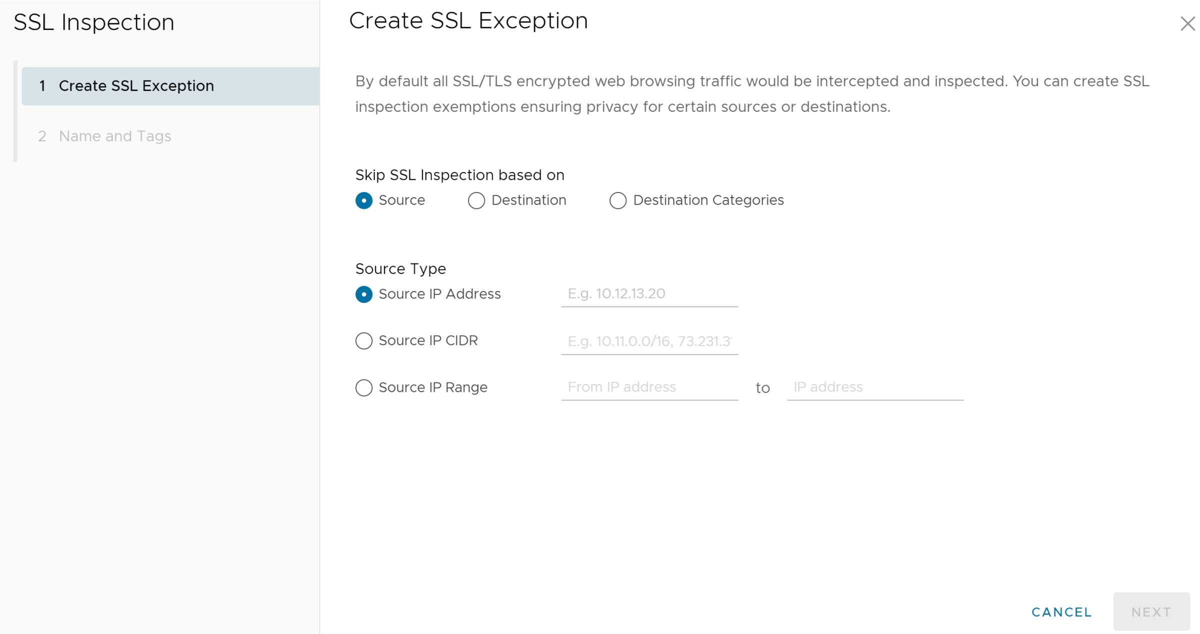
2 Select a security policy to configure SSL inspection rule and then click the **SSL Inspection** tab.

3 In the **SSL Inspection** tab of the **Security Policies** screen, click **+ ADD RULE** to configure an SSL Inspection Exception rule.



Name	Source	Destination	Action	Reason
Zoom	Any	Domains (1)	● Bypass	Zoom Outbound traffic
Quick Exception Rule	Any	Domains (1)	● Bypass	test
Default SSL Inspection Rule	Any	Any	● Inspect	

The **Create SSL Exception** screen appears.



By default all SSL/TLS encrypted web browsing traffic would be intercepted and inspected. You can create SSL inspection exemptions ensuring privacy for certain sources or destinations.

Skip SSL Inspection based on

● Source ○ Destination ○ Destination Categories

Source Type

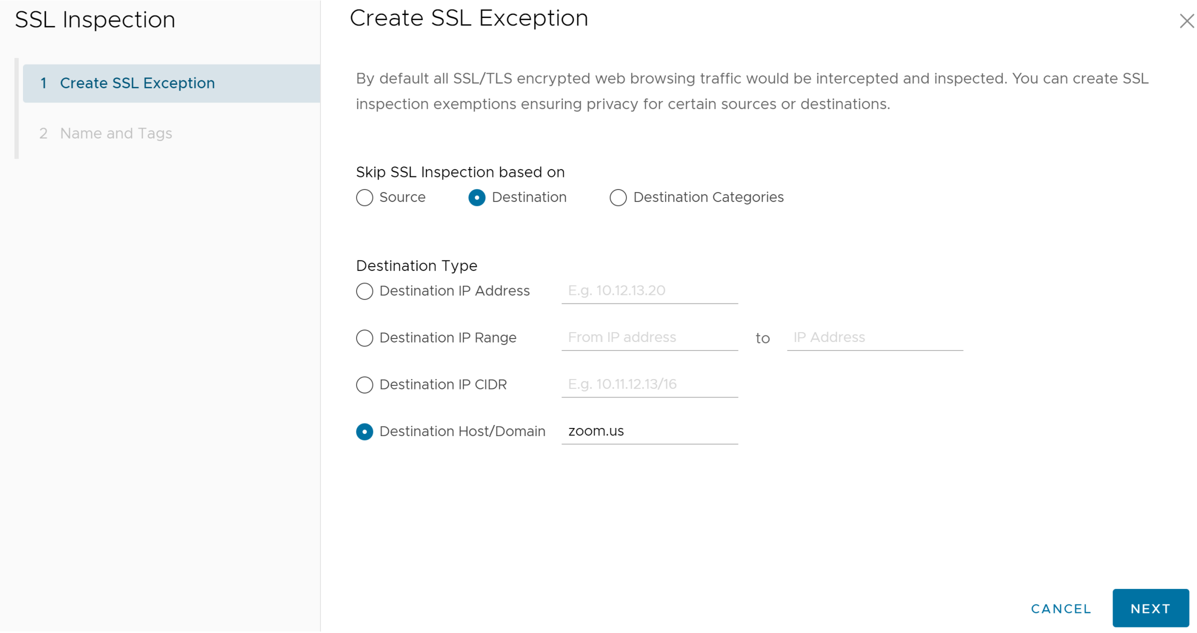
● Source IP Address E.g. 10.12.13.20

○ Source IP CIDR E.g. 10.11.0.0/16, 73.231.3

○ Source IP Range From IP address to IP address

4 In the **Create SSL Exception** screen, users can choose which type of traffic to bypass SSL Inspection by selecting either **Source**, **Destination**, or **Destination Categories**.

For example, users can create a rule that bypassed SSL inspection for all traffic destined for zoom.us, by configuring the rule as a destination rule and then choosing the destination type by either destination IP or host/domain as shown in the following sample screen.



Create SSL Exception

By default all SSL/TLS encrypted web browsing traffic would be intercepted and inspected. You can create SSL inspection exemptions ensuring privacy for certain sources or destinations.

Skip SSL Inspection based on

○ Source ● Destination ○ Destination Categories

Destination Type

○ Destination IP Address E.g. 10.12.13.20

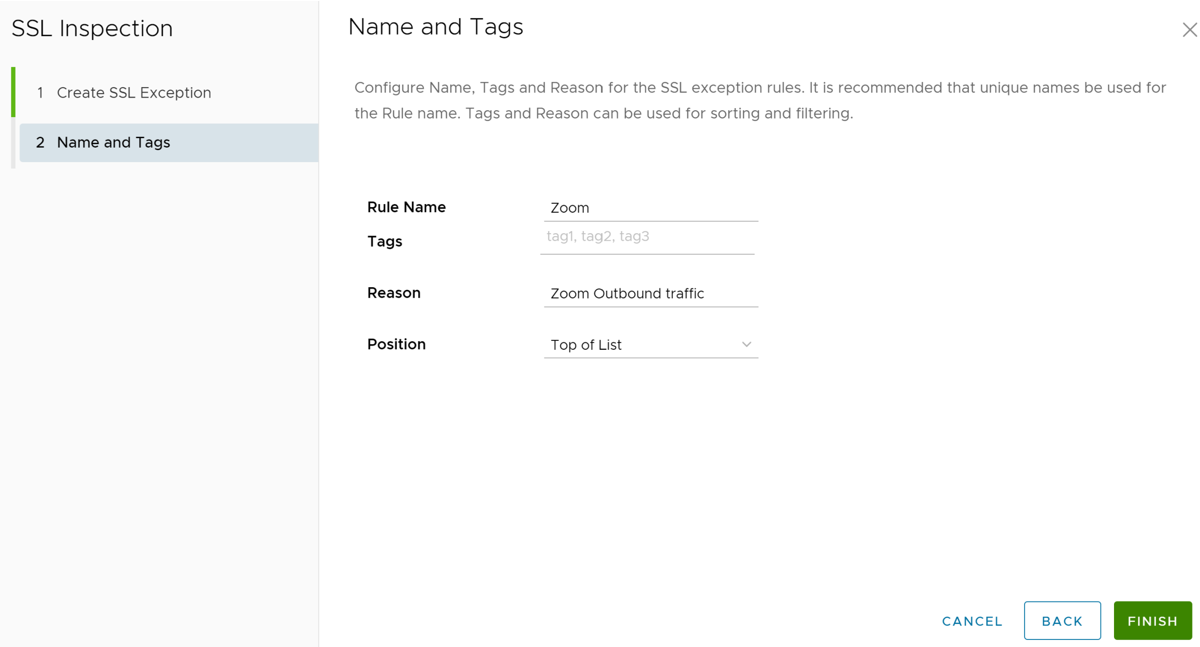
○ Destination IP Range From IP address to IP Address

○ Destination IP CIDR E.g. 10.11.12.13/16

● Destination Host/Domain zoom.us

5 Click the **Next** button.

6 In the **Name and Tags** screen, provide the Rule Name, Tags, a Reason (if needed) for why the bypass rule was created, and a Position for the rule on the list of SSL Inspection rules (the options are either 'Top of List' or 'Bottom of List').



Name and Tags

Configure Name, Tags and Reason for the SSL exception rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering.

Rule Name Zoom

Tags tag1, tag2, tag3

Reason Zoom Outbound traffic

Position Top of List

7 Click **Finish**.

The SSL Inspection rule is now added to the Security Policy.

8 Users have the following options: configure another SSL Inspection rule, configure a different Security Policy category, or if finished, click the **Publish** button to publish the Security Policy.

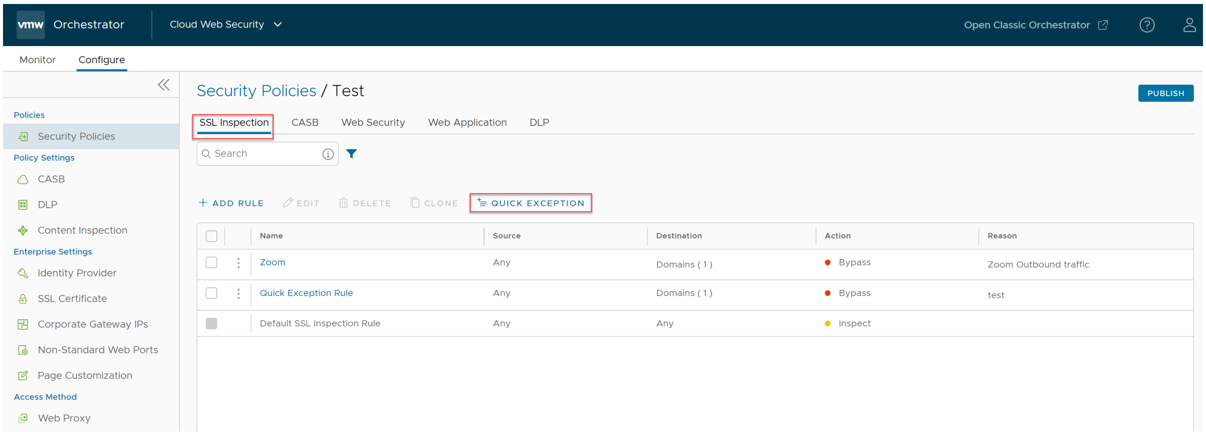
9 After publishing the Security Policy, users can Applying a Security Policy.

Easy SSL Inspection Bypass/Quick Exceptions

The Easy SSL Bypass feature allows users to bypass SSL inspection for commonly used Web applications.

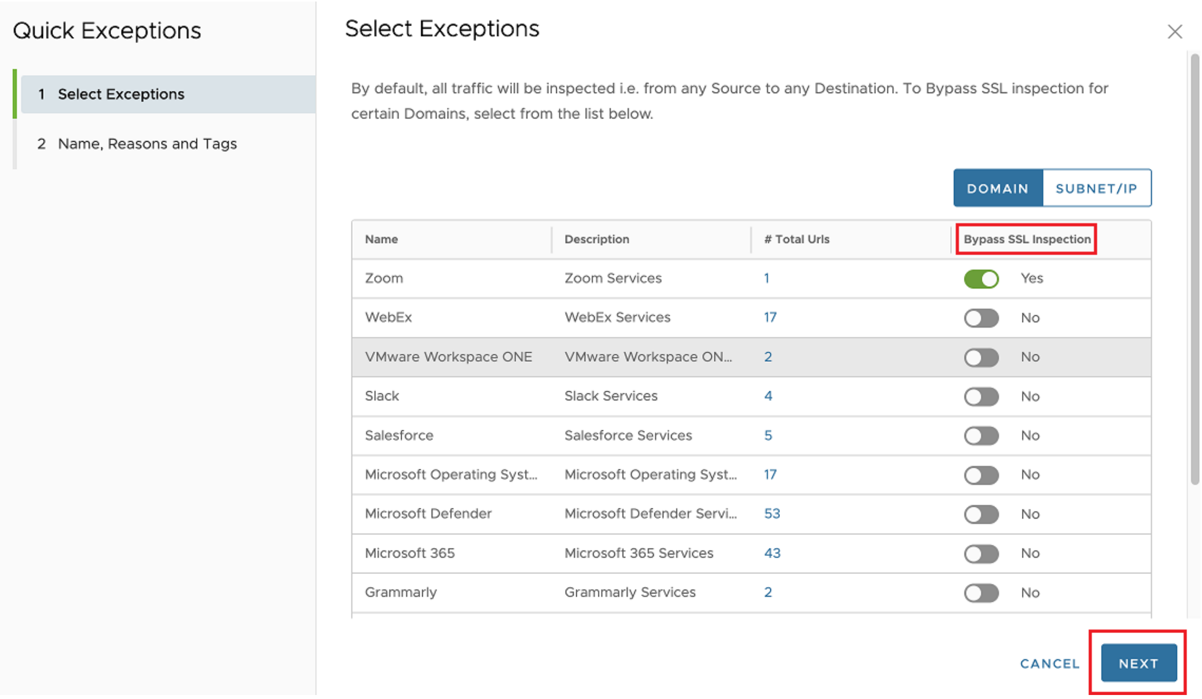
To configure an SSL Bypass rule using Quick Exception, perform the following steps:

1 On the **SSL Inspection** tab of the **Security Policies** screen, click **ADD QUICK EXCEPTION**.



Name	Source	Destination	Action	Reason
Zoom	Any	Domains (1)	● Bypass	Zoom Outbound traffic
Quick Exception Rule	Any	Domains (1)	● Bypass	test
Default SSL Inspection Rule	Any	Any	● Inspect	

The **Quick Exceptions** configuration screen appears.

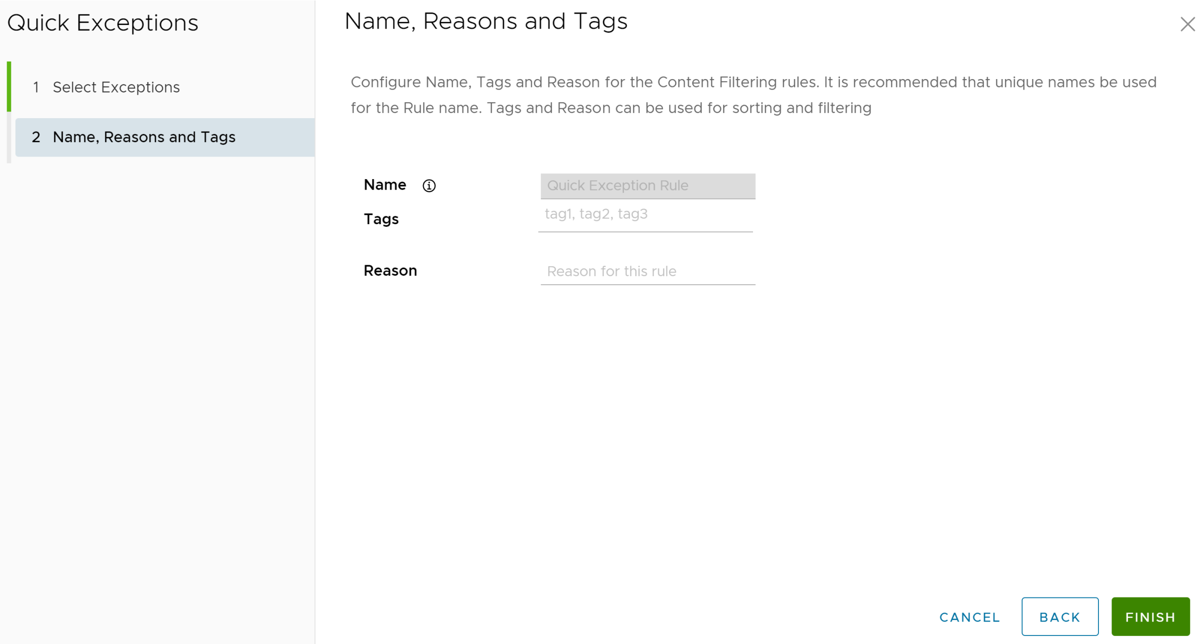


By default, all traffic will be inspected i.e. from any Source to any Destination. To Bypass SSL inspection for certain Domains, select from the list below.

Name	Description	# Total Urls	Bypass SSL Inspection
Zoom	Zoom Services	1	Yes
WebEx	WebEx Services	17	No
VMware Workspace ONE	VMware Workspace ON...	2	No
Slack	Slack Services	4	No
Salesforce	Salesforce Services	5	No
Microsoft Operating Syst...	Microsoft Operating Syst...	17	No
Microsoft Defender	Microsoft Defender Servi...	53	No
Microsoft 365	Microsoft 365 Services	43	No
Grammarly	Grammarly Services	2	No

2 To bypass SSL inspection for certain domains or subnet IP ranges, in the **Select Exceptions** page, select one or more applications that user want excepted from SSL inspection by turning on the toggle button, and click **Next**. When users select an application, all the URLs associated with the selected applications are also excluded from SSL inspection.

3 In the **Name, Reasons and Tags** screen, provide Tags and a Reason (if needed) for why the quick exception rule was created and click **Finish**.



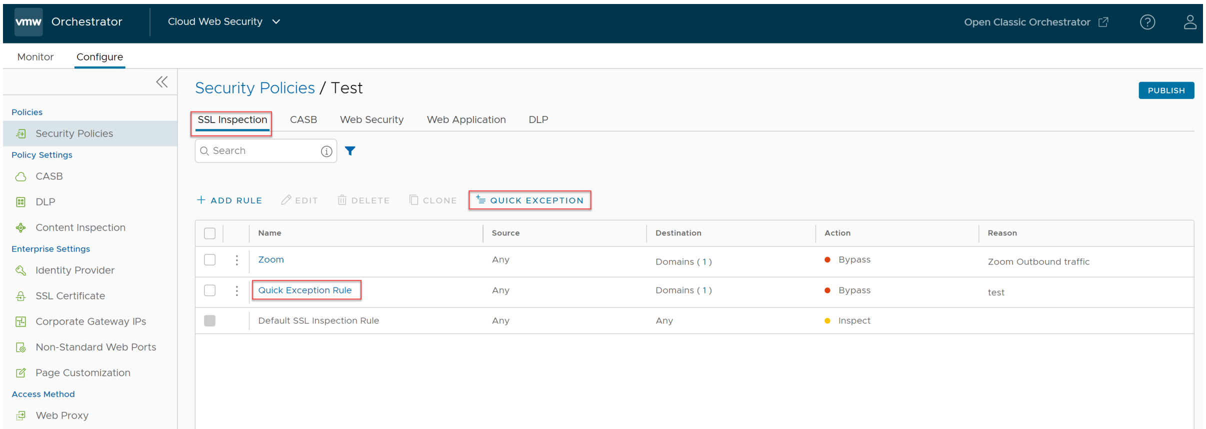
Configure Name, Tags and Reason for the Content Filtering rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering

Name: Quick Exception Rule

Tags: tag1, tag2, tag3

Reason: Reason for this rule

The **Quick Exception Rule** is created, and it appears in the SSL Inspection Rule listing page as shown in the following screenshot.



☐	Name	Source	Destination	Action	Reason
☐	Zoom	Any	Domains (1)	● Bypass	Zoom Outbound traffic
☐	Quick Exception Rule	Any	Domains (1)	● Bypass	test
☐	Default SSL Inspection Rule	Any	Any	● Inspect	

Note Only one rule is created, and no additional rules can be created. This rule is always named as "Quick Exception Rule" and the name cannot be changed in the Quick Exception wizard.

Note The rule will always be the second to last rule in the SSL Inspection Rule listing page and can quickly be accessed by clicking the **Quick Exception Rule** name. After the Quick Exception Rule is added, the **Add Quick Exceptions** button name changes to **Quick Exception**, indicating there is an existing Quick Exception Rule that can be edited, and no additional rules of this type can be added.

Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended

This page contains lists of domains and CIDRs for which configuring a bypass rule is recommended to ensure SSL Inspection does not break traffic associated with these applications.

This list of domains and CIDRs are also part of the **SSL Quick Exception List**, which can be easily toggled on/off when configuring **SSL Bypass** in Cloud Web Security.

With most Internet Web traffic encrypted, it is necessary to decrypt SSL traffic to apply advanced security controls. By default, Cloud Web Security SSL Inspection decrypts all SSL traffic for this reason.

SSL Inspection solutions use a "man-in-the-middle" technique to decrypt traffic that can disrupt specific types of communications by applications. Traffic that can break from a "man-in-the-middle" includes those that use certificate pinning, mutual TLS (mTLS), and WebSocket.

To ensure the Cloud Web Security service does not break these types of traffic, users can configure SSL Bypass rule(s) that override the default SSL Inspection behavior. Cloud Web Security users can still control traffic to these applications using the URL Filtering feature.

Tip To configure an SSL Inspection bypass rule, see Configuring a Security Policy.

Table of Contents

  - Apple
  - Cisco WebEx
  - Dropbox
  - Druva
  - GitHub
  - GoTo
  - Grammarly
  - Microsoft 365 (Formerly Office 365)
  - Microsoft Defender
  - Microsoft Operating Systems
  - RingCentral
  - Salesforce
  - Slack
  - VMware Workspace ONE
  - Zoom
- **Recommended Rules (Consolidated Applications Lists)**
  - Domains Bypass Rules
  - CIDRs Bypass Rules

Applications

Below is a list of applications and their associated domains and CIDR blocks that are known to break when SSL Inspection is applied.

Adobe

References

Category: Domains

Entries: 13

```
sstats.adobe.com, acrobat.com, stats.adobe.com, fpdownload.adobe.com, newrelic.com,
get3.adobe.com, echocdn.com, get.adobe.com, echosign.com, platformdl.adobe.com,
dlmping2.adobe.com, dlmping3.adobe.com, bam.nr-data.net
```

Apple

References

Category: Domains

Entries: 80

```
xp-cdn.apple.com, humb.apple.com, configuration.apple.com, mesu.apple.com,
gdmf.apple.com, business.apple.com, iwork.apple.com, albert.apple.com, ess.apple.com,
static.ips.apple.com, swscan.apple.com, certs.apple.com, appattest.apple.com, apple-
cloudkit.com, swdist.apple.com, identity.apple.com, push.apple.com, api.apps.apple.com,
ls.apple.com, iprofiles.apple.com, diagassets.apple.com, oscdn.apple.com, appleid.cdn-
apple.com, swdownload.apple.com, vpp.itunes.apple.com, gs.apple.com, doh.dns.apple.com,
valid.apple.com, idmsa.apple.com, axm-adm-mdm.apple.com, lcdn-registration.apple.com,
cssubmissions.apple.com, school.apple.com, bpapi.apple.com, skl.apple.com, xp.apple.com,
sq-device.apple.com, deviceenrollment.apple.com, mask.icloud.com, gnf-mr.apple.com,
ocsp2.apple.com, apps.apple.com, mask-api.icloud.com, ig.apple.com, axm-adm-scep.apple.com,
axm-adm-enroll.apple.com, fba.apple.com, smp-device-content.apple.com, swquery.apple.com,
setup.icloud.com, icloud.apple.com, icloud-content.com, axm-app.apple.com, swcdn.apple.com,
mzstatic.com, ppq.apple.com, gsa.apple.com, mask-h2.icloud.com, itunes.apple.com,
gc.apple.com, serverstatus.apple.com, gsas.apple.com, apple-livephotoskit.com,
gnf-mdn.apple.com, appleid.apple.com, gg.apple.com, updates.cdn-apple.com, lcdn-
locator.apple.com, icloud.com.cn, mdmenrollment.apple.com, ns.itunes.apple.com, cdn-
apple.com, apzones.com, tbsc.apple.com, icloud.com, osrecovery.apple.com, smoot.apple.com,
captive.apple.com, deviceservices-external.apple.com, ws-ee-maidsvc.icloud.com
```

Dropbox

References

Category: Domains

Entries: 4

```
cfl.dropboxstatic.com, dropboxusercontent.com, content.dropboxapi.com, dropbox.com
```

Druva

References

Category: Domains

Entries: 1

```
druva.com
```

GitHub

References

Category: Domains

Entries: 3

```
github.com, gist.githubusercontent.com, githubusercontent.com
```

GoTo

Category: Domains

References

Entries: 75

```
internap.net, api.opentok.com, 123rescue.com, jointraining.com, hvoice.net, meet.goto.com,
logmein.eu, fastsupport.com, gotomeeting.com, joinwebinar.com, helpme.net, jiveip.net,
getgoservices.net, lastpass.eu, lmi-antivirus-live.azureedge.net, logmein-gateway.com,
gotomeet.at, google-analytics.com, gotoassist.at, browse.logmeinusercontent.com,
webinar.com, gotoassist.me, gotoroom.com, gotomeet.me, enterprise.opentok.com,
lmi-appupdates-live.azureedge.net, jive.com, joingotomeeting.com, getgocdn.com, psyjs-
cdn.personify.live, LogMeIn123.com, logmeinrescue.com, expertcity.com, anvil.opentok.com,
gotostage.com, goto.com, googleapis.com, static.opentok.com, logmeinusercontent.com,
dolbyvoice.com, join.me, getgoservices.com, gototraining.com, logmein.com, firebaseapp.com,
accounts.logme.in, cdn.walkme.com, hamachi.cc, gotoconference.com, logmeininc.com,
openvoice.com, psyjs-cdn.nuvixa.com, goto-desktop.s3.amazonaws.com, onjive.com, go2assist.me,
firebaseio.com, gofastchat.com, tokbox.com, goto-rtc.com, logmeinrescue-enterprise.com,
jmp.tw, internapcdn.net, gotowebinar.com, assist.com, gotomypc.com, support.me, lastpass.com,
app.goto.com, getgo.com, rtcprov.net, gotoassist.com, cdngetgo.com, raas.io, google.com,
logmeinrescue.eu
```

Grammarly (Domains)

References

Category: Domains

Entries: 2

```
grammarly.io, grammarly.com
```

Microsoft 365 (Formerly Office 365)

References

Category: Domains

Entries: 43

```
companymanager.microsoftonline.com, login.microsoftonline.com, officeapps.live.com,
becws.microsoftonline.com, passwordreset.microsoftonline.com, broadcast.skype.com,
sharepoint.com, loginex.microsoftonline.com, lync.com, login.microsoftonline-
p.com, msidentity.com, outlook.office.com, msftidentity.com,
security.microsoft.com, login-us.microsoftonline.com, autologon.microsoftazuread-
sso.com, logincert.microsoftonline.com, accounts.accesscontrol.windows.net,
defender.microsoft.com, login.microsoft.com, clientconfig.microsoftonline-p.net,
provisioningapi.microsoftonline.com, account.office.net, outlook.office365.com,
compliance.microsoft.com, api.passwordreset.microsoftonline.com, protection.office.com,
office.live.com, adminwebservice.microsoftonline.com, protection.outlook.com,
auth.microsoft.com, skypeforbusiness.com, graph.microsoft.com, login.windows.net,
online.office.com, nexus.microsoftonline-p.com, account.activedirectory.windowsazure.com,
mail.protection.outlook.com, graph.windows.net, ccs.login.microsoftonline.com,
device.login.microsoftonline.com, teams.microsoft.com, smtp.office365.com
```

Microsoft Defender

References

Category: Domains

Entries: 53

```
ussus4eastprod.blob.core.windows.net, wsus2westprod.blob.core.windows.net,
ussus4westprod.blob.core.windows.net, winatp-gw-neu.microsoft.com,
automatedirstrprdeus3.blob.core.windows.net, automatedirstrprduks.blob.core.windows.net,
automatedirstrprdcus3.blob.core.windows.net, automatedirstrprdeus.blob.core.windows.net,
wsuk1westprod.blob.core.windows.net, usseu1northprod.blob.core.windows.net,
ussuk1southprod.blob.core.windows.net, officecdn-microsoft-com.akamaized.net,
unitedkingdom.x.cp.wd.microsoft.com, automatedirstrprdneu.blob.core.windows.net,
wdcp.microsoft.com, automatedirstrprdcus.blob.core.windows.net, europe.x.cp.wd.microsoft.com,
ussus2eastprod.blob.core.windows.net, wseu1westprod.blob.core.windows.net, us-
v20.events.data.microsoft.com, automatedirstrprdneu3.blob.core.windows.net,
wd.microsoft.com, winatp-gw-neu3.microsoft.com, winatp-gw-cus.microsoft.com,
x.cp.wd.microsoft.com, winatp-gw-cus3.microsoft.com, wsus1westprod.blob.core.windows.net,
wsus2eastprod.blob.core.windows.net, wseu1northprod.blob.core.windows.net,
ussus2westprod.blob.core.windows.net, wsuk1southprod.blob.core.windows.net,
ussuk1westprod.blob.core.windows.net, automatedirstrprdweu.blob.core.windows.net, winatp-
gw-eus.microsoft.com, packages.microsoft.com, unitedstates.x.cp.wd.microsoft.com,
wsus1eastprod.blob.core.windows.net, winatp-gw-weu3.microsoft.com,
automatedirstrprdweu3.blob.core.windows.net, automatedirstrprdukw.blob.core.windows.net,
ussus1westprod.blob.core.windows.net, eu-v20.events.data.microsoft.com,
ussus3westprod.blob.core.windows.net, uk-v20.events.data.microsoft.com,
usseu1westprod.blob.core.windows.net, winatp-gw-uks.microsoft.com,
ussus1eastprod.blob.core.windows.net, ussus3eastprod.blob.core.windows.net,
cdn.x.cp.wd.microsoft.com, winatp-gw-weu.microsoft.com, winatp-gw-eus3.microsoft.com, winatp-
gw-ukw.microsoft.com, events.data.microsoft.com
```

Microsoft Operating Systems

References

Category: Domains

Entries: 17

```
musicimage.xboxlive.com, dl.delivery.mp.microsoft.com, windowsupdate.com, store-
images.microsoft.com, sls.microsoft.com, windowsupdate.microsoft.com, wustat.windows.com,
prod.do.dsp.mp.microsoft.com, mp.microsoft.com, download.microsoft.com, cdn.microsoft.com,
tsfe.trafficshaping.dsp.mp.microsoft.com, media-assetcatalog.microsoft.com, store-images.s-
microsoft.com, mediadiscovery.microsoft.com, update.microsoft.com, ntservicepack.microsoft.com
```

RingCentral

References

Category: CIDRs

Entries: 9

```
199.68.212.0/22, 192.209.24.0/21, 199.255.120.0/22, 80.81.128.0/20, 208.87.40.0/22,
104.245.56.0/21, 66.81.240.0/20, 185.23.248.0/22, 103.44.68.0/22
```

Salesforce

References

Category: Domains

Entries: 5

```
content.force.com, salesforce.com, lightning.force.com, visual.force.com, documentforce.com
```

Slack

References

Category: Domains

Entries: 4

```
wss-backup.slack.com, wss-mobile.slack.com, lb.slack-msgs.com, wss-primary.slack.com
```

VMware Workspace ONE

References

Category: Domains

SSL Pinning and Outbound SSL Interception Proxies (2960709)

Entries: 2

```
vidmpreview.com, awmdm.com
```

WebEx

References

Category: Domains

Entries: 17

```
vbrickrev.com, webex.com, slido.com, lencr.org, accompany.com, godaddy.com, intel.com,
sli.do, wbx2.com, webexcontent.com, appdynamics.com, identrust.com, digicert.com,
data.logentries.com, quovadisglobal.com, eum-appdynamics.com, ciscospark.com
```

WebEx

Categoty: Subnets

Entries: 26

```
20.53.87.0/24, 173.39.224.0/19, 150.253.128.0/17, 170.133.128.0/18, 40.119.234.0/24,
66.114.160.0/20, 44.234.52.192/26, 66.163.32.0/19, 20.68.154.0/24, 20.50.235.0/24,
20.120.238.0/23, 210.4.192.0/20, 173.243.0.0/20, 20.76.127.0/24, 62.109.192.0/18,
216.151.128.0/19, 23.89.0.0/16, 114.29.192.0/19, 20.108.99.0/24, 207.182.160.0/19,
20.57.87.0/24, 209.197.192.0/19, 69.26.160.0/19, 64.68.96.0/19, 52.232.210.0/24, 170.72.0.0/16
```

Zoom

References

Category: Domains

Entries: 1

```
zoom.us
```

Recommended Rules (Consolidated Applications Lists)

The rules below consolidate every application listed above and can be easily copied and pasted into a single Cloud Web Security SSL Inspection bypass rule. However, should users prefer to not include an exemption for every application covered in this document, users can create individual bypass rule(s) for specific application(s) using the information provided above.

SSL Bypass Domains

Entries: 320

```
automatedirstrprdweu3.blob.core.windows.net, oscdn.apple.com, goto-desktop.s3.amazonaws.com,
gc.apple.com, logmeinrescue.com, broadcast.skype.com, meet.goto.com, visual.force.com,
msftidentity.com, wsus2westprod.blob.core.windows.net, sq-device.apple.com, cdn-apple.com,
identrust.com, content.force.com, gdmf.apple.com, mesu.apple.com, icloud.com,
musicimage.xboxlive.com, tbsc.apple.com, osrecovery.apple.com, firebaseapp.com,
jmp.tw, cssubmissions.apple.com, quovadisglobal.com, outlook.office.com,
companymanager.microsoftonline.com, automatedirstrprdcus3.blob.core.windows.net, axm-
app.apple.com, goto.com, lastpass.com, mzstatic.com, wss-primary.slack.com, lastpass.eu,
druva.com, sharepoint.com, ocsp2.apple.com, automatedirstrprdneu.blob.core.windows.net,
mask-api.icloud.com, hvoice.net, automatedirstrprdeus3.blob.core.windows.net,
becws.microsoftonline.com, deviceenrollment.apple.com, appleid.apple.com, smtp.office365.com,
github.com, serverstatus.apple.com, store-images.microsoft.com, lcdn-registration.apple.com,
app.goto.com, browse.logmeinusercontent.com, login.microsoftonline-p.com, gnf-mr.apple.com,
wsuk1southprod.blob.core.windows.net, wseu1westprod.blob.core.windows.net, online.office.com,
lync.com, assist.com, smoot.apple.com, automatedirstrprdcus.blob.core.windows.net,
dolbyvoice.com, eu-v20.events.data.microsoft.com, psyjs-cdn.personify.live, skl.apple.com,
webexcontent.com, appattest.apple.com, captive.apple.com, sls.microsoft.com, icloud.com.cn,
google.com, acrobat.com, enterprise.opentok.com, ussus3westprod.blob.core.windows.net,
deviceservices-external.apple.com, bpapi.apple.com, content.dropboxapi.com,
getgocdn.com, ussus4eastprod.blob.core.windows.net, wsus2eastprod.blob.core.windows.net,
mask-h2.icloud.com, logmein.com, iprofiles.apple.com, logmeininc.com,
usseu1westprod.blob.core.windows.net, automatedirstrprduks.blob.core.windows.net,
graph.microsoft.com, winatp-gw-eus.microsoft.com, vpp.itunes.apple.com, grammarly.com,
dlmping3.adobe.com, accounts.logme.in, api.passwordreset.microsoftonline.com,
swquery.apple.com, wbx2.com, vidmpreview.com, ussuk1westprod.blob.core.windows.net,
lmi-antivirus-live.azureedge.net, gist.githubusercontent.com, cfl.dropboxstatic.com,
dlmping2.adobe.com, fpdownload.adobe.com, lightning.force.com, xp-cdn.apple.com,
adminwebservice.microsoftonline.com, gg.apple.com, office.live.com, mask.icloud.com,
ccs.login.microsoftonline.com, iwork.apple.com, outlook.office365.com,
wsus1westprod.blob.core.windows.net, tsfe.trafficshaping.dsp.mp.microsoft.com, vbrickrev.com,
events.data.microsoft.com, europe.x.cp.wd.microsoft.com, webinar.com, itunes.apple.com,
logmeinrescue-enterprise.com, jiveip.net, ls.apple.com, apple-cloudkit.com,
ntservicepack.microsoft.com, xp.apple.com, gotoassist.me, getgoservices.net,
diagassets.apple.com, security.microsoft.com, automatedirstrprdeus.blob.core.windows.net,
clientconfig.microsoftonline-p.net, media-assetcatalog.microsoft.com, newrelic.com,
gofastchat.com, officecdn-microsoft-com.akamaized.net, logincert.microsoftonline.com,
usseu1northprod.blob.core.windows.net, gotomypc.com, winatp-gw-eus3.microsoft.com,
wustat.windows.com, dropbox.com, wss-mobile.slack.com, loginex.microsoftonline.com,
ussus2eastprod.blob.core.windows.net, gotomeet.me, onjive.com, data.logentries.com,
wd.microsoft.com, logmeinrescue.eu, idmsa.apple.com, ussus2westprod.blob.core.windows.net,
ussus1westprod.blob.core.windows.net, x.cp.wd.microsoft.com, winatp-gw-ukw.microsoft.com,
wseu1northprod.blob.core.windows.net, gotowebinar.com, download.microsoft.com, intel.com,
uk-v20.events.data.microsoft.com, unitedstates.x.cp.wd.microsoft.com, digicert.com,
unitedkingdom.x.cp.wd.microsoft.com, automatedirstrprdneu3.blob.core.windows.net,
getgoservices.com, echocdn.com, awmdm.com, internapcdn.net, gnf-mdn.apple.com,
ciscospark.com, protection.office.com, rtcprov.net, lmi-appupdates-live.azureedge.net,
echosign.com, expertcity.com, login.microsoft.com, gotoassist.com, us-
v20.events.data.microsoft.com, albert.apple.com, gotoroom.com, winatp-gw-cus.microsoft.com,
lencr.org, officeapps.live.com, gs.apple.com, tokbox.com, ig.apple.com,
ws-ee-maidsvc.icloud.com, gotoconference.com, winatp-gw-neu.microsoft.com,
githubusercontent.com, gotoassist.at, automatedirstrprdukw.blob.core.windows.net,
hamachi.cc, push.apple.com, winatp-gw-neu3.microsoft.com, logmeinusercontent.com,
api.opentok.com, school.apple.com, grammarly.io, support.me, teams.microsoft.com,
salesforce.com, swdist.apple.com, joinwebinar.com, certs.apple.com, swcdn.apple.com,
wsuk1westprod.blob.core.windows.net, google-analytics.com, gsa.apple.com, axm-
adm-enroll.apple.com, passwordreset.microsoftonline.com, eum-appdynamics.com,
smp-device-content.apple.com, apps.apple.com, windowsupdate.microsoft.com,
gotomeeting.com, ppq.apple.com, login-us.microsoftonline.com, windowsupdate.com,
account.activedirectory.windowsazure.com, ussus4westprod.blob.core.windows.net,
compliance.microsoft.com, firebaseio.com, graph.windows.net, identity.apple.com, logmein.eu,
go2assist.me, icloud.apple.com, cdn.x.cp.wd.microsoft.com, mediadiscovery.microsoft.com,
ussus1eastprod.blob.core.windows.net, 123rescue.com, ns.itunes.apple.com,
ussus3eastprod.blob.core.windows.net, swscan.apple.com, provisioningapi.microsoftonline.com,
jointraining.com, valid.apple.com, sli.do, mp.microsoft.com, nexus.microsoftonline-
p.com, swdownload.apple.com, setup.icloud.com, device.login.microsoftonline.com,
doh.dns.apple.com, automatedirstrprdweu.blob.core.windows.net, lcdn-locator.apple.com,
static.opentok.com, get3.adobe.com, fastsupport.com, joingotomeeting.com, helpme.net,
bam.nr-data.net, updates.cdn-apple.com, gotostage.com, business.apple.com, lb.slack-
msgs.com, gototraining.com, join.me, winatp-gw-cus3.microsoft.com, appleid.cdn-apple.com,
ussuk1southprod.blob.core.windows.net, protection.outlook.com, winatp-gw-uks.microsoft.com,
sstats.adobe.com, logmein-gateway.com, wss-backup.slack.com, platformdl.adobe.com,
apzones.com, axm-adm-scep.apple.com, fba.apple.com, prod.do.dsp.mp.microsoft.com,
wdcp.microsoft.com, cdn.microsoft.com, winatp-gw-weu.microsoft.com, static.ips.apple.com,
gsas.apple.com, get.adobe.com, LogMeIn123.com, mail.protection.outlook.com,
accounts.accesscontrol.windows.net, openvoice.com, dl.delivery.mp.microsoft.com,
mdmenrollment.apple.com, msidentity.com, cdngetgo.com, accompany.com, skypeforbusiness.com,
api.apps.apple.com, googleapis.com, ess.apple.com, auth.microsoft.com, getgo.com,
login.microsoftonline.com, goto-rtc.com, anvil.opentok.com, jive.com, documentforce.com,
axm-adm-mdm.apple.com, internap.net, slido.com, cdn.walkme.com, configuration.apple.com,
psyjs-cdn.nuvixa.com, winatp-gw-weu3.microsoft.com, account.office.net, humb.apple.com,
godaddy.com, update.microsoft.com, dropboxusercontent.com, webex.com, store-images.s-
microsoft.com, stats.adobe.com, apple-livephotoskit.com, zoom.us, appdynamics.com,
login.windows.net, autologon.microsoftazuread-sso.com, wsus1eastprod.blob.core.windows.net,
gotomeet.at, icloud-content.com, packages.microsoft.com, defender.microsoft.com, raas.io
```

SSL Bypass CIDRs

```
104.245.56.0/21, 185.23.248.0/22, 80.81.128.0/20, 199.255.120.0/22, 192.209.24.0/21,
199.68.212.0/22, 103.44.68.0/22, 66.81.240.0/20, 208.87.40.0/22, 20.53.87.0/24,
173.39.224.0/19, 150.253.128.0/17, 170.133.128.0/18, 40.119.234.0/24, 66.114.160.0/20,
44.234.52.192/26, 66.163.32.0/19, 20.68.154.0/24, 20.50.235.0/24, 20.120.238.0/23,
210.4.192.0/20, 173.243.0.0/20, 20.76.127.0/24, 62.109.192.0/18, 216.151.128.0/19,
23.89.0.0/16, 114.29.192.0/19, 20.108.99.0/24, 207.182.160.0/19, 20.57.87.0/24,
209.197.192.0/19, 69.26.160.0/19, 64.68.96.0/19, 52.232.210.0/24, 170.72.0.0/16
```

Configure Cloud Access Security Broker Rules

Describes in detail how to configure a Cloud Access Security Broker (CASB) rule for a selected Security Policy.

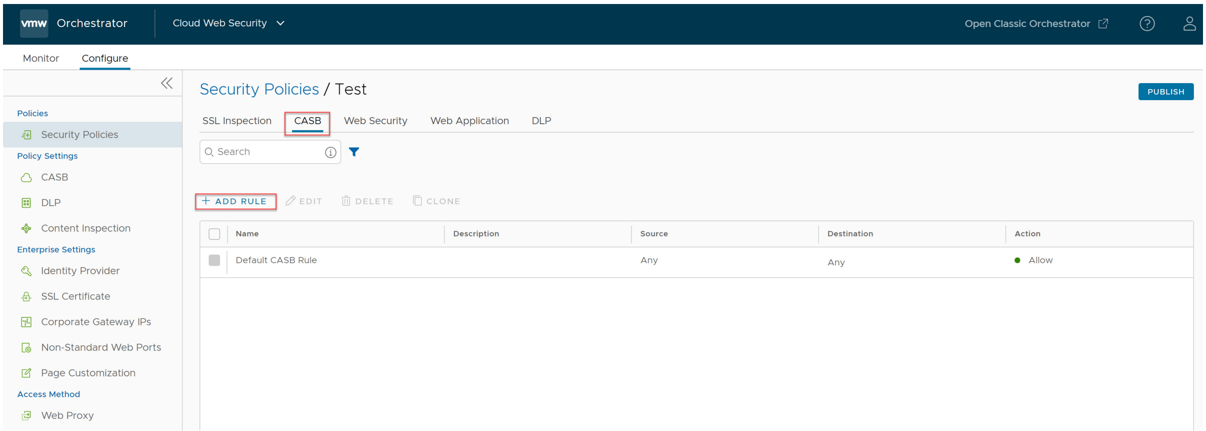
Before you begin

To configure a Security Policy, users must have first created a Security Policy. For specific instructions on how to create a Security Policy, see Create a Security Policy.

Configuration Steps

To configure a CASB rule, perform the following steps:

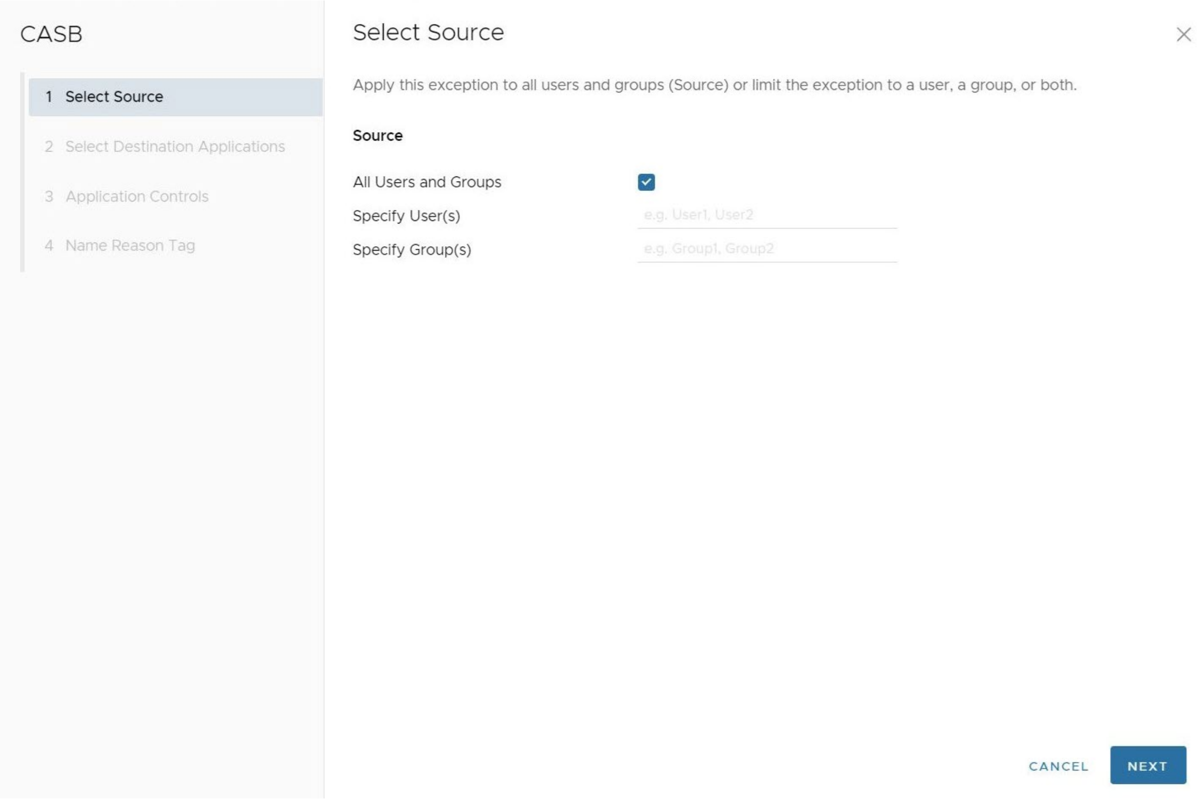
1. Navigate to **Cloud Web Security > Configure > Security Policies**.
2. Select a security policy to configure CASB rule and then click the **CASB** tab.
3. In the **CASB** tab of the **Security Policies** screen, click **+ ADD RULE**.



☐	Name	Description	Source	Destination	Action
☐	Default CASB Rule		Any	Any	● Allow

The **Select Source** screen appears.

4. In the **Select Source** screen, select the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.



Select Source

Apply this exception to all users and groups (Source) or limit the exception to a user, a group, or both.

Source

All Users and Groups ☑

Specify User(s) e.g. User1, User2

Specify Group(s) e.g. Group1, Group2

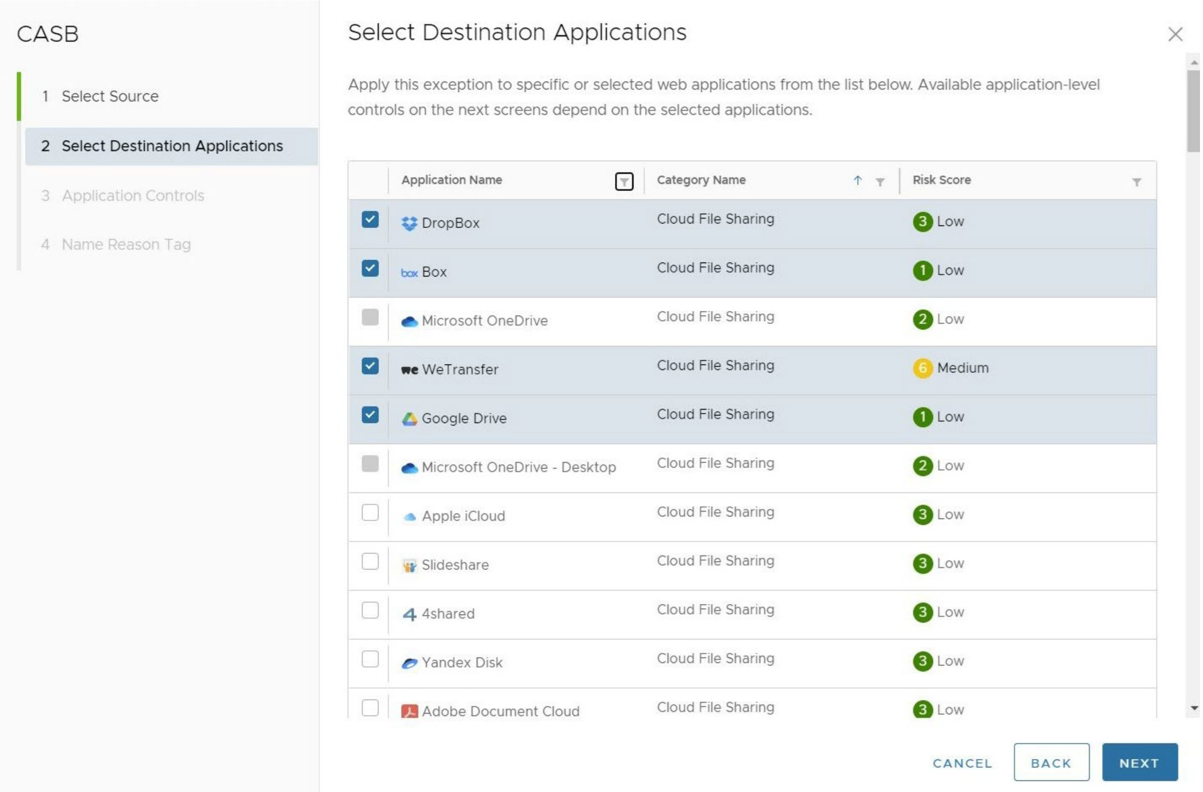
Note **All Users and Groups** is the only option for customers that do not have an Identity Provider (IdP) like Workspace ONE or Azure Active Directory (AD) configured for Cloud Web Security.

Important Cloud Web Security must be configured with an Identity Provider (IdP) like Workspace ONE or Azure Active Directory (AD) for specific Users and Groups to work.

Click **Next**, the **Select Destination Applications** screen appears.

5 In the **Select Destination Applications** screen, users can configure the CASB Control rule with one or more applications which will be applied to the rule. The selection screen allows users to sort applications by name, category name, or risk score.

Note At the bottom of the screen, users can configure the number of applications shown at one time, to a maximum of 100. The default value is 10. Users also have the option of showing all applications or only the selected applications.



Select Destination Applications

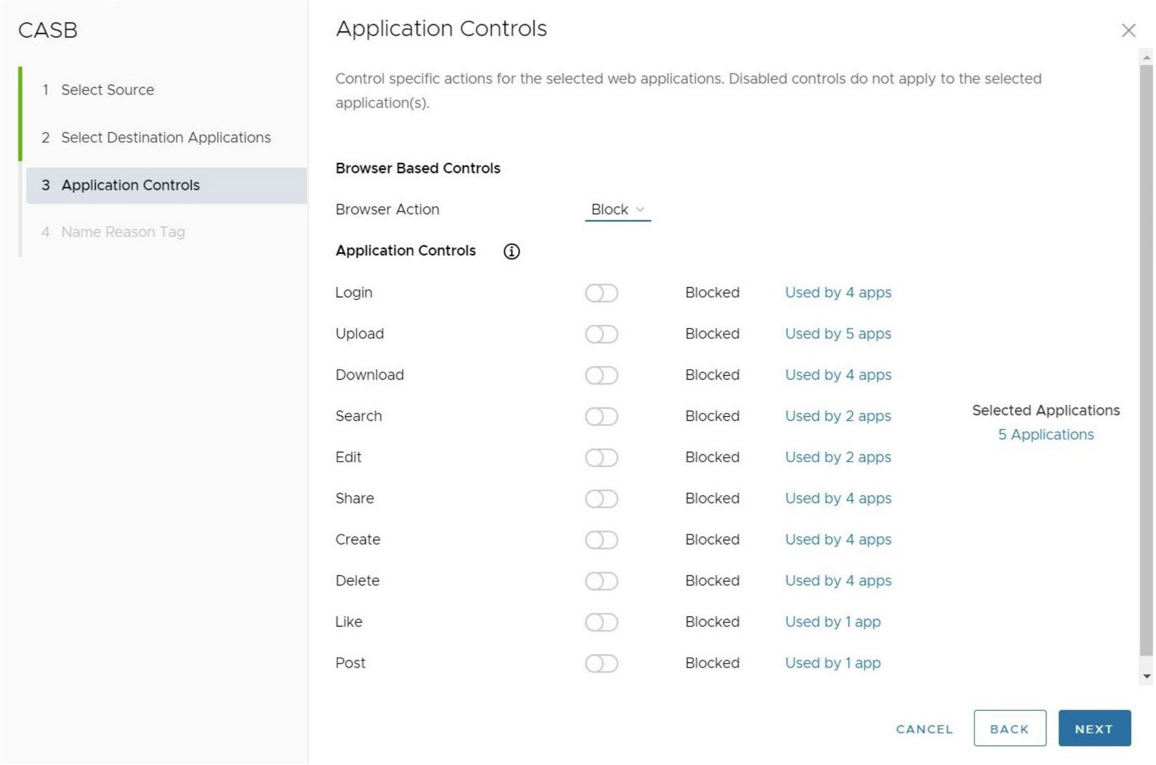
Apply this exception to specific or selected web applications from the list below. Available application-level controls on the next screens depend on the selected applications.

	Application Name	Category Name	Risk Score
☑	DropBox	Cloud File Sharing	3 Low
☑	Box	Cloud File Sharing	1 Low
☐	Microsoft OneDrive	Cloud File Sharing	2 Low
☑	WeTransfer	Cloud File Sharing	6 Medium
☑	Google Drive	Cloud File Sharing	1 Low
☐	Microsoft OneDrive - Desktop	Cloud File Sharing	2 Low
☐	Apple iCloud	Cloud File Sharing	3 Low
☐	Slideshare	Cloud File Sharing	3 Low
☐	4shared	Cloud File Sharing	3 Low
☐	Yandex Disk	Cloud File Sharing	3 Low
☐	Adobe Document Cloud	Cloud File Sharing	3 Low

After selecting the applications for this CASB Control rule, click **Next**.

6 In the **Applications Controls** screen, users can configure application control actions for the selected web applications that they can either block or allow. This includes Login, Upload, Download, Search, Edit, Share, Create, Delete, Like, and Post. Users can choose two paths for controlling the selected applications:

   a Users can select to block all application controls, in effect preventing the selected applications from operating in any way on the client's browser.



CASB

1 Select Source

2 Select Destination Applications

3 Application Controls

4 Name Reason Tag

Application Controls

Control specific actions for the selected web applications. Disabled controls do not apply to the selected application(s).

Browser Based Controls

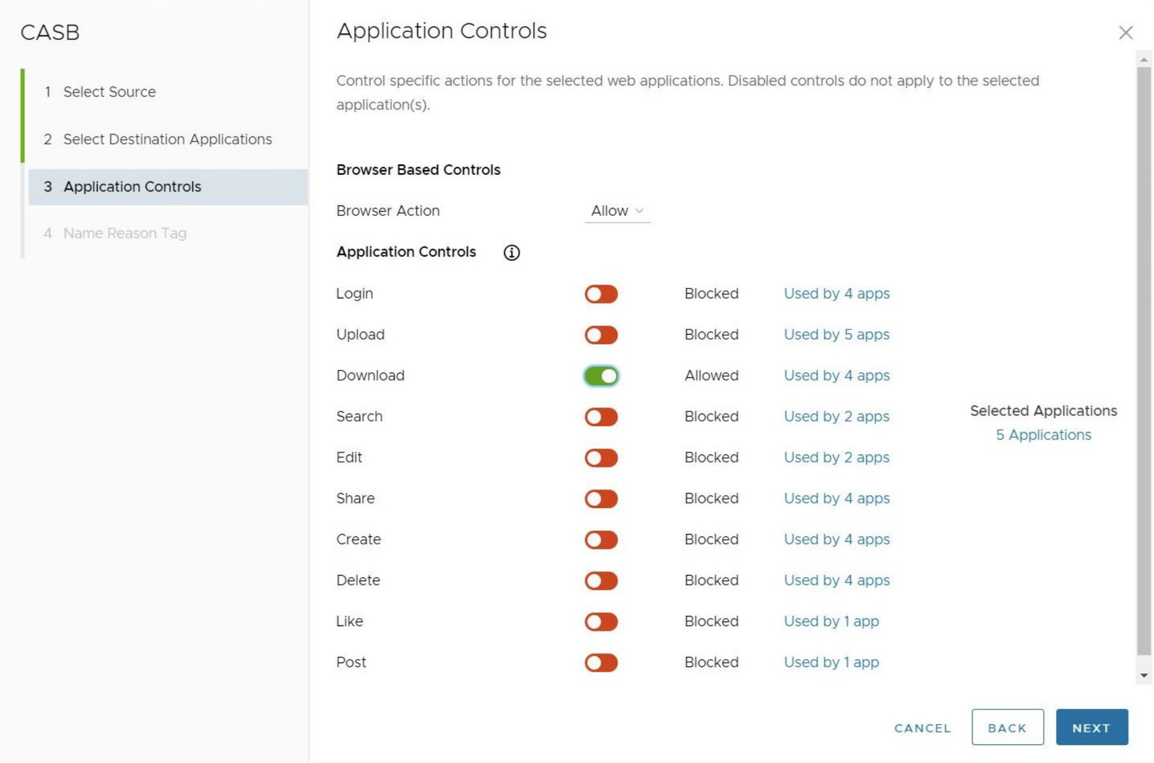
Browser Action: Block

Application Controls

Login	○	Blocked	Used by 4 apps
Upload	○	Blocked	Used by 5 apps
Download	○	Blocked	Used by 4 apps
Search	○	Blocked	Used by 2 apps
Edit	○	Blocked	Used by 2 apps
Share	○	Blocked	Used by 4 apps
Create	○	Blocked	Used by 4 apps
Delete	○	Blocked	Used by 4 apps
Like	○	Blocked	Used by 1 app
Post	○	Blocked	Used by 1 app

Selected Applications
5 Applications

b Or users can select which controls are blocked and which are allowed. In this instance blocking all application controls except the downloading files.



CASB

1 Select Source

2 Select Destination Applications

3 Application Controls

4 Name Reason Tag

Application Controls

Control specific actions for the selected web applications. Disabled controls do not apply to the selected application(s).

Browser Based Controls

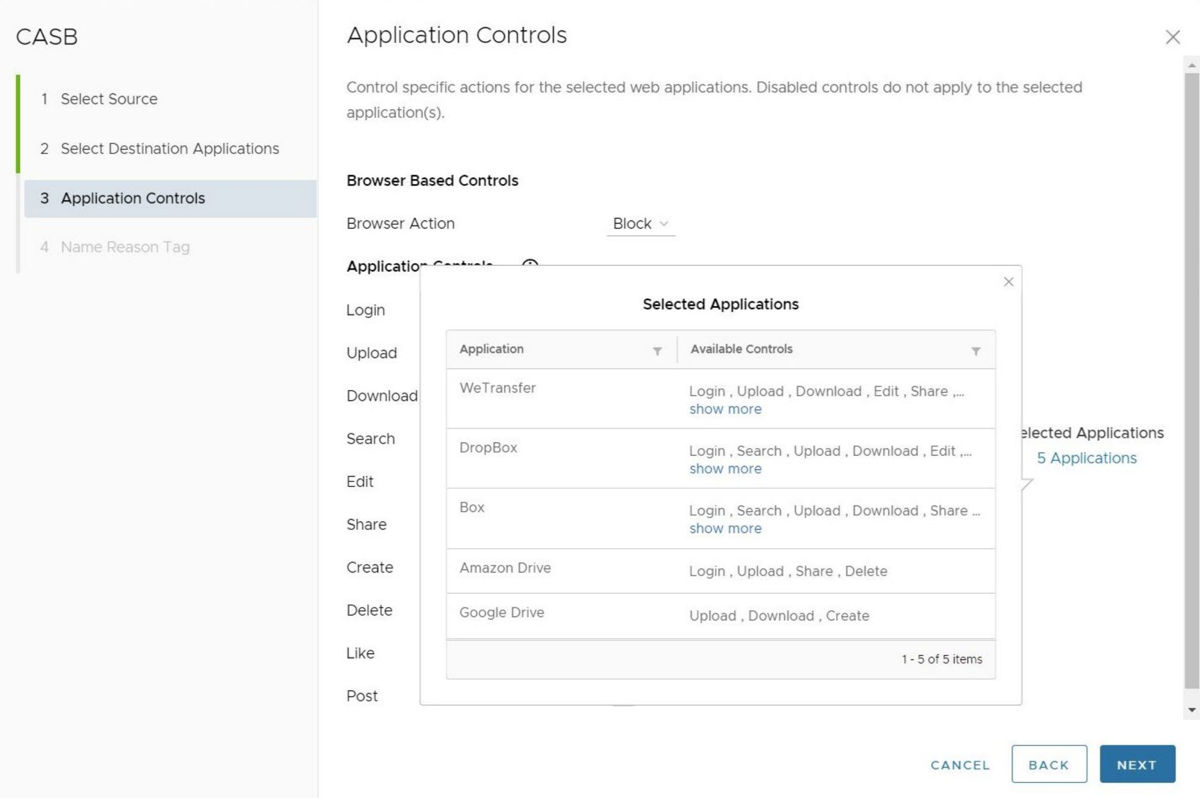
Browser Action: Allow

Application Controls

Login	●	Blocked	Used by 4 apps
Upload	●	Blocked	Used by 5 apps
Download	●	Allowed	Used by 4 apps
Search	●	Blocked	Used by 2 apps
Edit	●	Blocked	Used by 2 apps
Share	●	Blocked	Used by 4 apps
Create	●	Blocked	Used by 4 apps
Delete	●	Blocked	Used by 4 apps
Like	●	Blocked	Used by 1 app
Post	●	Blocked	Used by 1 app

Selected Applications
5 Applications

In the **Applications Controls** Screen, users can confirm which Applications are being used by this rule by clicking **# Applications** under the **Selected Applications** heading to the right of the screen.



CASB

1 Select Source

2 Select Destination Applications

3 Application Controls

4 Name Reason Tag

Application Controls

Control specific actions for the selected web applications. Disabled controls do not apply to the selected application(s).

Browser Based Controls

Browser Action: Block

Application Controls

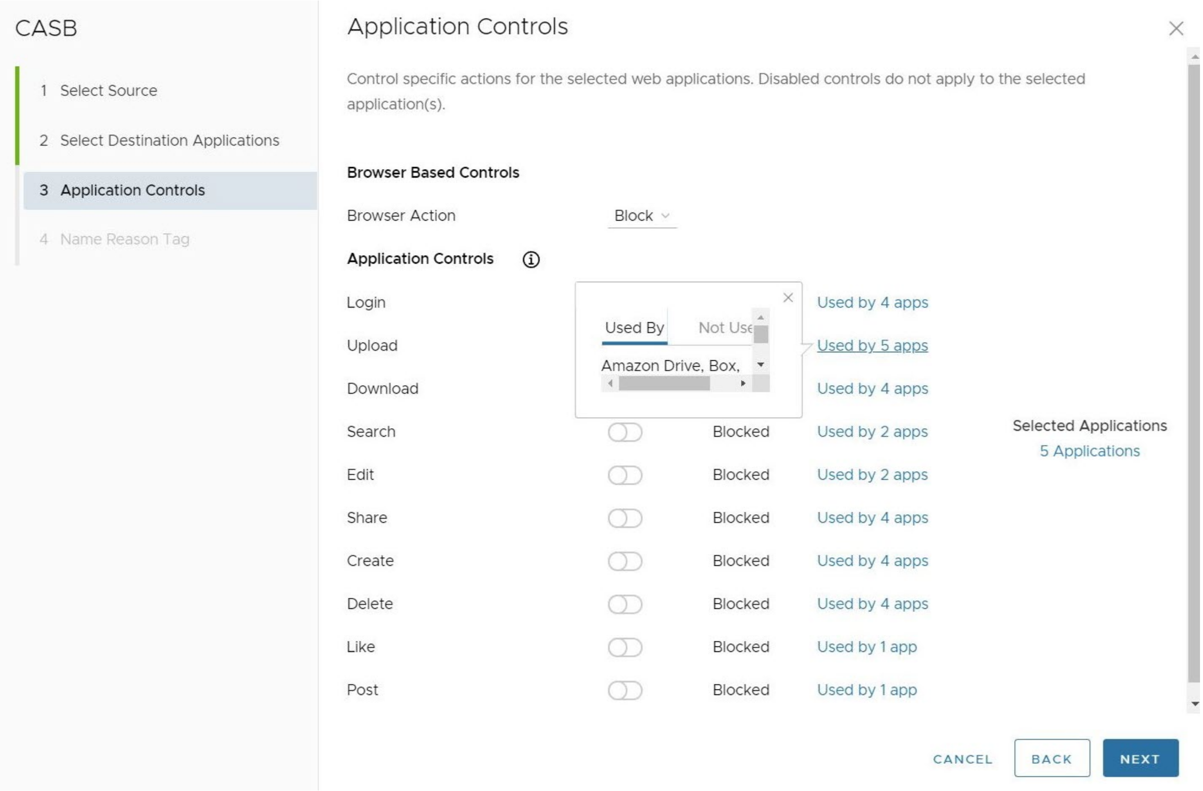
Selected Applications

Application	Available Controls
WeTransfer	Login , Upload , Download , Edit , Share ,... show more
DropBox	Login , Search , Upload , Download , Edit ,... show more
Box	Login , Search , Upload , Download , Share ... show more
Amazon Drive	Login , Upload , Share , Delete
Google Drive	Upload , Download , Create

1 - 5 of 5 items

elected Applications: 5 Applications

Users can also see which applications are used by a specific Application Control rule by clicking on the **Used by # apps** to the right of a particular Application Control.



CASB

1 Select Source
2 Select Destination Applications
3 Application Controls
4 Name Reason Tag

Application Controls

Control specific actions for the selected web applications. Disabled controls do not apply to the selected application(s).

Browser Based Controls

Browser Action: Block

Application Controls

Login			Used by 4 apps
Upload			Used by 5 apps
Download			Used by 4 apps
Search	○	Blocked	Used by 2 apps
Edit	○	Blocked	Used by 2 apps
Share	○	Blocked	Used by 4 apps
Create	○	Blocked	Used by 4 apps
Delete	○	Blocked	Used by 4 apps
Like	○	Blocked	Used by 1 app
Post	○	Blocked	Used by 1 app

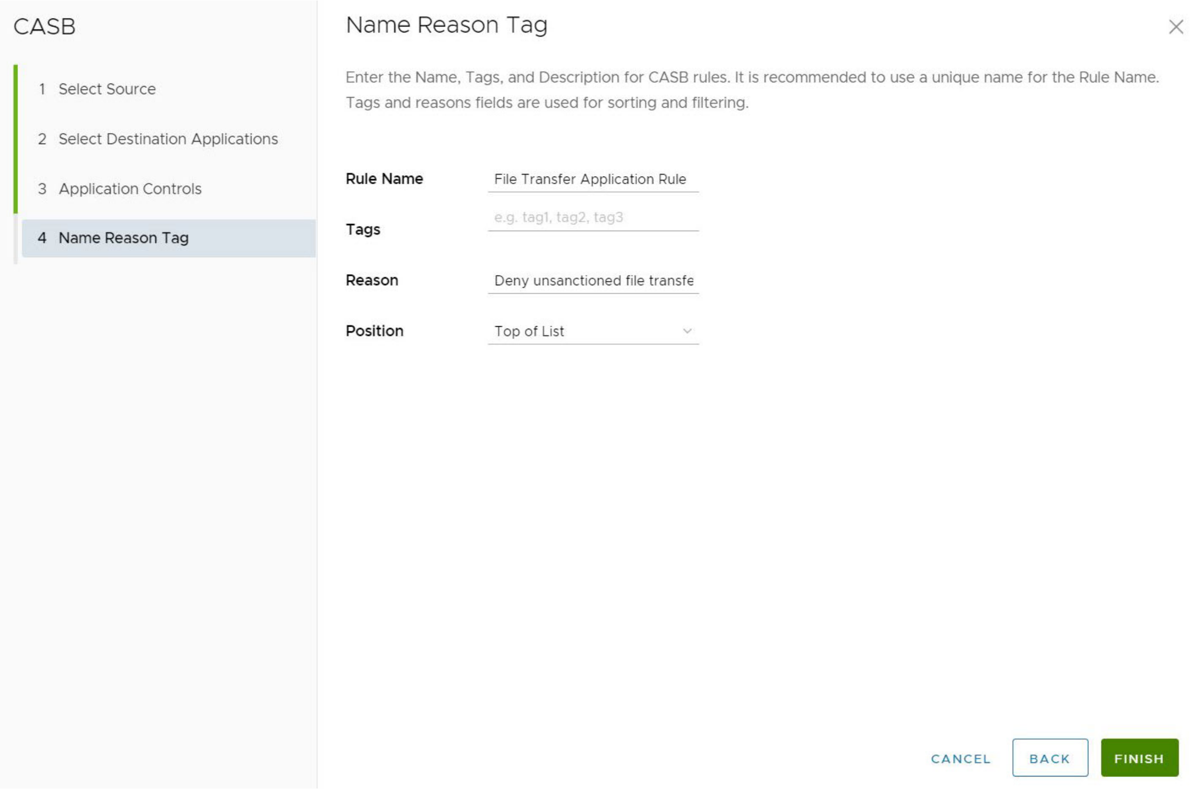
Used By | Not Use
Amazon Drive, Box,

Selected Applications
5 Applications

After configuring the set of Application Controls to be applied, click **Next**.

7 In the **Name Reason Tag** screen, configure a unique Rule Name (required), Tags (if used), Reason (if needed), and a Position for the rule on the list of CASB rules (the options are either 'Top of List' or 'Bottom of List').

Note The Position field designates the rule's position on the list of CASB rules.



Name Reason Tag

Enter the Name, Tags, and Description for CASB rules. It is recommended to use a unique name for the Rule Name. Tags and reasons fields are used for sorting and filtering.

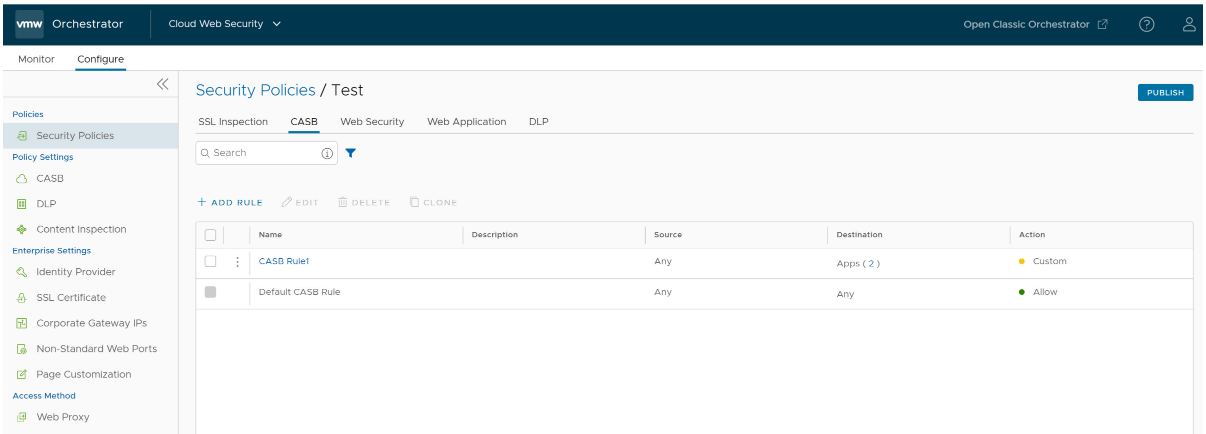
Rule Name: File Transfer Application Rule

Tags: e.g. tag1, tag2, tag3

Reason: Deny unsanctioned file transfe

Position: Top of List

8 Click **Finish**. A CASB rule is created for the selected applications. To apply the CASB Control Rule to traffic, click **Publish.**



Security Policies / Test

☐	Name	Description	Source	Destination	Action
☐	CASB Rule1		Any	Apps (2)	● Custom
☐	Default CASB Rule		Any	Any	● Allow

Note The Orchestrator requires up to five minutes to successfully publish the new rules.

After publishing, a rule can be edited and republished as needed in the same way that it was edited above.

Note The Default CASB Rule cannot be edited or changed in any way.

9 After publishing the Security Policy, users can Applying a Security Policy.

For more information about CASB Enterprise settings, see Chapter 2 Cloud Access Security Broker.

Configure Web Security Rules

Describes in detail how to configure a Web Security rule for a selected Security Policy.

Before you begin

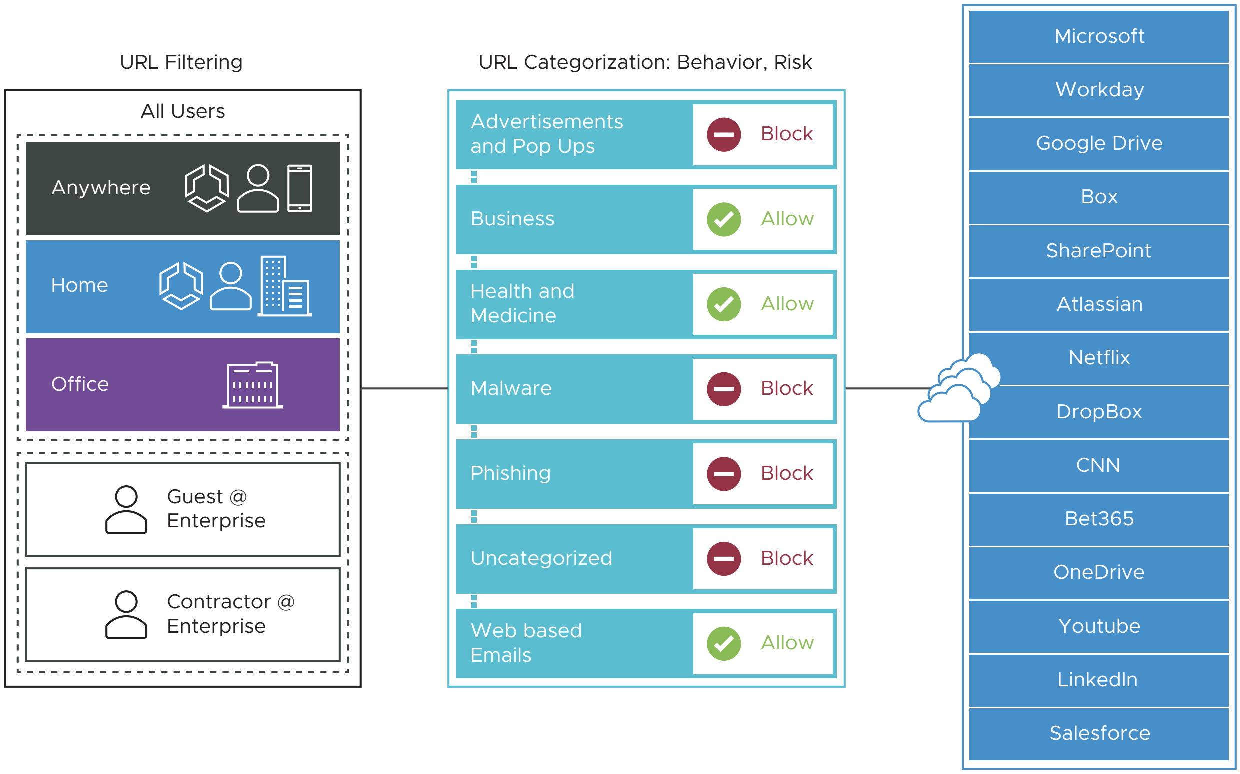
To configure a Security Policy, users must have first created a Security Policy. For specific instructions on how to create a Security Policy, see Create a Security Policy.

Web Security Categories

When creating a Web Security policy rule, users can configure the following categories:

- URL Filtering
- Geo-Based Filtering
- Content Filtering
- Content Inspection

URL Filtering



URL Filtering allows users to configure rules to limit user interaction to specific categories of web sites.

URL Filtering use cases include:

- Control employee web browsing with granular policies.
- Report high risk sites, useful with SaaS applications.
- Allow/Block based on pre-defined categories.
- Block URLs hosting objectionable content with an option to block custom domains.

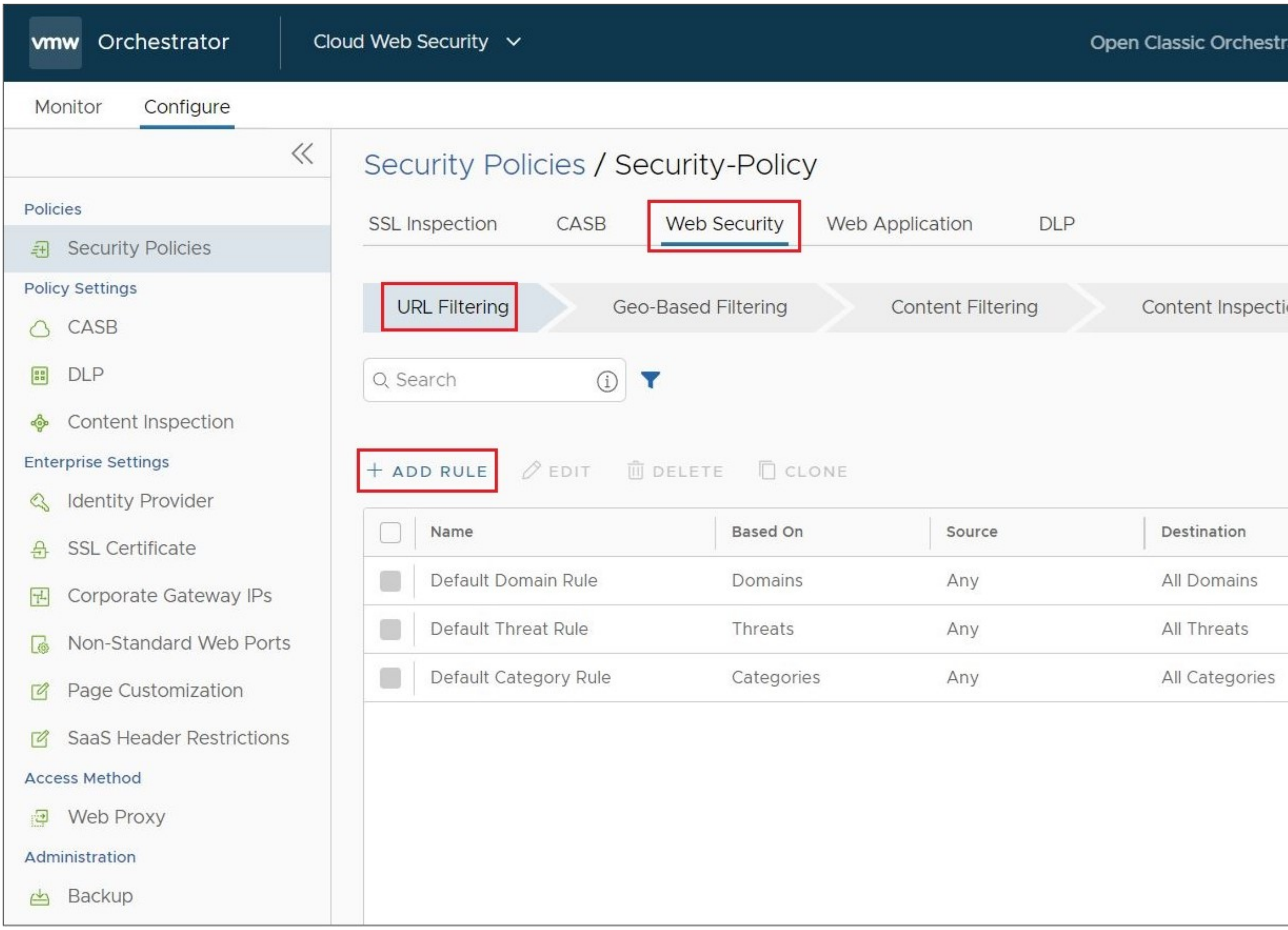
In contrast to SSL Inspection, where the default rule enforces stringent security by inspecting every SSL encrypted packet, the default rules for URL Filtering are permissive, allowing all traffic by default, regardless of potential danger. It is up to users to change the default behavior. In order to change the default behavior, users can choose from three kinds of rules URL Filtering enforces: Category, Threat, and Domain.

To configure a URL Filtering Rule, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

2 Select a security policy to configure a URL Filtering rule.

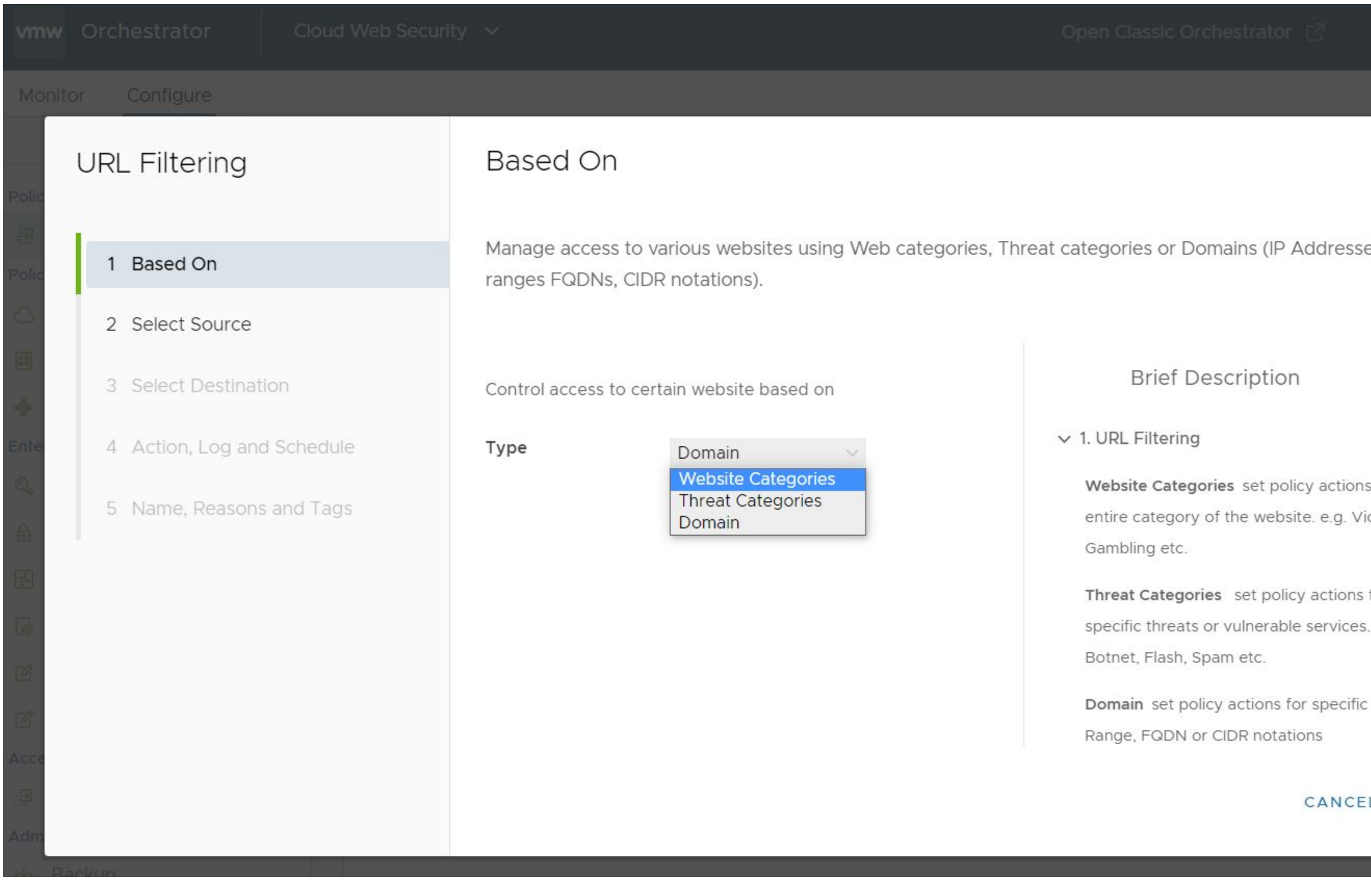
3 In the selected **Security Policies** screen, click the **Web Security** tab.



☐	Name	Based On	Source	Destination
☐	Default Domain Rule	Domains	Any	All Domains
☐	Default Threat Rule	Threats	Any	All Threats
☐	Default Category Rule	Categories	Any	All Categories

4 Under the **URL Filtering** tab, click **+ ADD RULE**.

The **Based On** screen appears.



Based On

Manage access to various websites using Web categories, Threat categories or Domains (IP Addresse
ranges FQDNs, CIDR notations).

Control access to certain website based on

Type Domain

Brief Description

1. URL Filtering

Website Categories set policy actions
entire category of the website. e.g. Vic
Gambling etc.

Threat Categories set policy actions f
specific threats or vulnerable services.
Botnet, Flash, Spam etc.

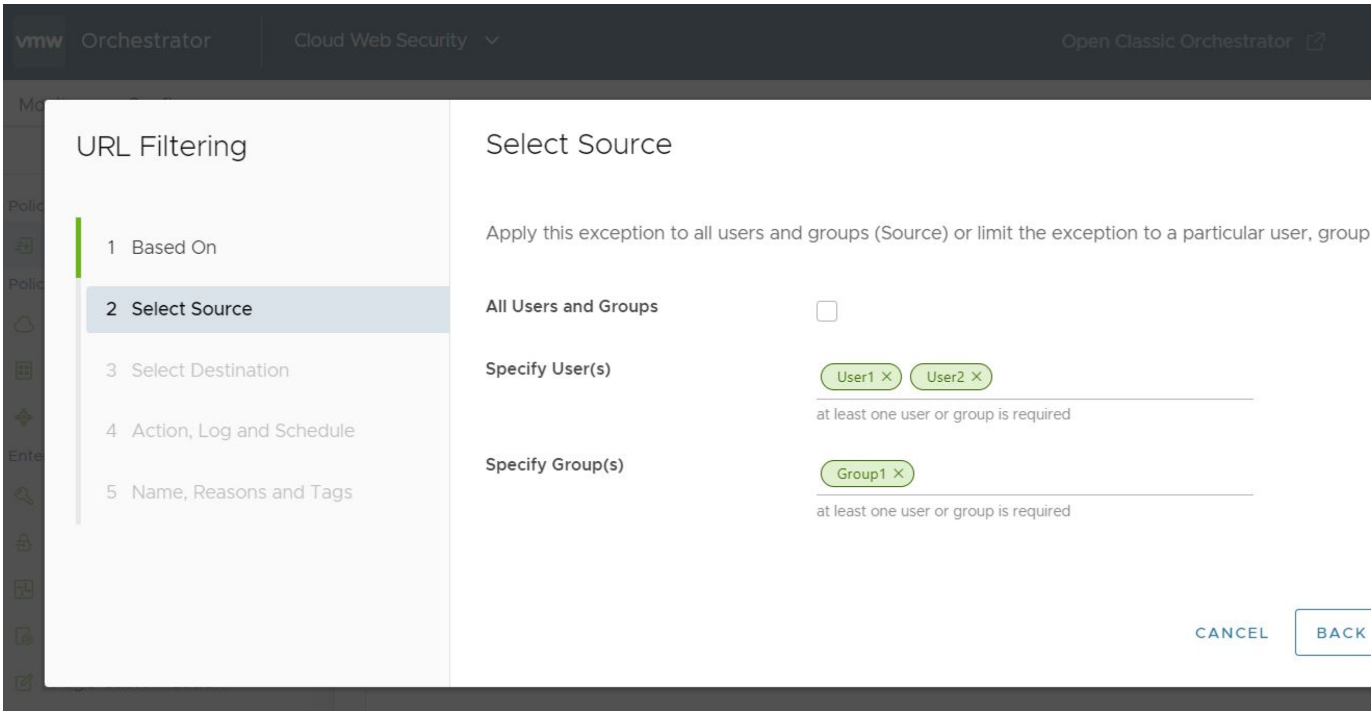
Domain set policy actions for specific
Range, FQDN or CIDR notations

5 In the **Based On** screen, from the **Type** drop-down menu, select one of the three options to control access to certain websites:

- **Website Categories** - Set policy actions for the entire category of the website. For example, Violence, Gambling, and others of the same kind.
- **Threat Categories** - Set policy actions for specific threats or vulnerable services. For example, Botnet, Flash, Spam, and others of the same kind.
- **Domain** - Set policy actions for specific IPs, IP Range, FQDN, or CIDR notations. This can be done manually with a static list configured in the rule or through the use of a domain list stored remotely that you can dynamically edit and update.

Click **Next**, the **Select Source** screen appears.

6 In the **Select Source** screen, select the source to apply the rule or exception.



Select Source

Apply this exception to all users and groups (Source) or limit the exception to a particular user, group

All Users and Groups ☐

Specify User(s): User1 ×, User2 ×

at least one user or group is required

Specify Group(s): Group1 ×

at least one user or group is required

Under **Source**, select the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.

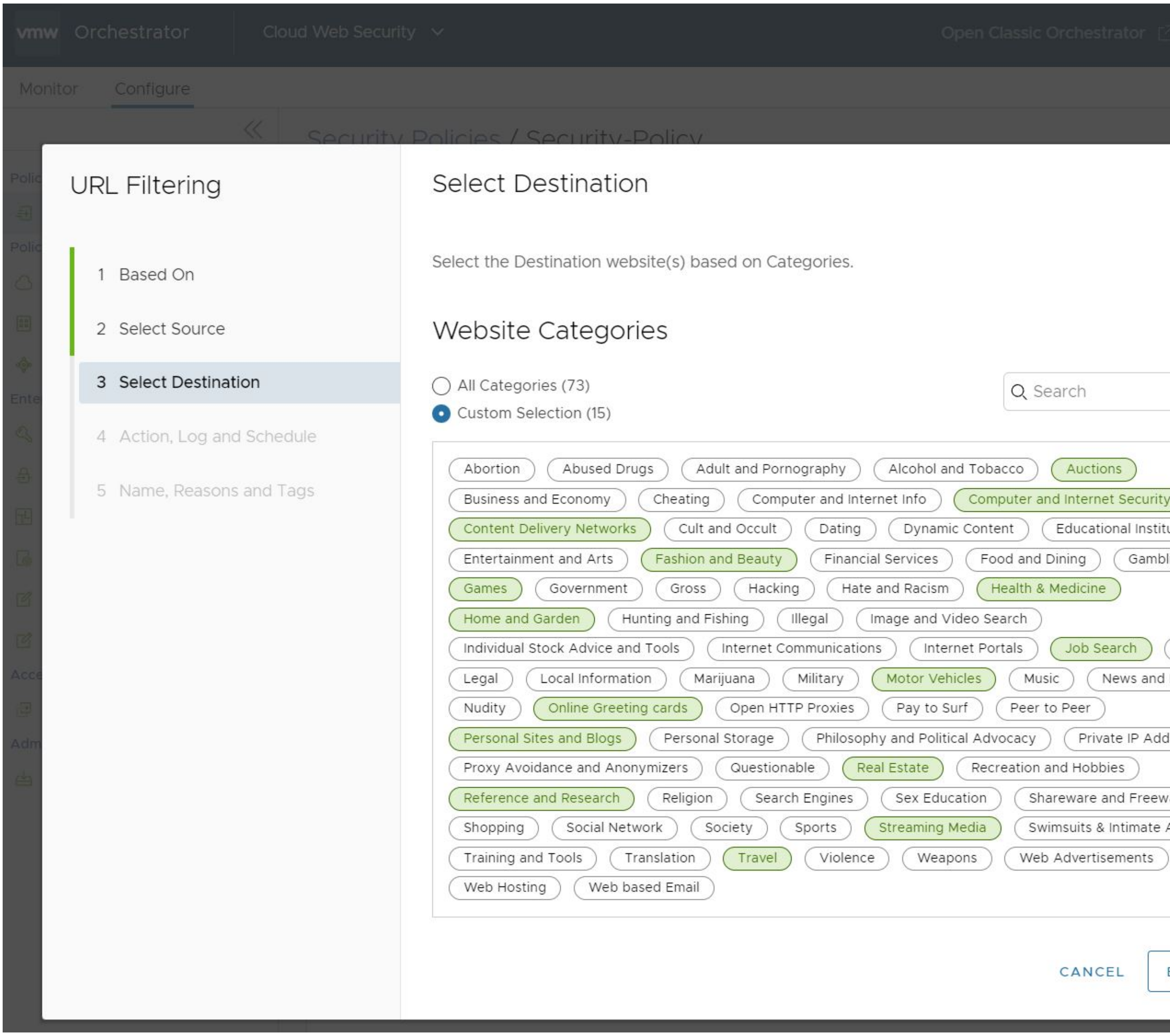
Click **Next**, the **Select Destination** screen appears.

Note A resource request may occasionally lack the authentication cookie necessary for user identification. Should this occur, a rule based on specific users or groups is not implemented for that resource request. Only rules matching **All Users and Groups** are applied in this scenario. For example, if you have a rule in place to block website 'A' for **All Users and Groups**, but a higher priority rule exists to allow website 'A' for certain users or groups, those specific users or groups may observe that while website 'A' loads, some resources or components, such as images or CSS, are missing.

---

7 Under **Select Destination**, you will see a screen based on the choice made in the **Based On** section: **Website Categories**, **Threat Categories**, or **Domains**.

   a **Website Categories**: Choose either **All Categories** or **Custom Selection**. The **All Categories** option highlights all available categories and applies them to the rule. The **Custom Selection** option allows users to specify which categories to apply to the rule by clicking on each category. You can also use the Search box to find a category.


vmw Orchestrator
Cloud Web Security
Open Classic Orchestrator
Monitor
Configure
Security Policies / Security-Policy
CANCEL

URL Filtering

1 Based On

2 Select Source

3 Select Destination

4 Action, Log and Schedule

5 Name, Reasons and Tags

Select Destination

Select the Destination website(s) based on Categories.

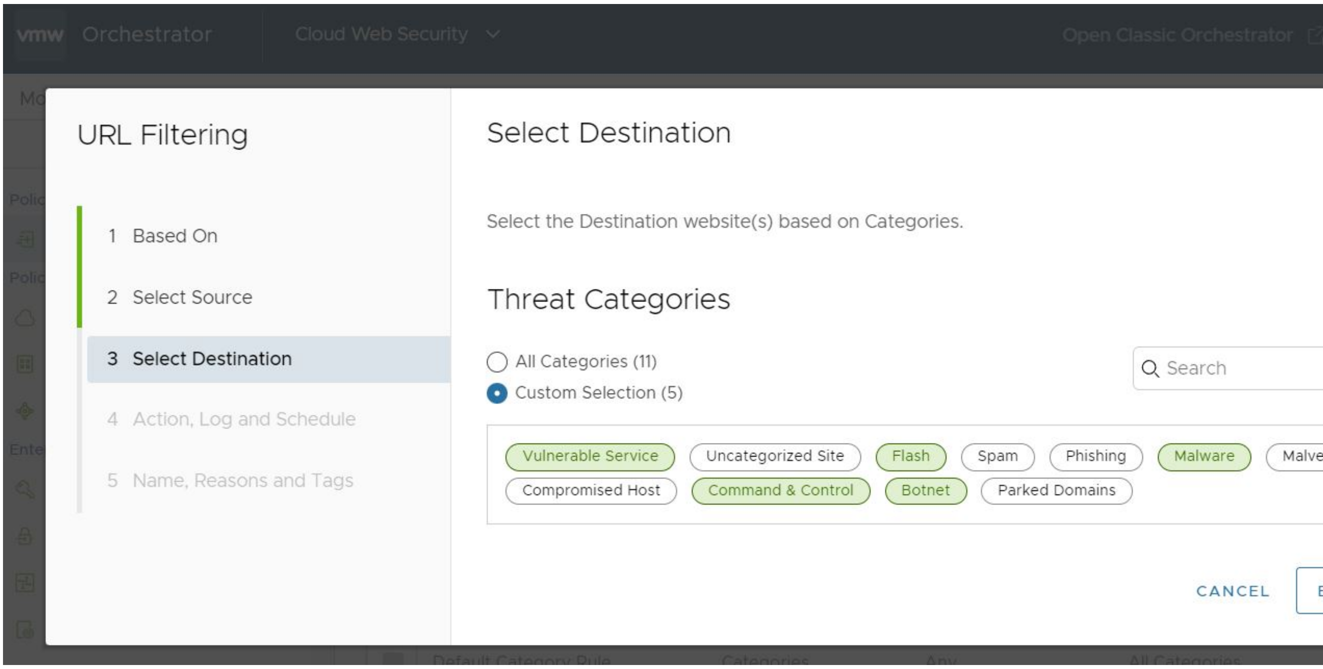
Website Categories

○ All Categories (73)
● Custom Selection (15)

Search

Abortion, Abused Drugs, Adult and Pornography, Alcohol and Tobacco, Auctions, Business and Economy, Cheating, Computer and Internet Info, Computer and Internet Security, Content Delivery Networks, Cult and Occult, Dating, Dynamic Content, Educational Institu, Entertainment and Arts, Fashion and Beauty, Financial Services, Food and Dining, Gambl, Games, Government, Gross, Hacking, Hate and Racism, Health & Medicine, Home and Garden, Hunting and Fishing, Illegal, Image and Video Search, Individual Stock Advice and Tools, Internet Communications, Internet Portals, Job Search, Legal, Local Information, Marijuana, Military, Motor Vehicles, Music, News and, Nudity, Online Greeting cards, Open HTTP Proxies, Pay to Surf, Peer to Peer, Personal Sites and Blogs, Personal Storage, Philosophy and Political Advocacy, Private IP Add, Proxy Avoidance and Anonymizers, Questionable, Real Estate, Recreation and Hobbies, Reference and Research, Religion, Search Engines, Sex Education, Shareware and Freew, Shopping, Social Network, Society, Sports, Streaming Media, Swimsuits & Intimate A, Training and Tools, Translation, Travel, Violence, Weapons, Web Advertisements, Web Hosting, Web based Email

b **Threat Categories**: Choose either **All Categories** or **Custom Selection**. The **All Categories** option highlights all available categories and applies them to the rule. The **Custom Selection** option allows users to specify which categories to apply to the rule by clicking on each category. You can also use the Search box to find a category.



Select Destination

Select the Destination website(s) based on Categories.

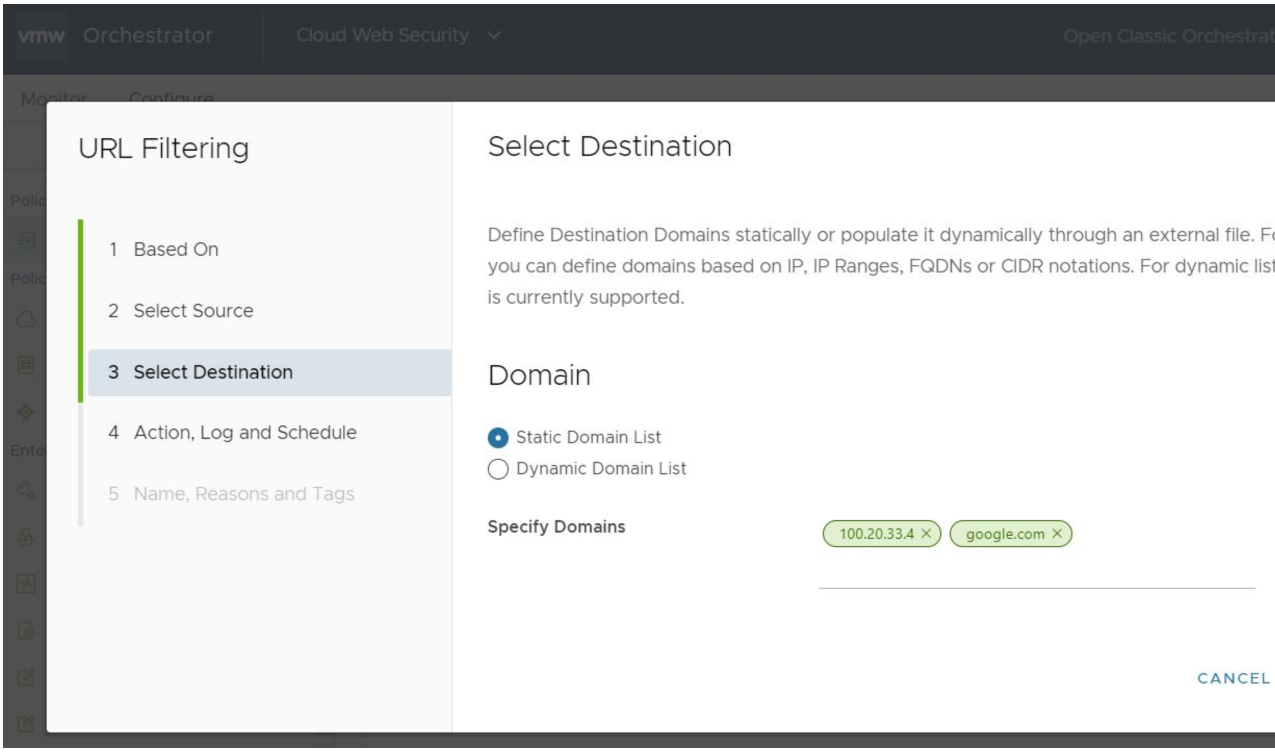
Threat Categories

○ All Categories (11)
● Custom Selection (5)

Vulnerable Service, Uncategorized Site, Flash, Spam, Phishing, Malware, Malve
Compromised Host, Command & Control, Botnet, Parked Domains

c **Domain**: The Domain Destination can be configured in one of two ways: **Static Domain List** or **Dynamic Domain List**.

1 **Static Domain List**: For the Static Domain List, enter domains formatted as either IP Address, IP Address Ranges, FQDNs, or CIDR notations. The domain formats can be mixed as needed. The list is static in the sense that you must update the rule manually each time you want to change the list.



Select Destination

Define Destination Domains statically or populate it dynamically through an external file. Fo
you can define domains based on IP, IP Ranges, FQDNs or CIDR notations. For dynamic list
is currently supported.

Domain

● Static Domain List
○ Dynamic Domain List

Specify Domains: 100.20.33.4 × google.com ×

2 **Dynamic Domain List**: For this option Cloud Web Security references a text list of FQDN formatted domains which is stored remotely at a location of your choosing. The location must be publicly accessible to the service. The advantage of this option is that you can make a domain list with a large number of domains and that can be edited and updated easily.

   Note While the Static Domain List allows domains in a variety formats (IP Address, IP Address Ranges, FQDNs, or CIDR notations), the Dynamic Domain List you create and maintain can only use FQDN formatted domains.

   The Dynamic Domain List screen has three configuration fields:

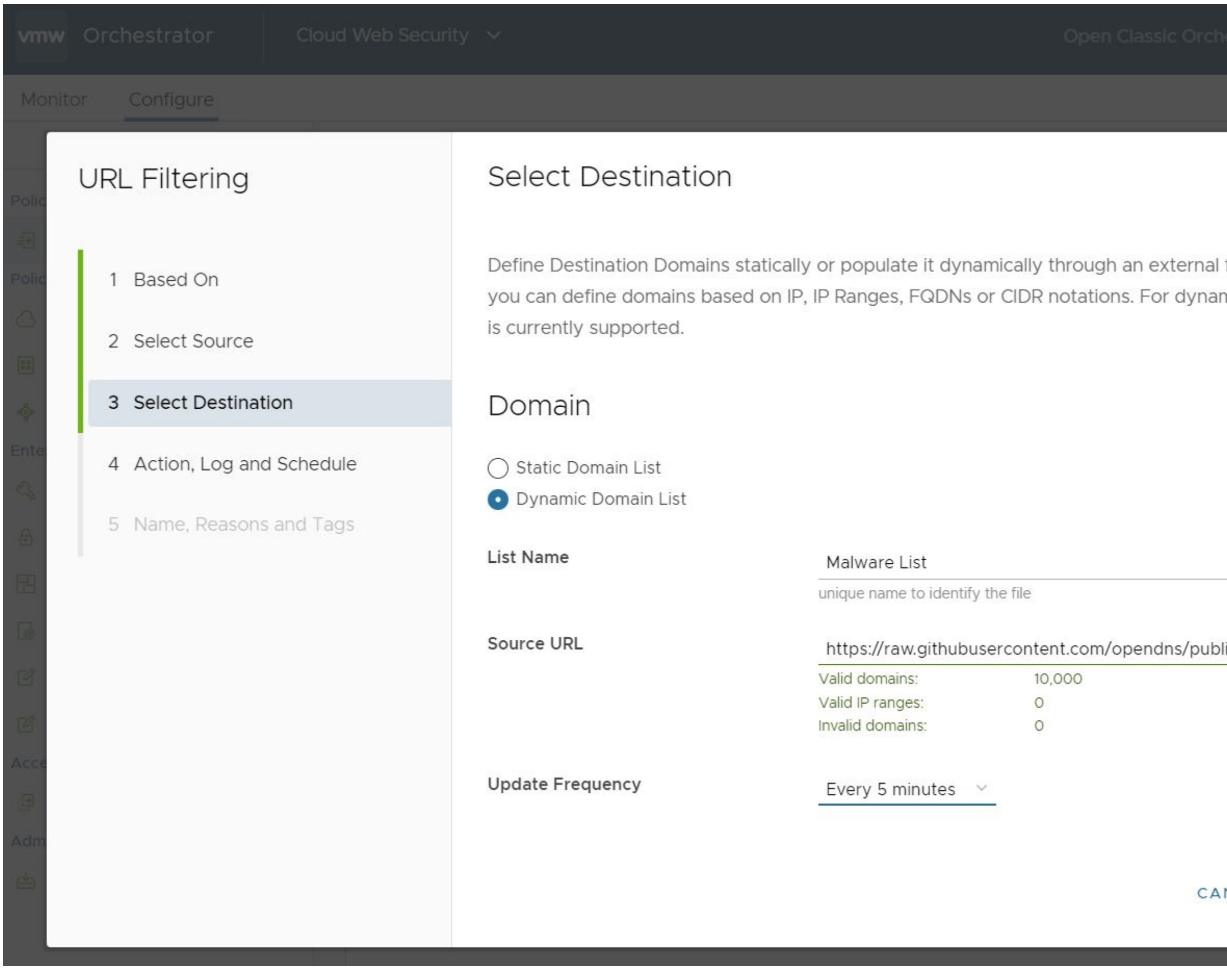
   a **List Name**: Specify a unique name for the domain list being referenced.

   b **Source URL**: The location of the text file list. This URL must be publicly available so that Cloud Web Security can access it. For example, a user could create a text file and store it on Dropbox where you configure the file so that it is available to anyone with the link.

      In the below example, we have used https://raw.githubusercontent.com/opendns/public-domain-lists/master/opendns-top-domains.txt as our remote URL. This is a simple list of the top public domains per OpenDNS.

      Once the **Source URL** is entered, click on **Validate URL**. Cloud Web Security will then check the URL to confirm that URL reachable and then check the text file and determine the validity of the domains on the list. If all the domains are valid you will see all green text and can then configure the Update Frequency as seen in the below image.

Figure 1-1. Dynamic Domain List With All Valid Domains



Select Destination

Define Destination Domains statically or populate it dynamically through an external f
you can define domains based on IP, IP Ranges, FQDNs or CIDR notations. For dynan
is currently supported.

Domain

○ Static Domain List
● Dynamic Domain List

List Name: Malware List
unique name to identify the file

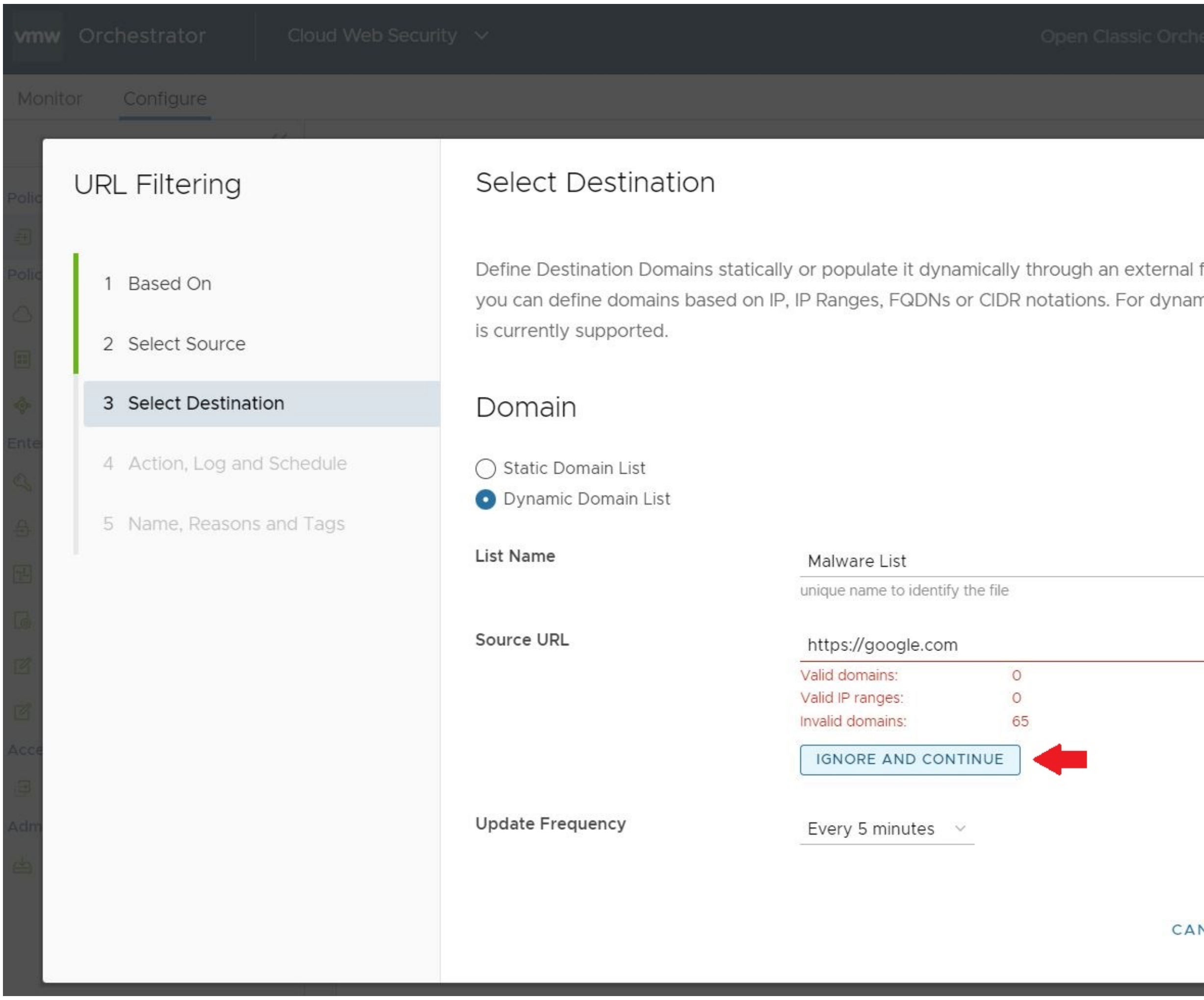
Source URL: https://raw.githubusercontent.com/opendns/publi
Valid domains: 10,000
Valid IP ranges: 0
Invalid domains: 0

Update Frequency: Every 5 minutes

If there are invalid domains in the **Dynamic Domain List**, the test output appears as red text and lists both the number of valid domains and the number of invalid domains as seen in the image below. You can either troubleshoot your domain list and retest it, or can optionally continue with the domain list as is by clicking on **Ignore and Continue**. The invalid domains on the list will be ignored by Cloud Web Security when applying the **URL Filtering Rule**.

Note While the Validate URL test outputs the number the invalid domains, it does not specify which domains on your list are invalid. You will need to troubleshoot your domain list separately to ensure all listed domains are valid.

Figure 1-2. Dynamic Domain List With Invalid Domains



URL Filtering

1 Based On
2 Select Source
3 Select Destination
4 Action, Log and Schedule
5 Name, Reasons and Tags

Select Destination

Define Destination Domains statically or populate it dynamically through an external f
you can define domains based on IP, IP Ranges, FQDNs or CIDR notations. For dynam
is currently supported.

Domain

○ Static Domain List
● Dynamic Domain List

List Name: Malware List
unique name to identify the file

Source URL: https://google.com
Valid domains: 0
Valid IP ranges: 0
Invalid domains: 65

Update Frequency: Every 5 minutes

c **Update Frequency**: Configure how often you want Cloud Web Security to check your Dynamic Domain List to update this **URL Filtering** rule. The options are every: 5 minutes, 30 minutes, Hourly (60 minutes), Daily (24 hours).

Click **Next**, the **Action, Log and Schedule** screen appears.

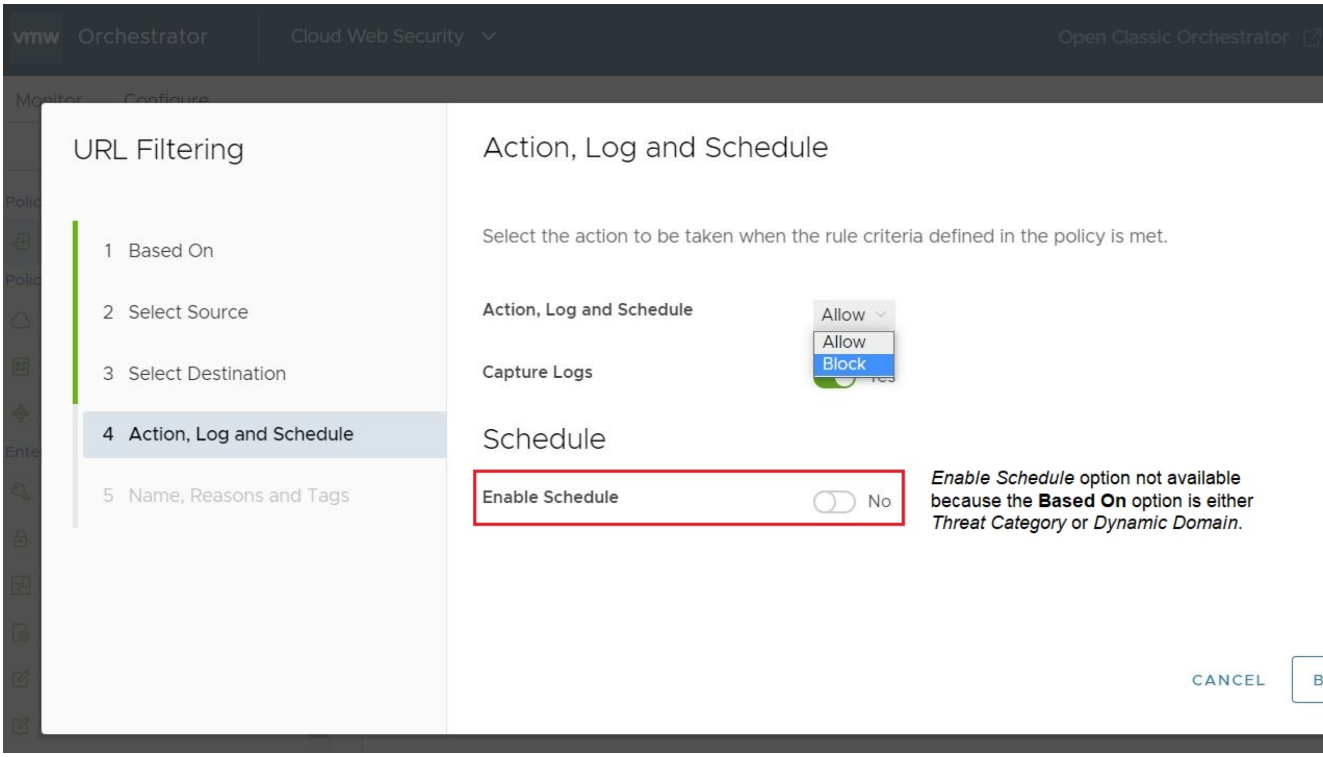
8 In the **Action, Log and Schedule** screen, you have the option of deciding what action should be taken when a **URL Filtering Rule** is matched, whether those incidents should be logged, and whether this rule applies at all times or during specified time periods.

   a The **Action** option determines whether traffic matching the rule criteria defined in the policy is allowed or blocked. Select the action **Block** or **Allow** from the **Action** drop-down menu.

   b When the **Capture Logs** option is configured as **Yes**, Cloud Web Security logs every instance that the **URL Filtering** rule is applied and these logged events can be observed in the **Monitor > Events** or compiled and downloaded as a report under **Monitor > Reports**.

c Finally, toggle **Enable Schedule** to optionally configure the days and time periods the rule is applied.

Note The **Schedule** feature is available for rules where the **Based On** type is either **Website Categories** or **Domain > Static Domain List**. **Schedule** is not available for **Based On** type **Threat Categories** or **Domain > Dynamic Domain List**, and in those instances the toggle button will be inaccessible.



URL Filtering

1 Based On
2 Select Source
3 Select Destination
4 Action, Log and Schedule
5 Name, Reasons and Tags

Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Allow (Allow / Block)

Capture Logs: Yes

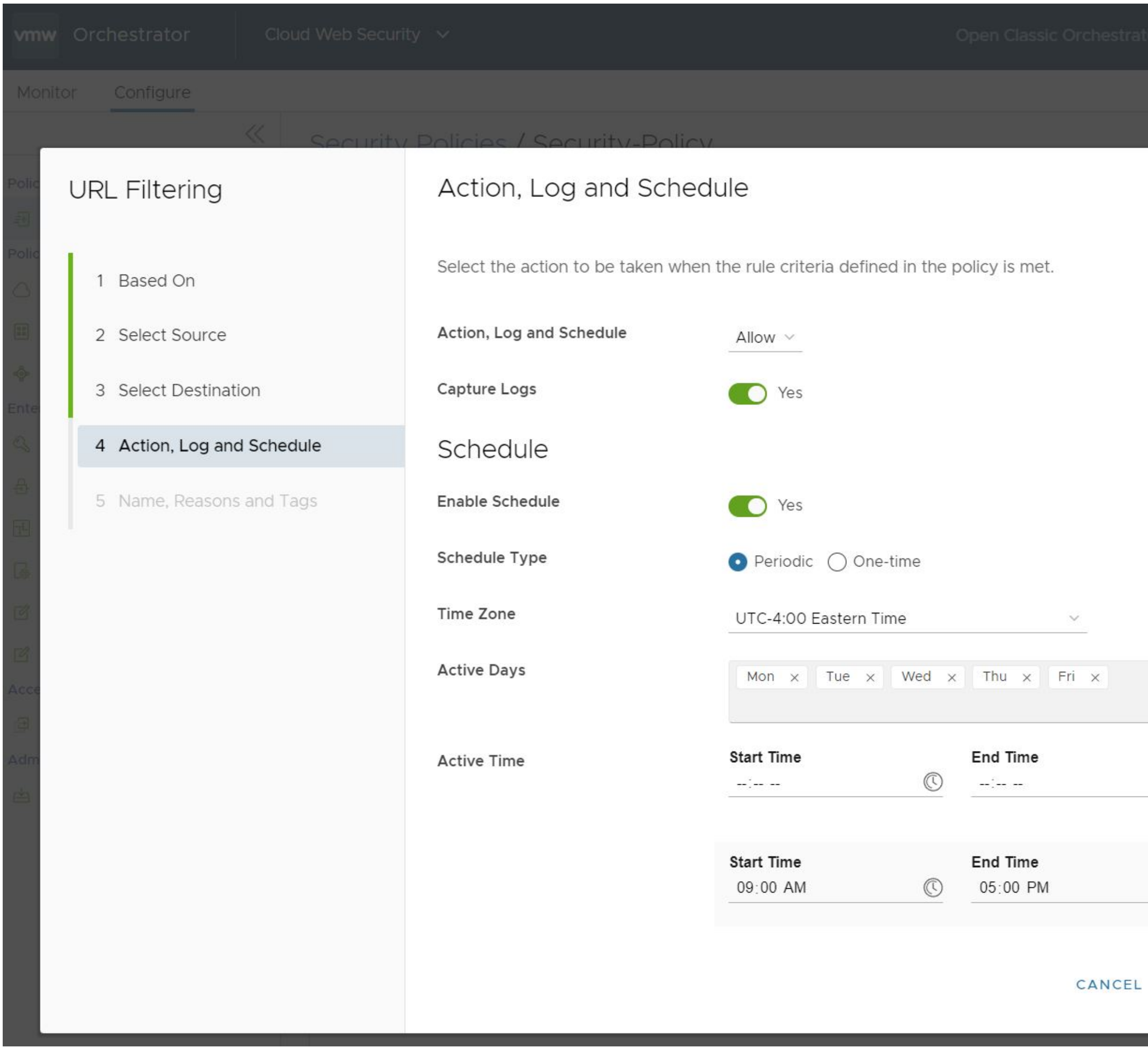
Schedule

Enable Schedule: No

Enable Schedule option not available because the **Based On** option is either *Threat Category* or *Dynamic Domain*.

Schedule offers two **Schedule Type** options for a URL Filtering Rule: **Periodic** and **One Time**.

1 The **Periodic** option allows you to configure a weekly, rotating schedule for when your URL Filtering Rule is applied. Selecting Periodic opens up three configurable options: **Time Zone**, **Active Days**, and **Active Time**. When initially selecting this option, the screen would include a default time period with preselected **Active Days** and **Active Time**. Your **Time Zone** is auto-detected and populated in the **Time Zone** parameter. You can edit each of these values and the initial values are provided as a useful starting point.



Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Allow

Capture Logs: Yes

Schedule

Enable Schedule: Yes

Schedule Type: ● Periodic ○ One-time

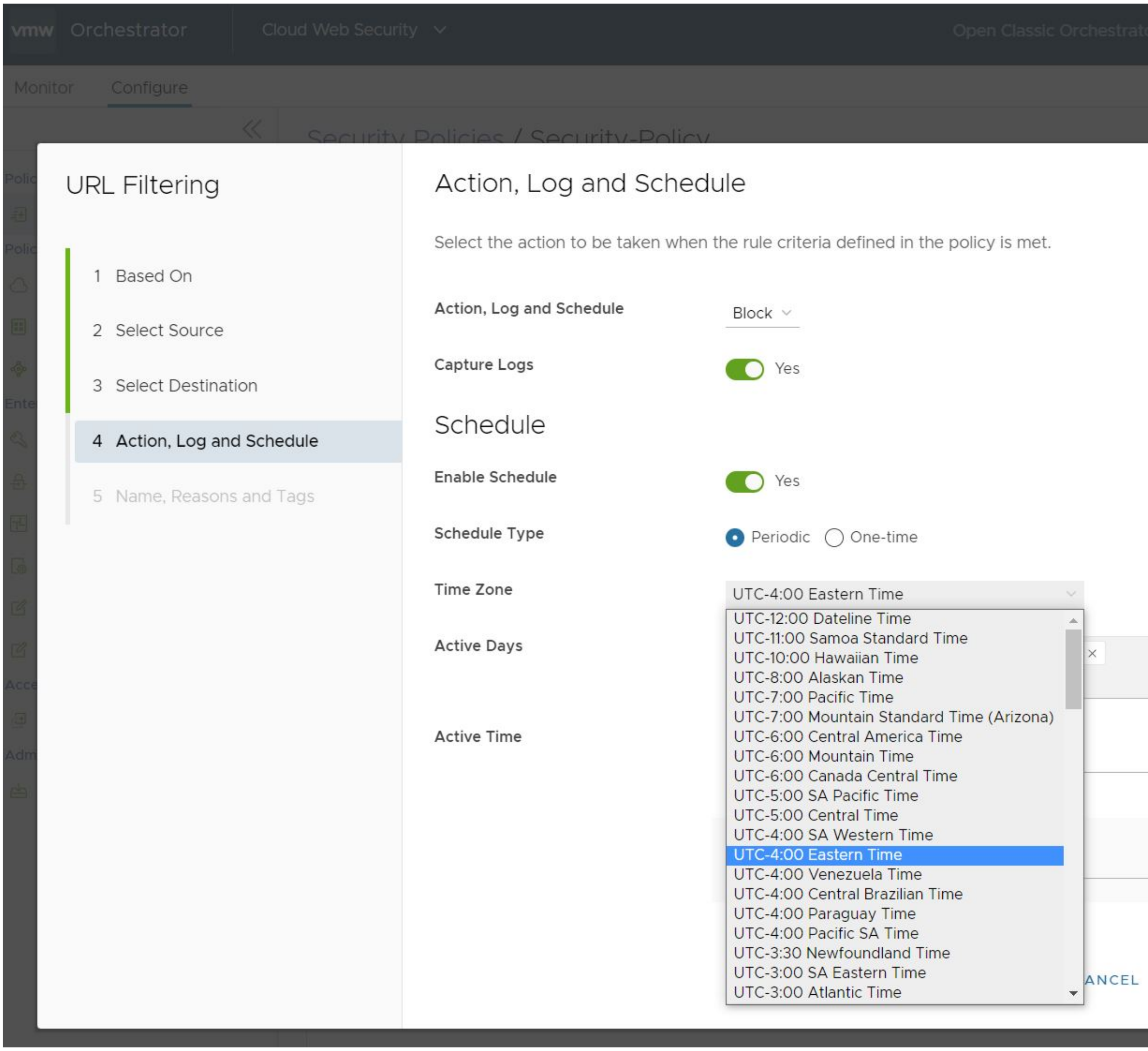
Time Zone: UTC-4:00 Eastern Time

Active Days: Mon × Tue × Wed × Thu × Fri ×

Active Time: Start Time --:-- -- End Time --:-- --

Start Time 09:00 AM End Time 05:00 PM

Time Zone specifies the time zone the rule will refer to when implementing the **Active Time** and is expressed in the UTC offset that reflects that time zone's current status relative to Daylight Savings/Summer Time versus Standard Time. For example, in the below screenshot the United States time zones are all expressed in the Daylight Savings UTC offset value and would adjust to the Standard Time offsets when applicable.



URL Filtering

1 Based On
2 Select Source
3 Select Destination
4 Action, Log and Schedule
5 Name, Reasons and Tags

Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Block
Capture Logs: Yes

Schedule

Enable Schedule: Yes
Schedule Type: ● Periodic ○ One-time
Time Zone: UTC-4:00 Eastern Time
Active Days
Active Time

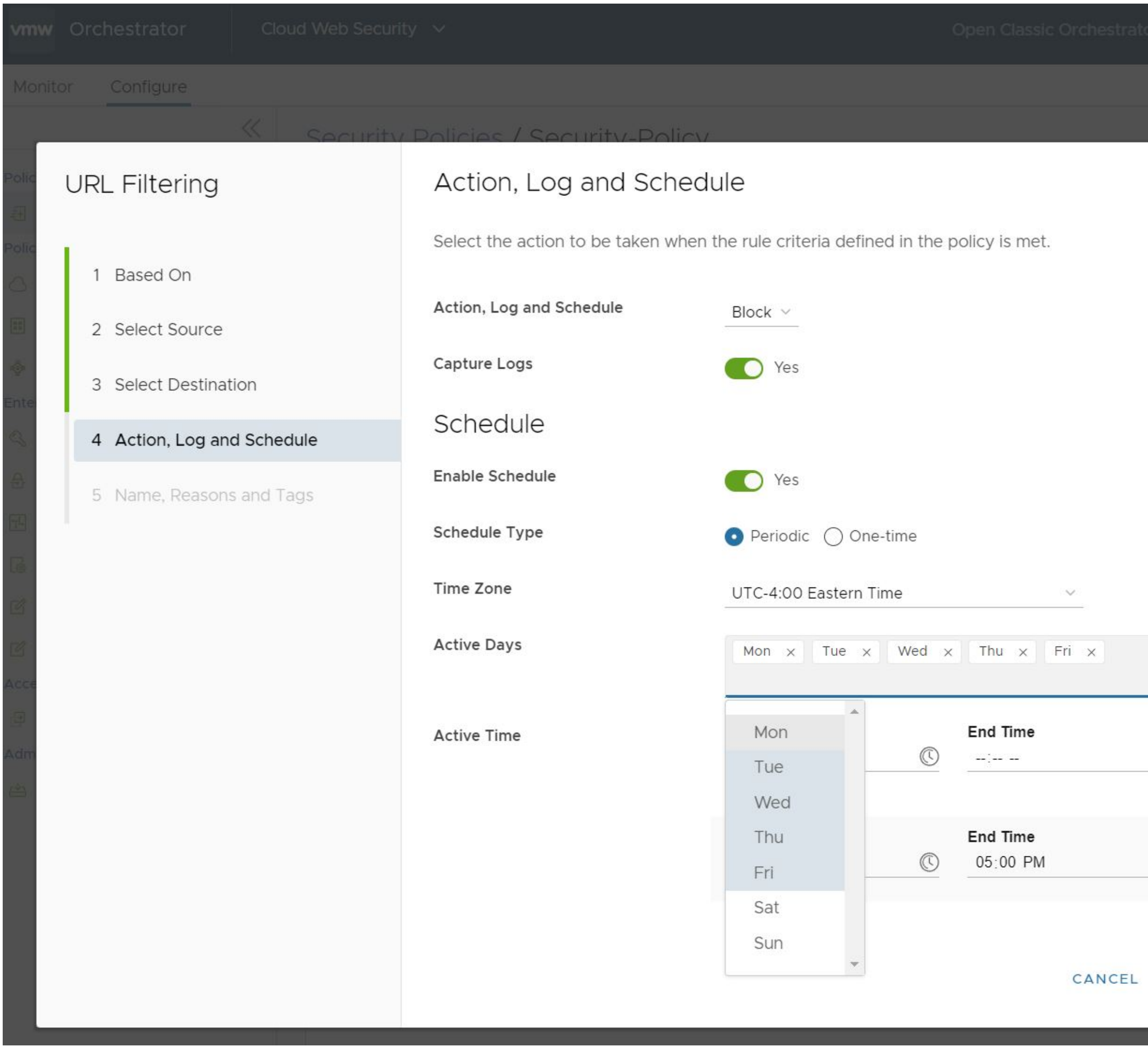
UTC-12:00 Dateline Time
UTC-11:00 Samoa Standard Time
UTC-10:00 Hawaiian Time
UTC-8:00 Alaskan Time
UTC-7:00 Pacific Time
UTC-7:00 Mountain Standard Time (Arizona)
UTC-6:00 Central America Time
UTC-6:00 Mountain Time
UTC-6:00 Canada Central Time
UTC-5:00 SA Pacific Time
UTC-5:00 Central Time
UTC-4:00 SA Western Time
UTC-4:00 Eastern Time
UTC-4:00 Venezuela Time
UTC-4:00 Central Brazilian Time
UTC-4:00 Paraguay Time
UTC-4:00 Pacific SA Time
UTC-3:30 Newfoundland Time
UTC-3:00 SA Eastern Time
UTC-3:00 Atlantic Time

Attention The **Time Zone** parameter is static and implements the **Active Time** only with reference to the configured **Time Zone**. The Scheduling feature does not auto-detect a user's time zone and dynamically adjust so that the rule applies the same **Active Time** for each user based on their location.

For example, if a user sets the **Time Zone** as UTC-4:00 Eastern Time with a **Start Time** of 09:00 AM and an **End Time** of 05:00 PM, for a user in the Eastern Time, this is when the rule would be implemented. However, if a user is in the UTC-7:00 Pacific Time Zone, the rules are implemented 3 hours earlier, from 6:00 AM to 2:00 PM. For a user in UTC +1:00 UK and Ireland, the rules are implemented 5 hours later.

Active Times are automatically adjusted for Daylights Savings/Summer Time as applicable for the selected time zone and this is reflected in the UTC offset value.

The **Active Days Schedule Type** specifies the days of the week the rule is applied. You can add and remove days by clicking the arrow to open the drop down menu.



Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Block

Capture Logs: Yes

Schedule

Enable Schedule: Yes

Schedule Type: ● Periodic ○ One-time

Time Zone: UTC-4:00 Eastern Time

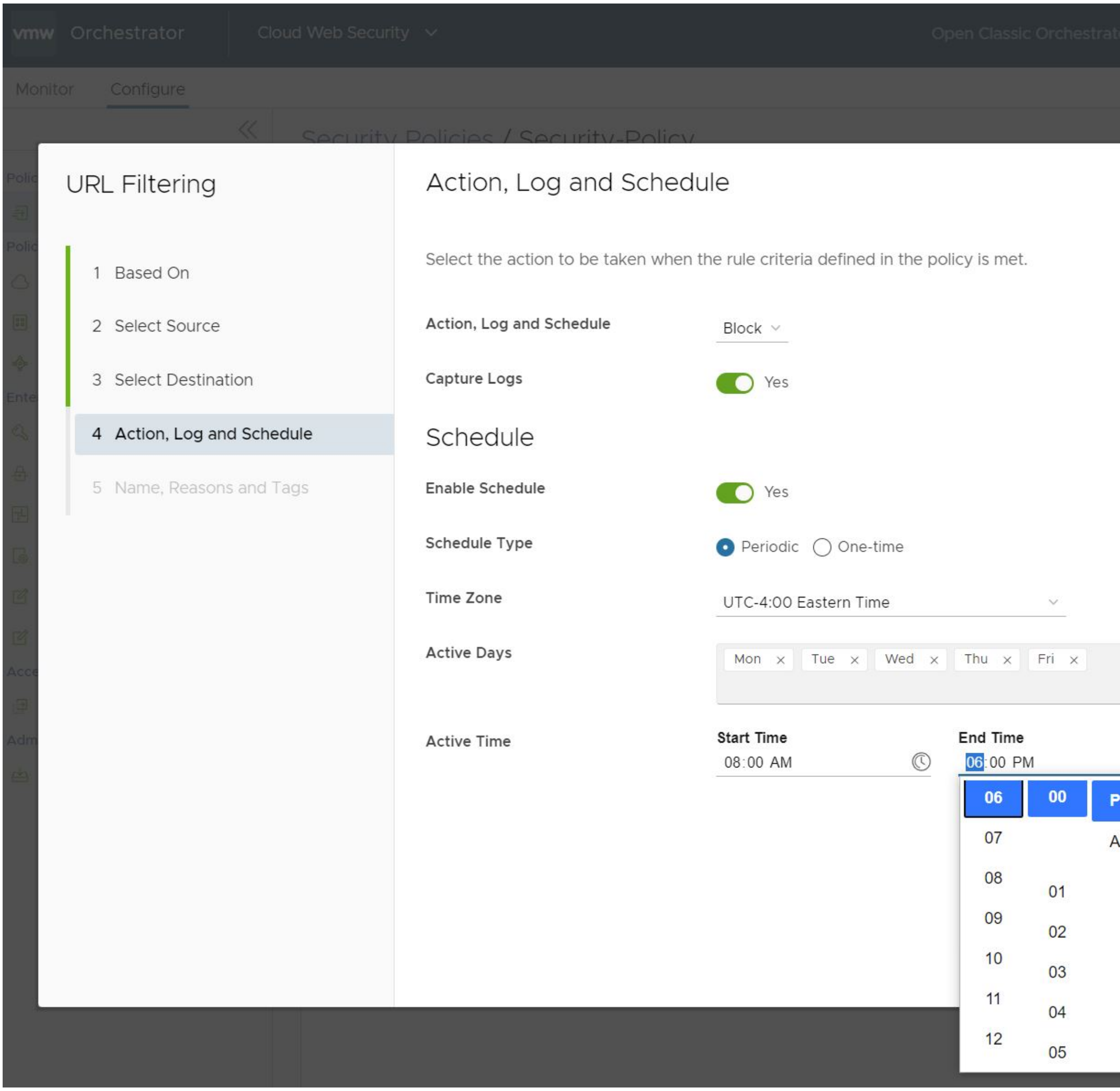
Active Days: Mon × Tue × Wed × Thu × Fri ×

Active Time

End Time: --:-- --

End Time: 05:00 PM

Active Time specifies the time period or periods when the rule is applied relative to the configured **Time Zone**. You can specify multiple **Active Time** periods by clicking **ADD**, and remove a time period by clicking the trash can icon.



URL Filtering

1 Based On
2 Select Source
3 Select Destination
4 Action, Log and Schedule
5 Name, Reasons and Tags

Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Block

Capture Logs: Yes

Schedule

Enable Schedule: Yes

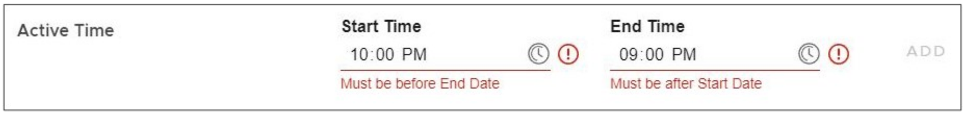
Schedule Type: ● Periodic ○ One-time

Time Zone: UTC-4:00 Eastern Time

Active Days: Mon × Tue × Wed × Thu × Fri ×

Active Time: Start Time 08:00 AM; End Time 06:00 PM

Note Make certain that your Start Time is a value prior to your End Time or you will observe an error.



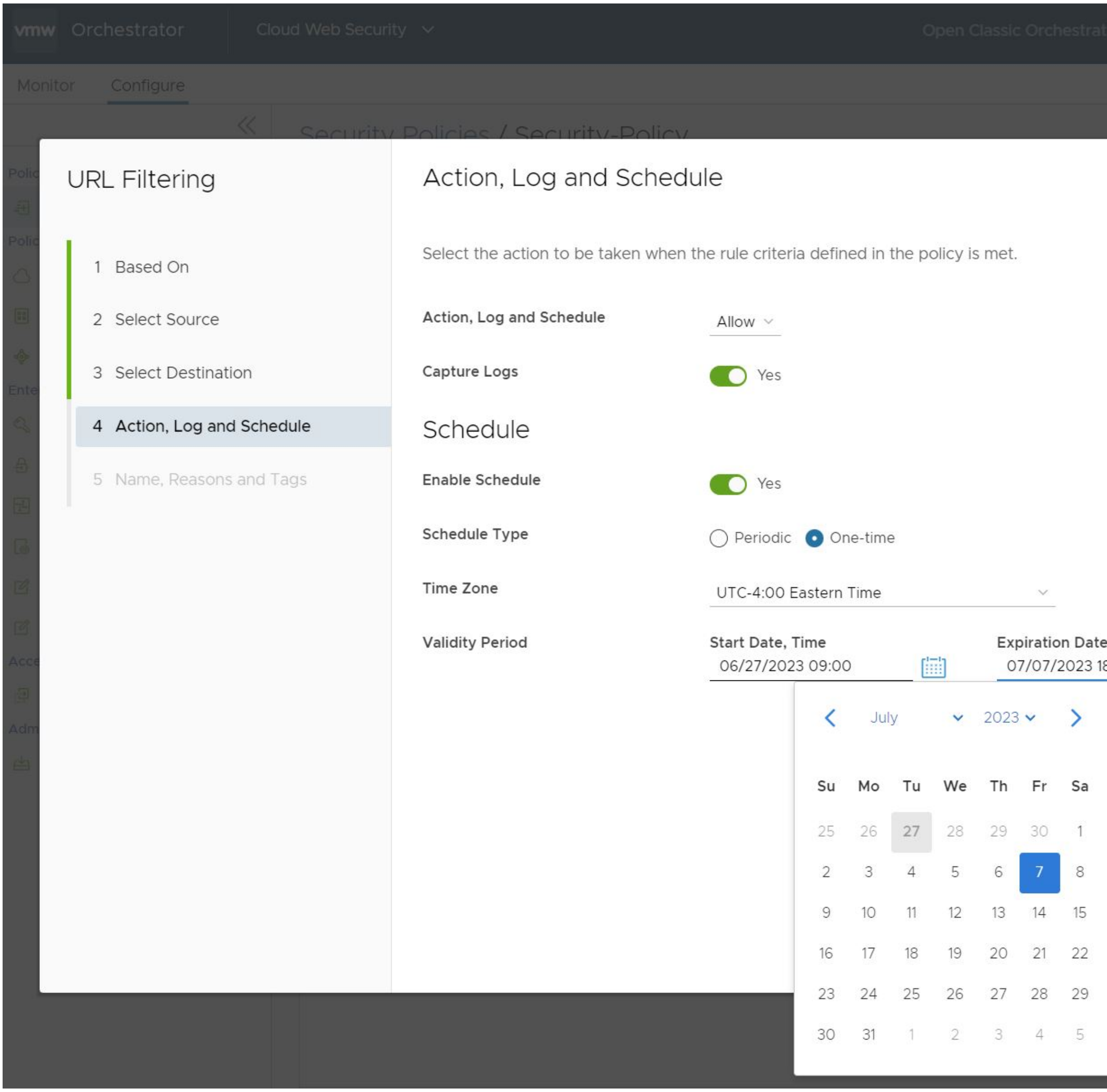
Active Time

Start Time: 10:00 PM — Must be before End Date

End Time: 09:00 PM — Must be after Start Date

Also, the Start Time and End Time must exist within the same calendar day. For example, you cannot configure a Start Time of 11:00 PM and an End Time of 01:00 AM because while you may understand that 01:00 AM as two hours after 11 PM, Cloud Web Security understands that 01:00 AM as that particular calendar day's time and 22 hours earlier, and thus invalid.

2 The **One-time Schedule Type** option specifies either one single block of time with a start and expiration date and time when the rule is applied, or a starting date and time from which the rule is indefinitely applied.



Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Allow

Capture Logs: Yes

Schedule

Enable Schedule: Yes

Schedule Type: ○ Periodic ● One-time

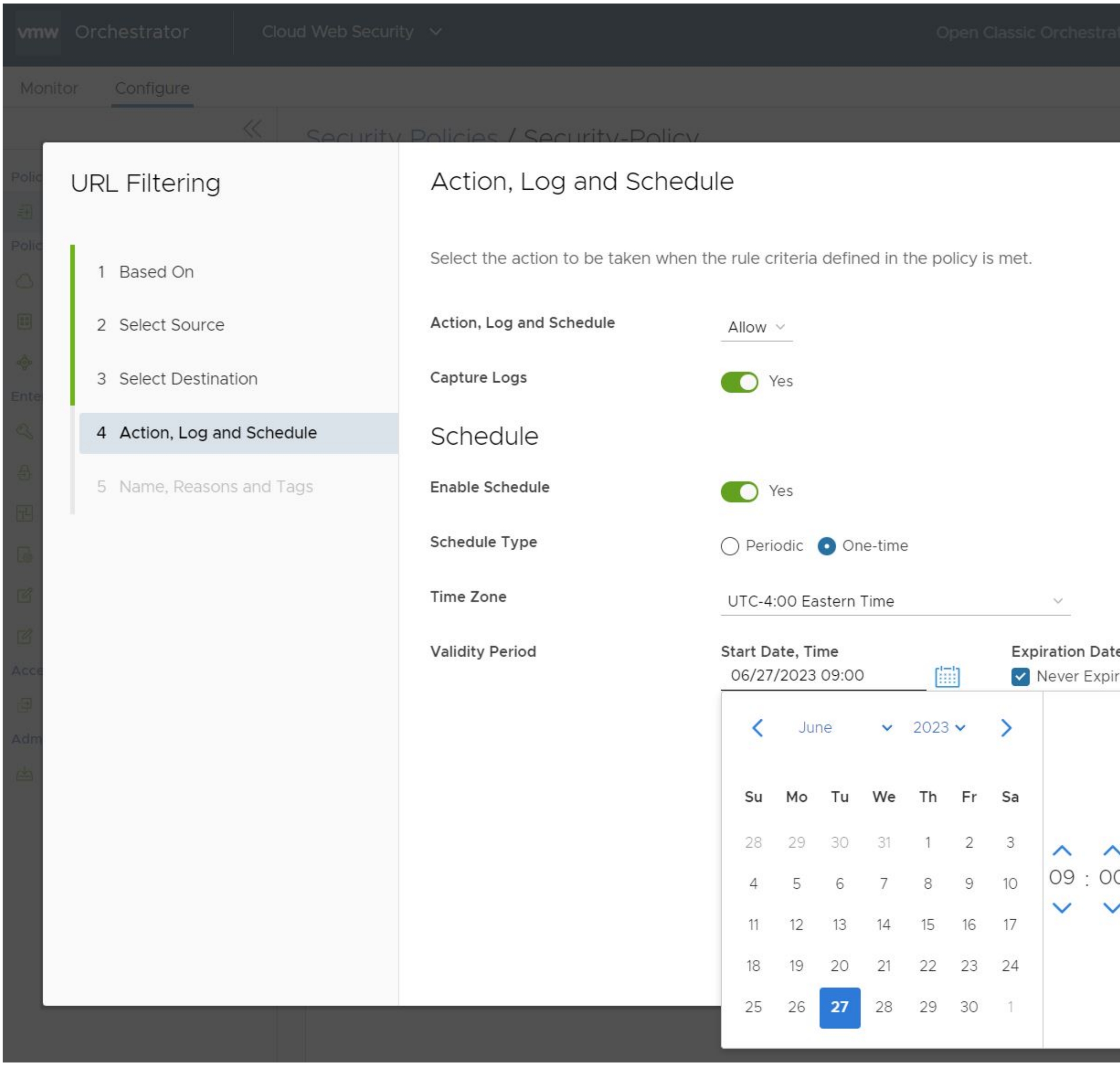
Time Zone: UTC-4:00 Eastern Time

Validity Period: Start Date, Time 06/27/2023 09:00; Expiration Date 07/07/2023 18

For either option a user configures a **Time Zone**, which specifies the time zone the rule will refer to when implementing the **Validity Period** and is expressed in the UTC offset that reflects that time zone's current status relative to Daylight Savings/ Summer Time versus Standard Time. For example, in the above screenshot the Eastern Time zone is selected with a Daylight Savings UTC offset value and would adjust to the Standard Time UTC offset when applicable. For additional information, see the section on the Time Zone option in the **Periodic** section seen earlier.

For a **Validity Period** with both a Start and Expiration Date and Time, configure those time periods either by manually entering the values in each section, or clicking on the calendar icon to open the date and time configuration window.

The second option is to configure a rule with a **Validity Period** that has a Start Date and Time, but no Expiration Date. This is done by configuring the **Start Date, Time** as before, but this time checking the box for **Never Expires**. This rule is applied indefinitely from the Start Date and Time until the user edits or removes the **Schedule** option for it.



Action, Log and Schedule

Select the action to be taken when the rule criteria defined in the policy is met.

Action, Log and Schedule: Allow

Capture Logs: Yes

Schedule

Enable Schedule: Yes

Schedule Type: ○ Periodic ● One-time

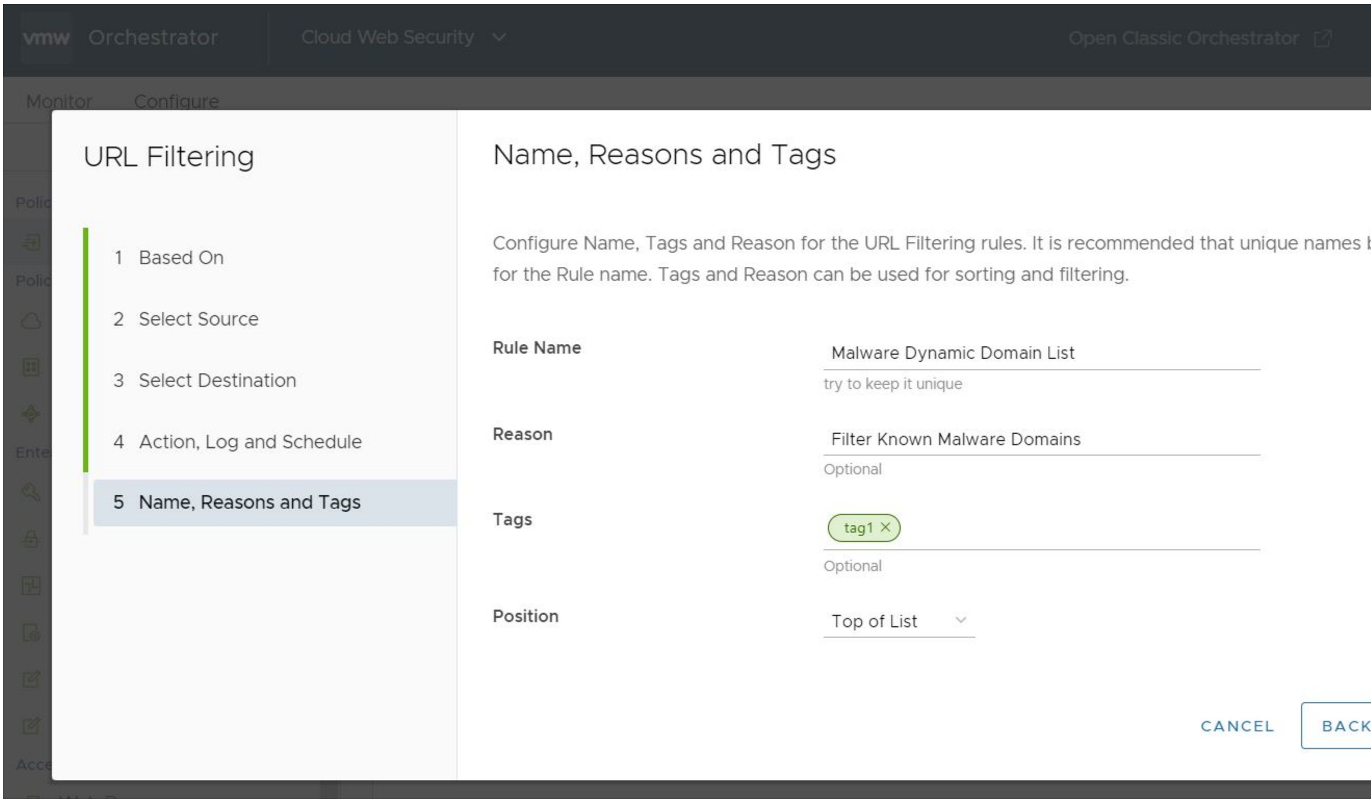
Time Zone: UTC-4:00 Eastern Time

Validity Period: Start Date, Time 06/27/2023 09:00; Expiration Date ☑ Never Expir

Once you have configured all desired parameters for **Action, Log, and Schedule**, click **Next**, and the **Name, Reasons, and Tags** screen appears.

9 In the **Name, Reasons, and Tags** screen, configure a unique **Rule Name** (required), **Tags** (if used), **Reason** (if needed), and a **Position** for the rule on the list of URL Filtering rules (the options are either 'Top of List' or 'Bottom of List').

Note The Position field designates the rule's position on the list of URL Filtering rules.



Name, Reasons and Tags

Configure Name, Tags and Reason for the URL Filtering rules. It is recommended that unique names b for the Rule name. Tags and Reason can be used for sorting and filtering.

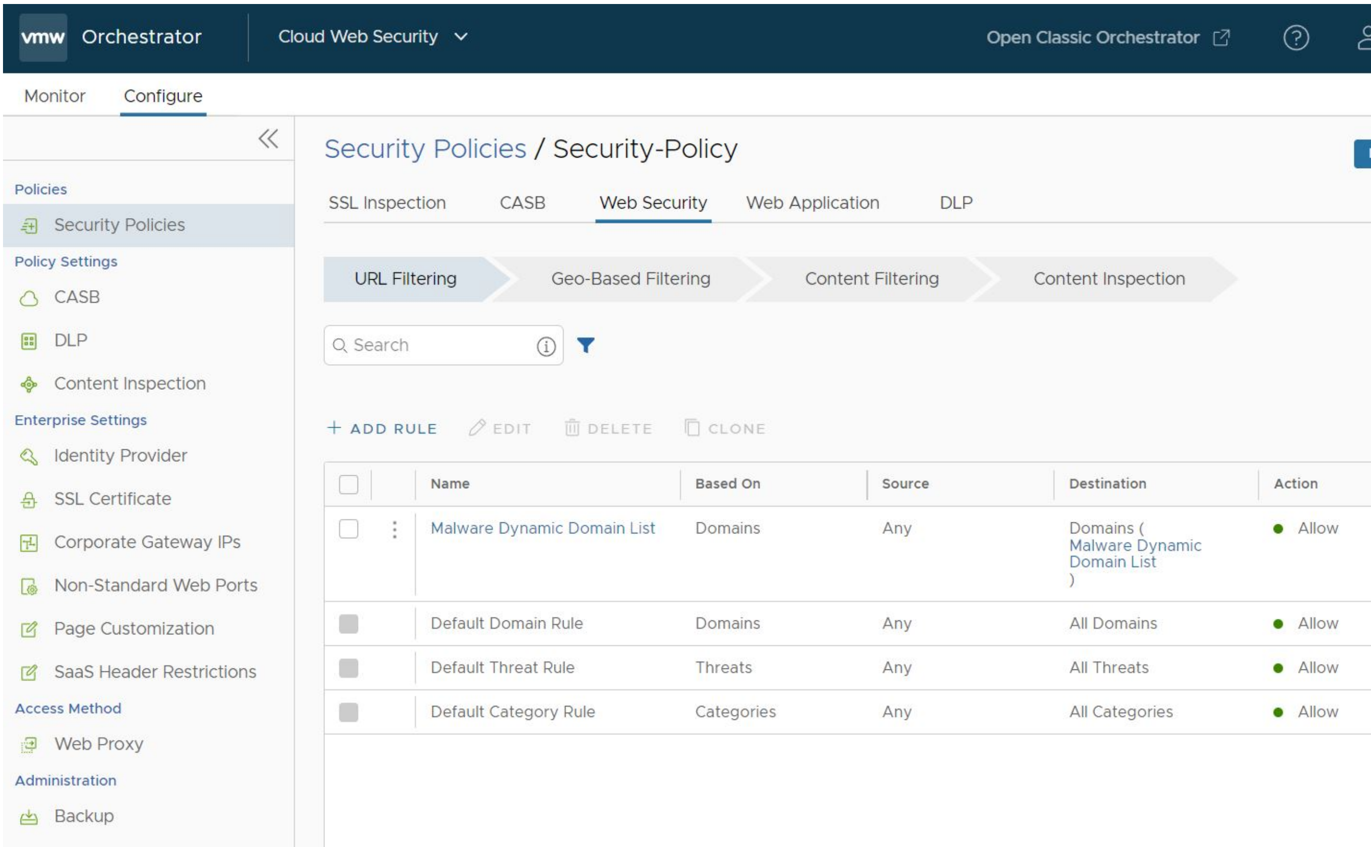
Rule Name: Malware Dynamic Domain List (try to keep it unique)

Reason: Filter Known Malware Domains (Optional)

Tags: tag1 (Optional)

Position: Top of List

10 Click **Finish** and the newly created URL Filtering rule appears in the **URL Filtering** list.



☐	Name	Based On	Source	Destination	Action
☐	Malware Dynamic Domain List	Domains	Any	Domains (Malware Dynamic Domain List)	● Allow
☐	Default Domain Rule	Domains	Any	All Domains	● Allow
☐	Default Threat Rule	Threats	Any	All Threats	● Allow
☐	Default Category Rule	Categories	Any	All Categories	● Allow

11 For the new Security Policy rule to take effect, select the rule and click the **Publish** button on the upper right-hand corner of the screen.

12 After publishing the Security Policy, users can Apply the Security Policy.

13 For an existing security policy, user can perform the following actions by selecting the check box of the policy:

- **Edit** - Allows to modify an existing policy rule.
- **Clone** - Allows to clone a policy from an existing one.
- **Delete** - Allows to delete a policy.

Geo-Based Filtering

Geo-Based Filtering allows users to configure a rule to either block or allow internet traffic based on the geographic region of the content. Cloud Web Security uses MaxMind to resolve the destination IP address and determine the traffic's destination country.

Geo-Based Filtering allows an administrator to:

- Control employee web browsing based on the geographic source and destination of the traffic.
- Allow/Block based on a list of 251 countries.

The default rule for Geo-Based Filtering is:

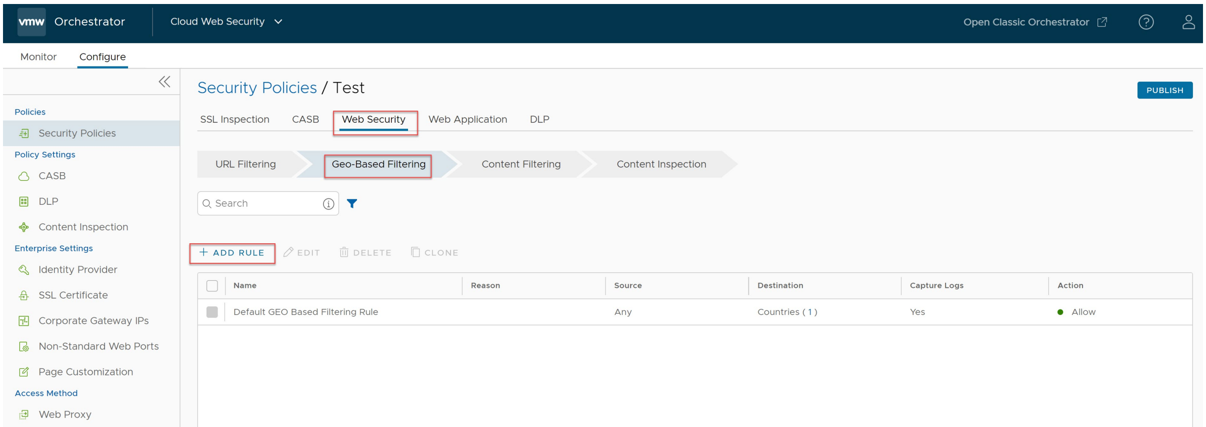
- All downloads and uploads are allowed regardless of their geographic region.

To configure a Geo-Based Filtering rule, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

2 Select a security policy to configure a Geo-Based Filtering rule.

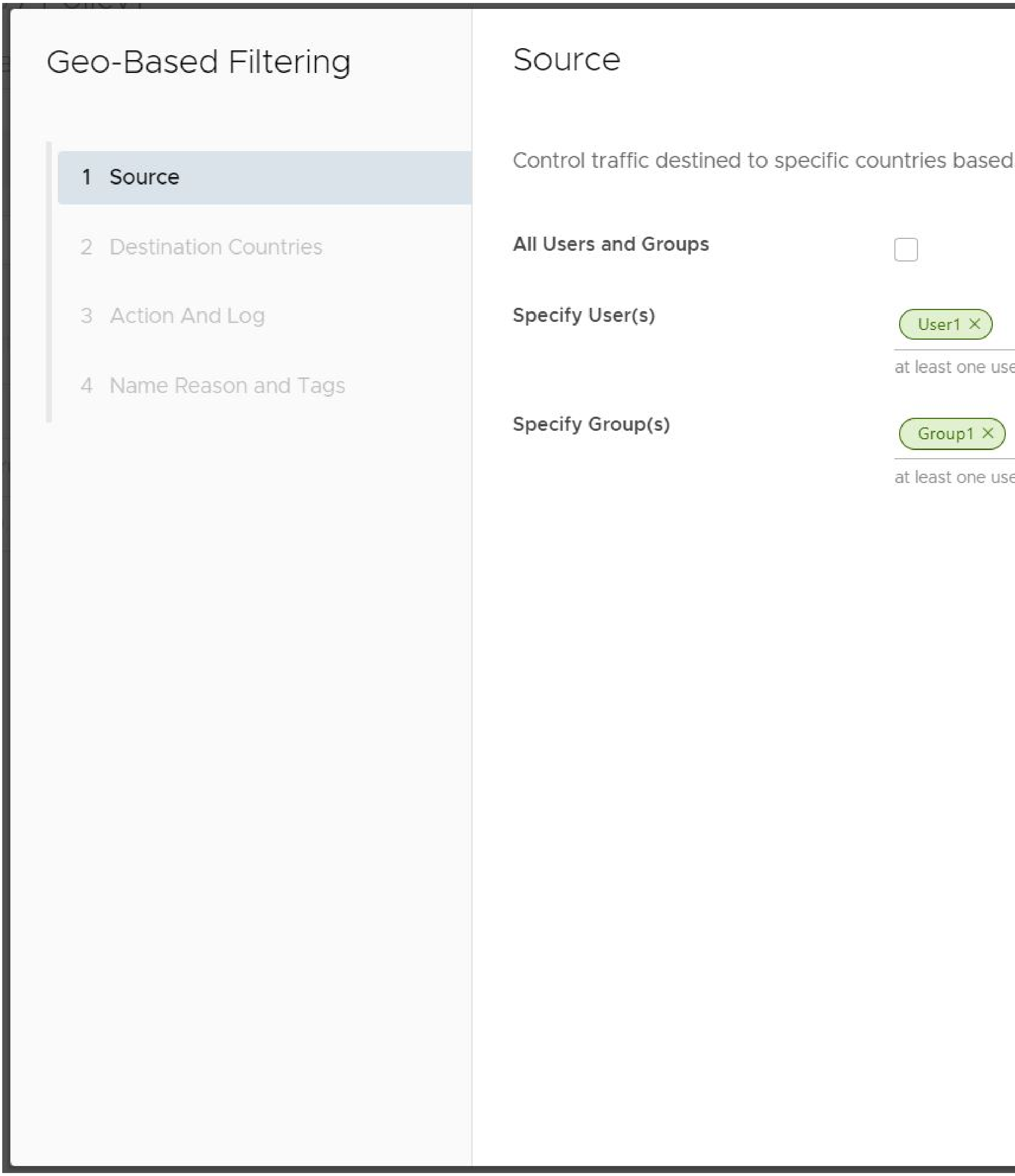
3 In the selected **Security Policies** screen, click the **Web Security** tab.



☐	Name	Reason	Source	Destination	Capture Logs	Action
☐	Default GEO Based Filtering Rule		Any	Countries (1)	Yes	● Allow

4 Under the **Geo-Based Filtering** tab, click **+ ADD RULE**.

The **Source** screen appears.



Geo-Based Filtering

1 Source

2 Destination Countries

3 Action And Log

4 Name Reason and Tags

Source

Control traffic destined to specific countries based

All Users and Groups ☐

Specify User(s) User1 ×

at least one use

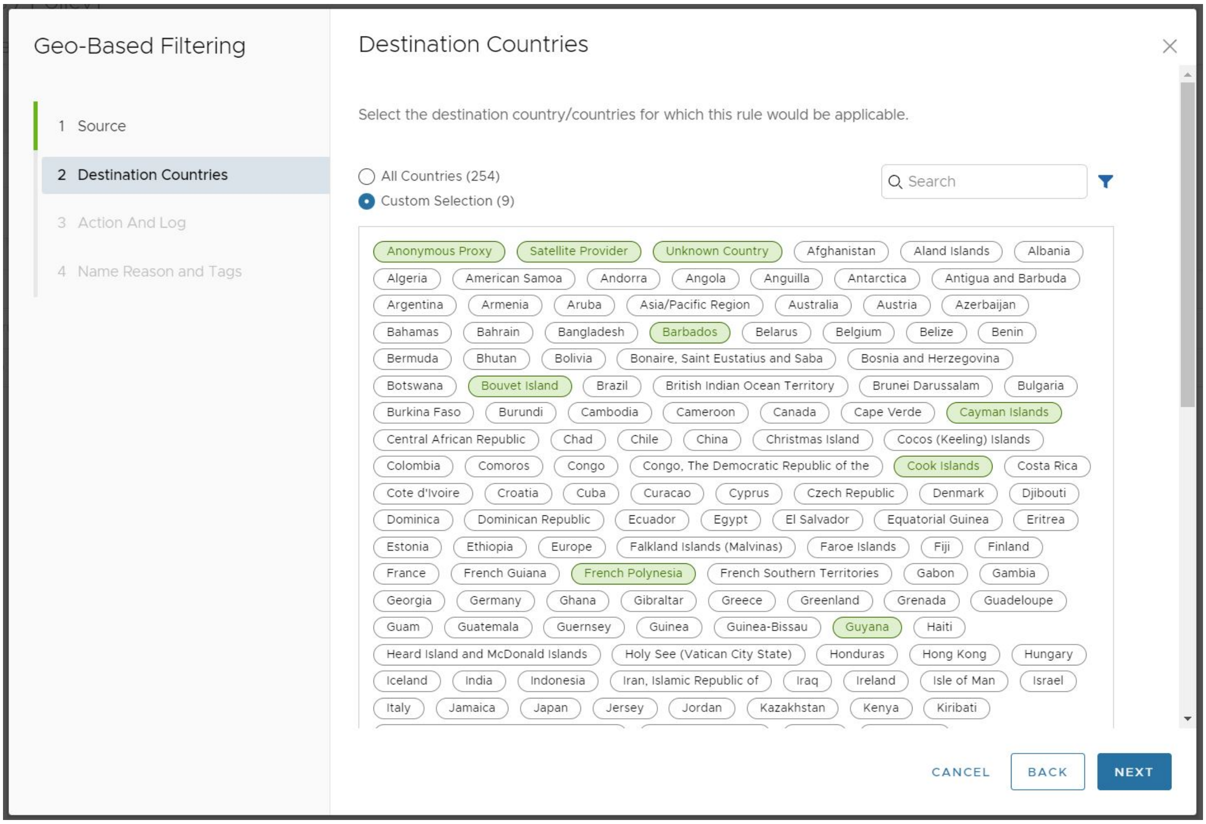
Specify Group(s) Group1 ×

at least one use

5 In the **Source** screen, choose **All Users and Groups** to have the Geo-Based rule apply to everyone in the enterprise. Choose **Specify User(s)** and **Specify Group(s)** fields to specify one or more users and/or groups to which the rule would apply.

Click **Next**, the **Destination Countries** screen appears.

6 In the **Destination Countries** screen, select the countries to apply the rule or exception.



Select the destination country/countries for which this rule would be applicable.

○ All Countries (254)

● Custom Selection (9)

Click **All Countries** and all 251 countries plus Anonymous Proxy, Satellite Provider, and Unknown Country would be part of the rule. Otherwise, use the **Custom Selection** to individually select every country to which you want the rule to apply.

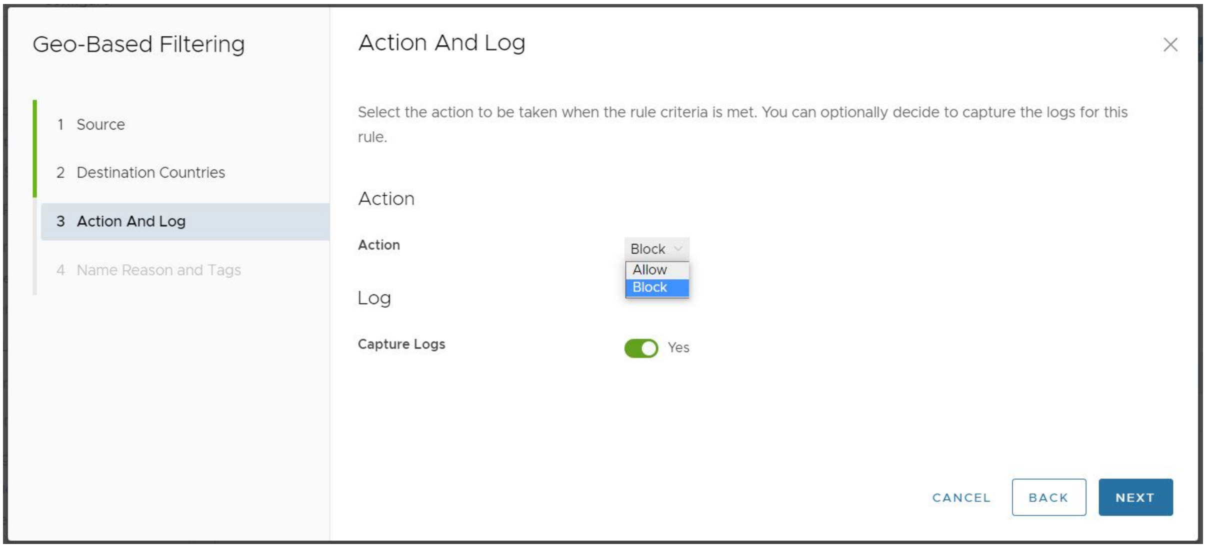
Note The categories **Anonymous Proxy** and **Satellite Provider** are used to help ensure the rule is not circumvented. A client can use an anonymous proxy or a satellite provider link to make traffic going to a selected country appear to be going to one not selected. Adding these two Destinations to a Geo-Based Rule helps mitigate the success of that approach.

Note **Unknown Country** category ensures traffic that MaxMind does not successfully resolve and identifies as "Unknown" is nonetheless subject to a Geo-Based Rule. For more information about MaxMind's geolocation accuracy for a particular country, see their GeoIP2 City Accuracy page. If a country has a low level of geolocation accuracy, select **Unknown Country** to ensure complete coverage under the rule.

Click **Next**, the **Action and Log** screen appears.

7 In the **Action and Log** screen, select the action **Block** or **Allow** from the **Action** drop-down menu to be taken when the rule criteria defined in the policy are met.

Next specify whether **Capture Logs** should be used when the rule is applies to traffic.



Geo-Based Filtering

1 Source
2 Destination Countries
3 Action And Log
4 Name Reason and Tags

Action And Log

Select the action to be taken when the rule criteria is met. You can optionally decide to capture the logs for this rule.

Action

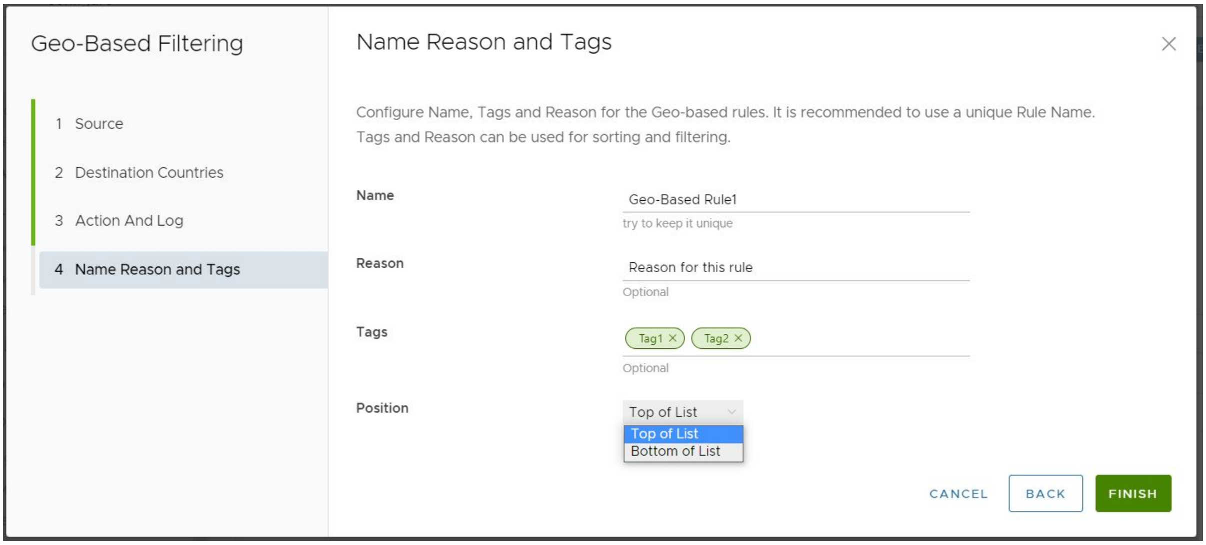
Action: Block (Allow / Block)

Log

Capture Logs: Yes

Click **Next**, the **Name, Reasons, and Tags** screen appears.

8 In the **Name, Reasons, and Tags** screen, configure a unique Rule Name (required), Tags (if used), Reason (if needed), and a Position for the rule on the list of URL Filtering rules (the options are either 'Top of List' or 'Bottom of List').



Geo-Based Filtering

1 Source
2 Destination Countries
3 Action And Log
4 Name Reason and Tags

Name Reason and Tags

Configure Name, Tags and Reason for the Geo-based rules. It is recommended to use a unique Rule Name. Tags and Reason can be used for sorting and filtering.

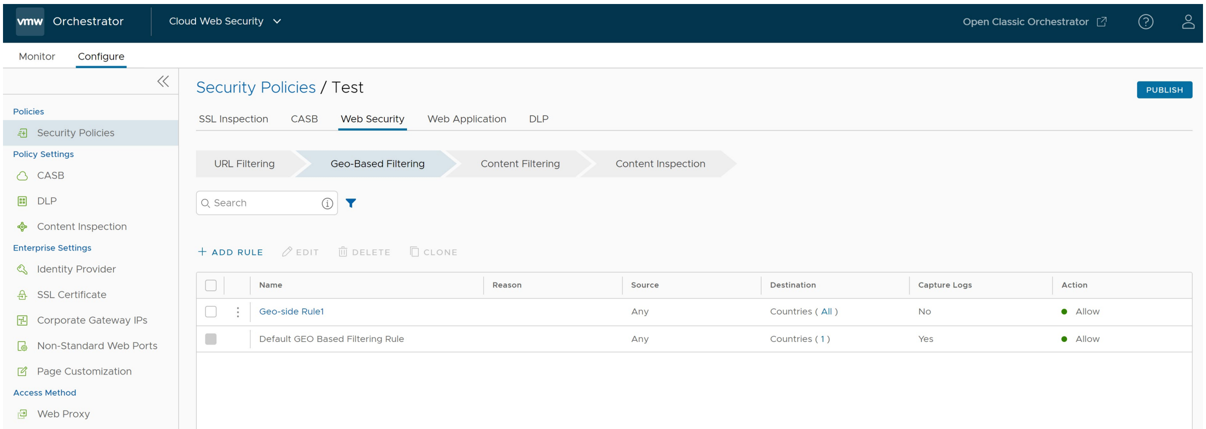
Name: Geo-Based Rule1
try to keep it unique

Reason: Reason for this rule
Optional

Tags: Tag1 × Tag2 ×
Optional

Position: Top of List (Top of List / Bottom of List)

9 Click **Finish** and the newly created Geo-Based Filtering rule appears in the **Geo-Based Filtering** list.



☐		Name	Reason	Source	Destination	Capture Logs	Action
☐	⋮	Geo-side Rule1		Any	Countries (All)	No	● Allow
☐		Default GEO Based Filtering Rule		Any	Countries (1)	Yes	● Allow

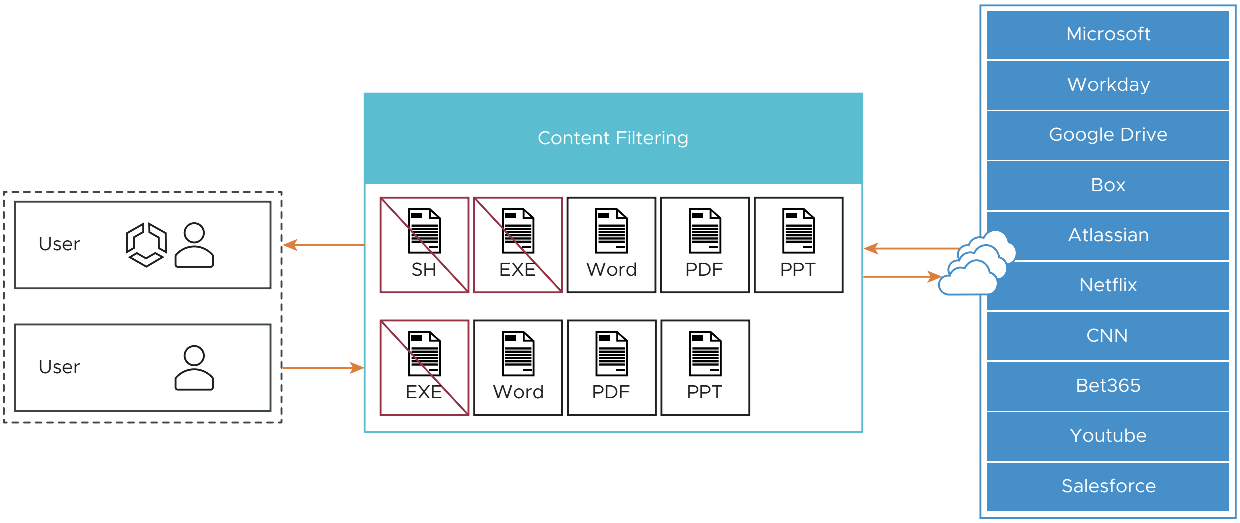
10 For the new Security Policy rule to take effect, select the rule and click the **Publish** button on the upper right-hand corner of the screen.

11 After publishing the Security Policy, users can Apply the Security Policy.

12 For an existing security policy, user can perform the following actions by selecting the check box of the policy:

- **Edit** - Allows to modify an existing policy rule.
- **Clone** - Allows to clone a policy from an existing one.
- **Delete** - Allows to delete a policy.

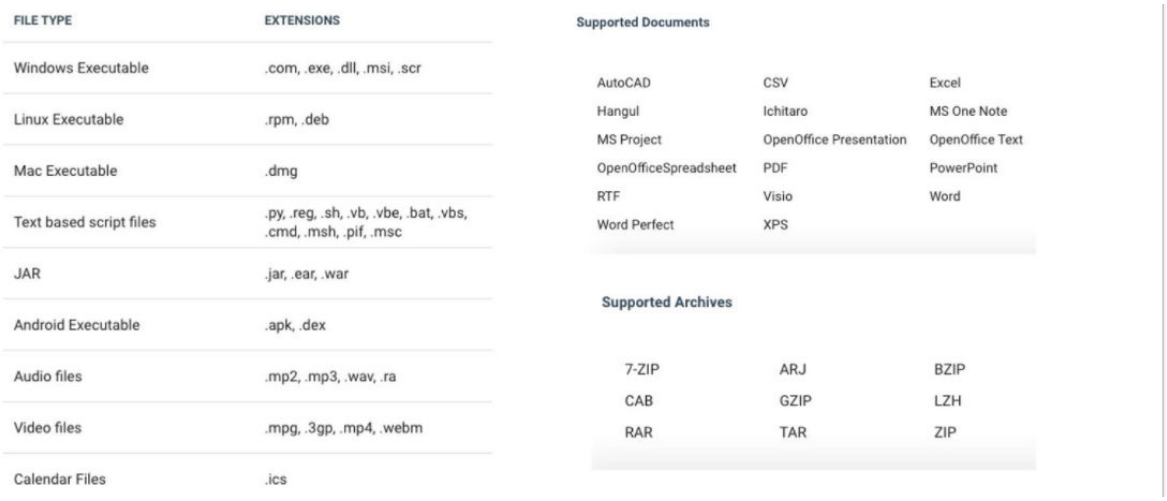
Content Filtering



Content Filtering rules allow an administrator to:

- Reduce attack surface by allowing only required types of content.
- Control content for both uploads and downloads.

  The following document and file types are listed are supported.



FILE TYPE	EXTENSIONS
Windows Executable	.com, .exe, .dll, .msi, .scr
Linux Executable	.rpm, .deb
Mac Executable	.dmg
Text based script files	.py, .reg, .sh, .vb, .vbe, .bat, .vbs, .cmd, .msh, .pif, .msc
JAR	.jar, .ear, .war
Android Executable	.apk, .dex
Audio files	.mp2, .mp3, .wav, .ra
Video files	.mpg, .3gp, .mp4, .webm
Calendar Files	.ics

Supported Documents

AutoCAD	CSV	Excel
Hangul	Ichitaro	MS One Note
MS Project	OpenOffice Presentation	OpenOffice Text
OpenOfficeSpreadsheet	PDF	PowerPoint
RTF	Visio	Word
Word Perfect	XPS	

Supported Archives

7-ZIP	ARJ	BZIP
CAB	GZIP	LZH
RAR	TAR	ZIP

The default rule for Content Filtering are:

- All downloads are allowed, but first undergo a virus scan for harmful content.
- All uploads are allowed without inspection.

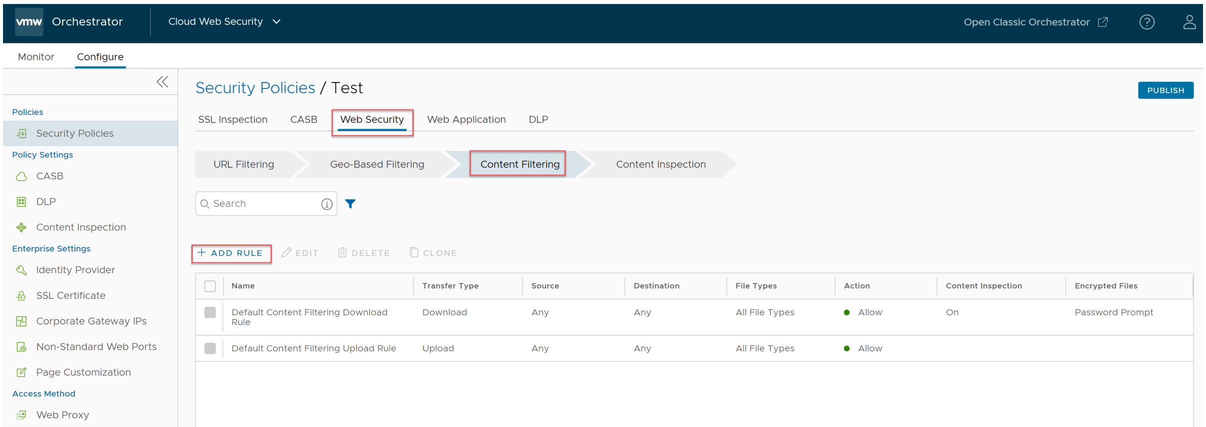
> **Note** Should the virus scan detect harmful content in a download, that download is blocked and logged in Events.

To configure Content Filtering, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

2 Select a security policy to configure a Content Filtering rule.

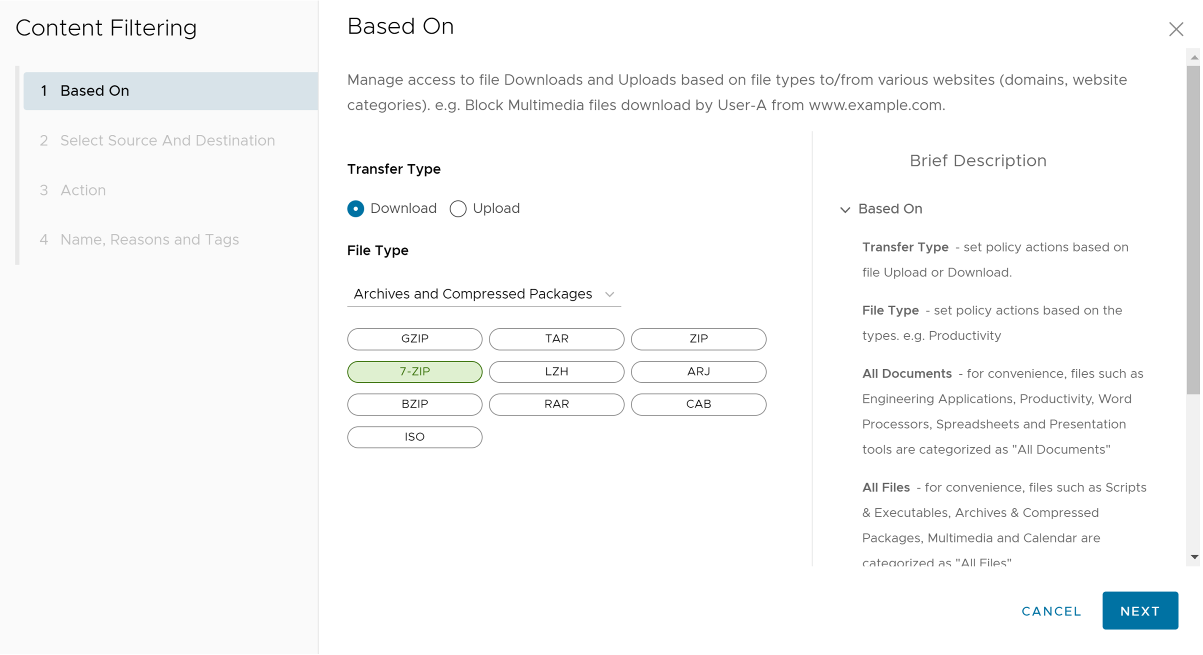
3 In the selected **Security Policies** screen, click the **Web Security** tab.



☐	Name	Transfer Type	Source	Destination	File Types	Action	Content Inspection	Encrypted Files
☐	Default Content Filtering Download Rule	Download	Any	Any	All File Types	● Allow	On	Password Prompt
☐	Default Content Filtering Upload Rule	Upload	Any	Any	All File Types	● Allow		

4 Under the **Content Filtering** tab, click **+ ADD RULE**.

The **Based On** screen appears.



Content Filtering

1 Based On

2 Select Source And Destination

3 Action

4 Name, Reasons and Tags

Based On

Manage access to file Downloads and Uploads based on file types to/from various websites (domains, website categories). e.g. Block Multimedia files download by User-A from www.example.com.

Transfer Type

● Download ○ Upload

File Type

Archives and Compressed Packages

Brief Description

Based On

Transfer Type - set policy actions based on file Upload or Download.

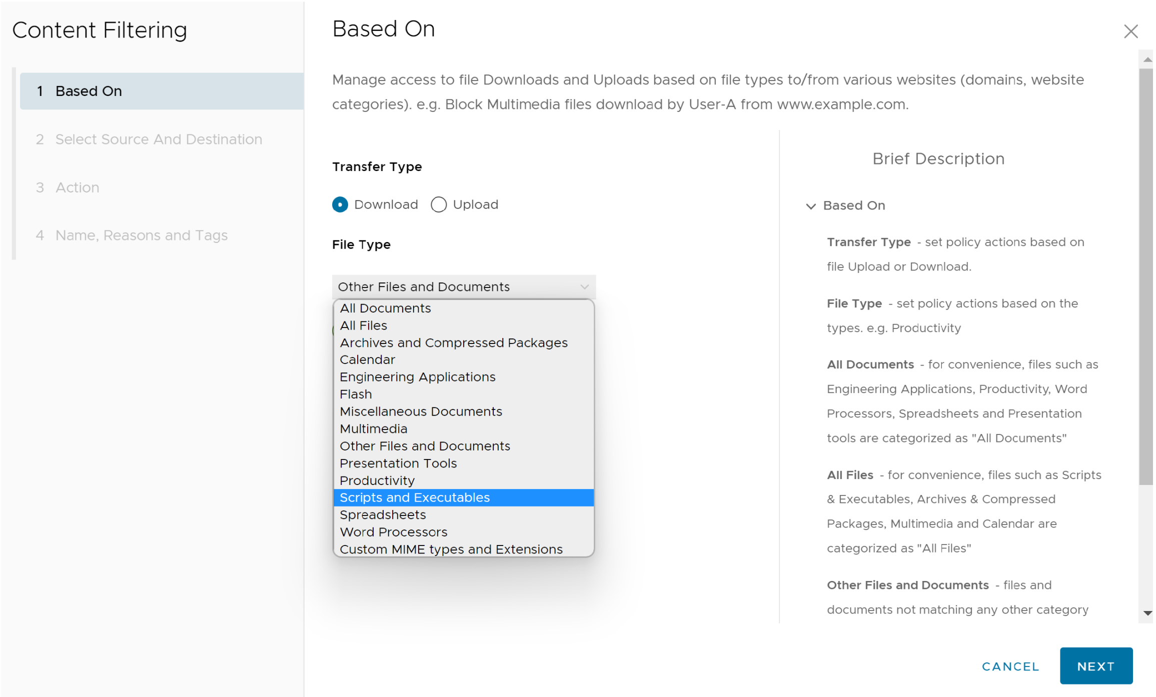
File Type - set policy actions based on the types. e.g. Productivity

All Documents - for convenience, files such as Engineering Applications, Productivity, Word Processors, Spreadsheets and Presentation tools are categorized as "All Documents"

All Files - for convenience, files such as Scripts & Executables, Archives & Compressed Packages, Multimedia and Calendar are categorized as "All Files"

5 In the **Based On** screen, configure the following settings to manage access to file Downloads and Uploads based on file types to/from various websites:

- For the **Transfer Type**, choose either the **Download** or **Upload** radio button. Users cannot select both options. If users want both a download and upload rule, two separate rules are required.
- From the **File Type** drop-down menu, select a file type.



Content Filtering

1 Based On

2 Select Source And Destination

3 Action

4 Name, Reasons and Tags

Based On

Manage access to file Downloads and Uploads based on file types to/from various websites (domains, website categories). e.g. Block Multimedia files download by User-A from www.example.com.

Transfer Type

● Download ○ Upload

File Type

Other Files and Documents

Brief Description

Based On

Transfer Type - set policy actions based on file Upload or Download.

File Type - set policy actions based on the types. e.g. Productivity

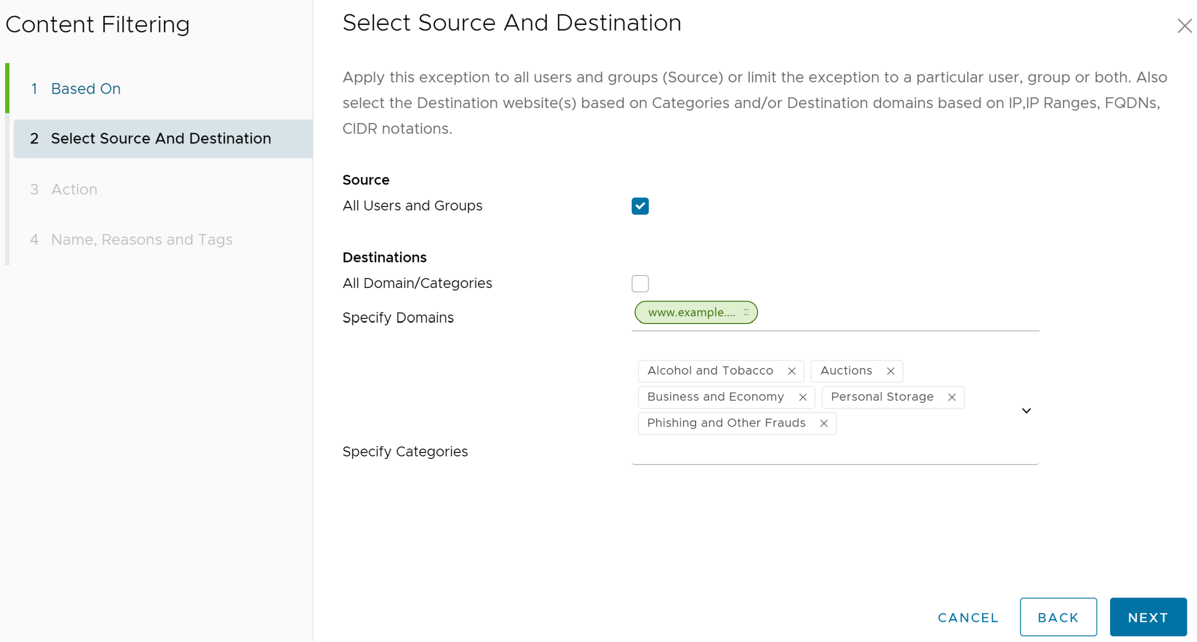
All Documents - for convenience, files such as Engineering Applications, Productivity, Word Processors, Spreadsheets and Presentation tools are categorized as "All Documents"

All Files - for convenience, files such as Scripts & Executables, Archives & Compressed Packages, Multimedia and Calendar are categorized as "All Files"

Other Files and Documents - files and documents not matching any other category

- Click **Next**, the **Select Source and Destination** screen appears.

6 In the **Select Source and Destination** screen, select the source and destination to apply the rule or exception.



Select Source And Destination

Apply this exception to all users and groups (Source) or limit the exception to a particular user, group or both. Also select the Destination website(s) based on Categories and/or Destination domains based on IP,IP Ranges, FQDNs, CIDR notations.

Source

All Users and Groups ☑

Destinations

All Domain/Categories ☐

Specify Domains: www.example....

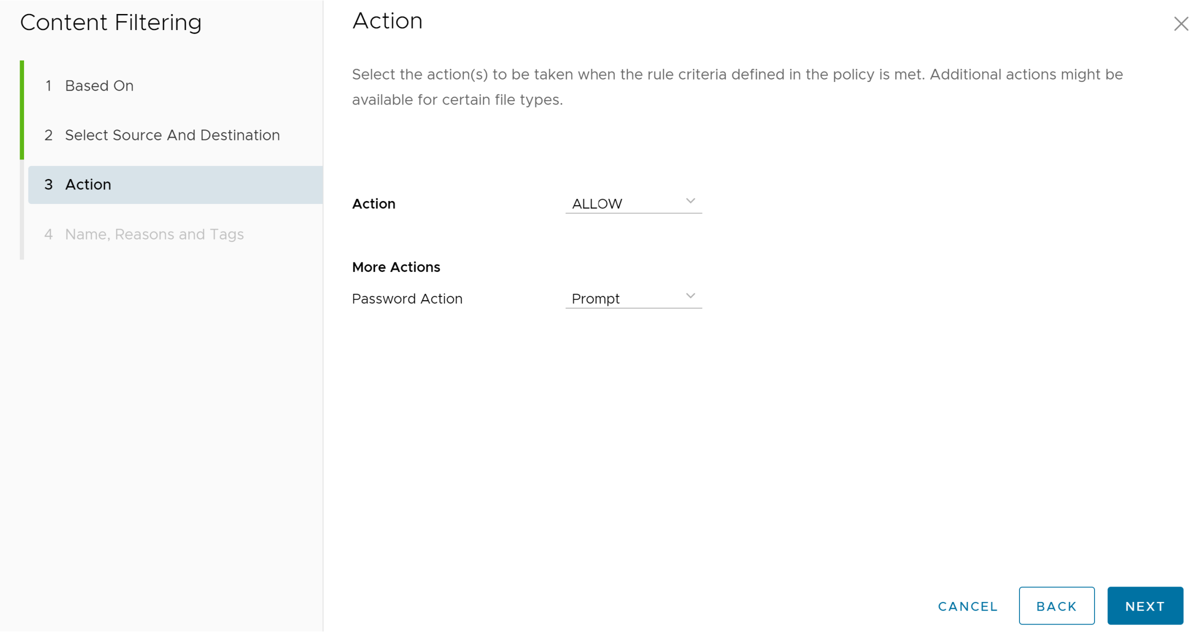
Specify Categories: Alcohol and Tobacco, Auctions, Business and Economy, Personal Storage, Phishing and Other Frauds

a Under **Source**, select the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.

b Under **Destinations**, select either **All Domain/Categories** check box to apply the rule to all available domains and categories, or deselect the check box to specify which Domains and Categories to apply to the rule.

c Click **Next**, the **Action** screen appears.

7 In the **Action** screen, select the action **Block** or **Allow** from the **Action** drop-down menu to be taken when the rule criteria defined in the policy are met. Additionally, users can set **Password Action** (Prompt, Allow, or Block) for certain file types.



Action

Select the action(s) to be taken when the rule criteria defined in the policy is met. Additional actions might be available for certain file types.

Action ALLOW

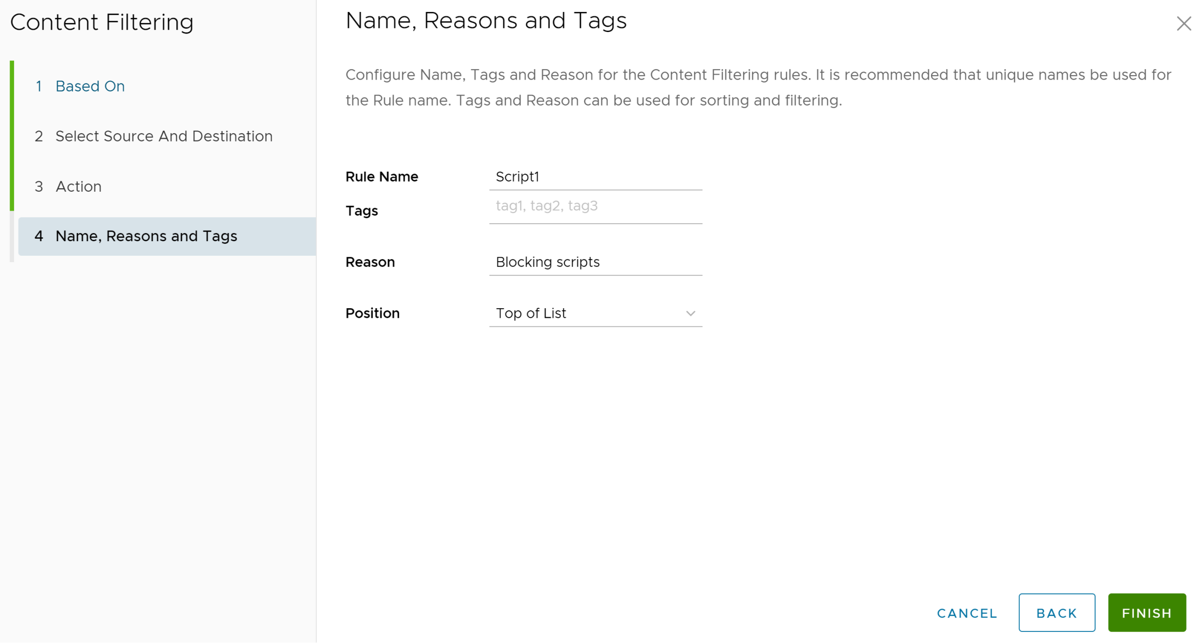
More Actions

Password Action Prompt

Click **Next**, the **Name, Reasons, and Tags** screen appears.

8 In the **Name, Reasons, and Tags** screen, configure a unique Rule Name (required), Tags (if used), Reason (if needed), and a Position for the rule on the list of Content Filtering rules (the options are either 'Top of List' or 'Bottom of List').

Note The Position field designates the rule's position on the list of Content Filtering rules.



Name, Reasons and Tags

Configure Name, Tags and Reason for the Content Filtering rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering.

Rule Name Script1

Tags tag1, tag2, tag3

Reason Blocking scripts

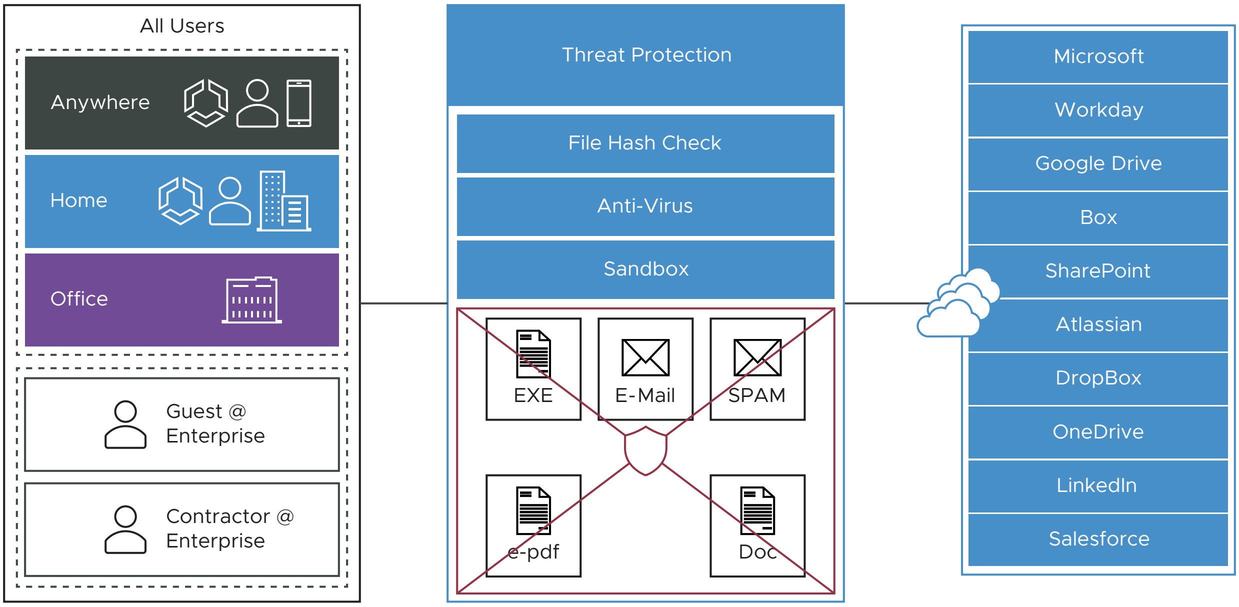
Position Top of List

9 Click **Finish** and the newly created Content Filtering rule appears in the **Content Filtering** list.

10 Users have the following options: configure another rule under Content Filtering, configure a different Security Policy category, or if finished, click the **Publish** button to publish the Security Policy.

11 After publishing the Security Policy, users can Applying a Security Policy.

Content Inspection



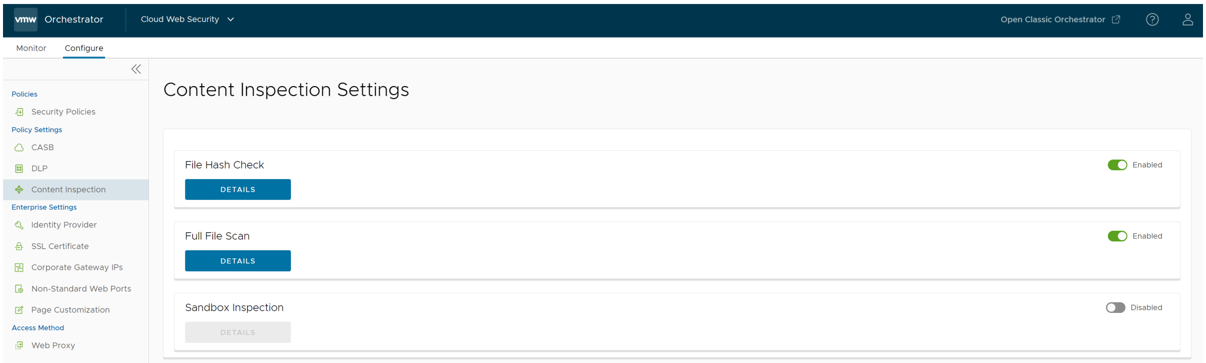
Content Inspection provides protection from active sites with malware content as well as protection against known and “Day 0” threats. Content allowed so far can be inspected to determine if it is harmful.

There are three options for Content Inspection:

- File Hash Check: The file is scanned to see if it matches a known file hash stored in the Cloud Web Security database. A file hash is a unique value and is compared against results from more than 50 AV engines. The result of a hash check can be clean, malicious, or unknown. If clean, the file is allowed onto the network. If malicious, the file is dropped. If unknown, the file will be either dropped or sent to the Anti-Virus Scan, depending on which options were selected. By default, this option is activated for your policy.
- Anti-Virus Scan: The file is scanned by the Cloud Web Security anti-virus application checking for known viruses and malware signatures. If the file matches a known virus or malware, the file is dropped. If the file does not match a known virus/malware, it is either dropped or sent to the Sandbox, depending on which options were selected. By default, this option is activated for your policy.
- Sandbox: The Sandbox is a contained environment where a file can be securely analyzed in two ways:
  - Static Analysis: inspects the file for libraries, functions imported, scans the code for strings, linking methods used, etc.

- Dynamic Analysis: runs the file in a contained environment and determines if the file is infected based on the behavior. Dynamic takes much more time to process.

By default, Sandbox Inspection is deactivated for your policy. You can activate Sandbox Inspection from **Configure > Policy Settings > Content Inspection** page.



File Hash Check: Enabled

Full File Scan: Enabled

Sandbox Inspection: Disabled

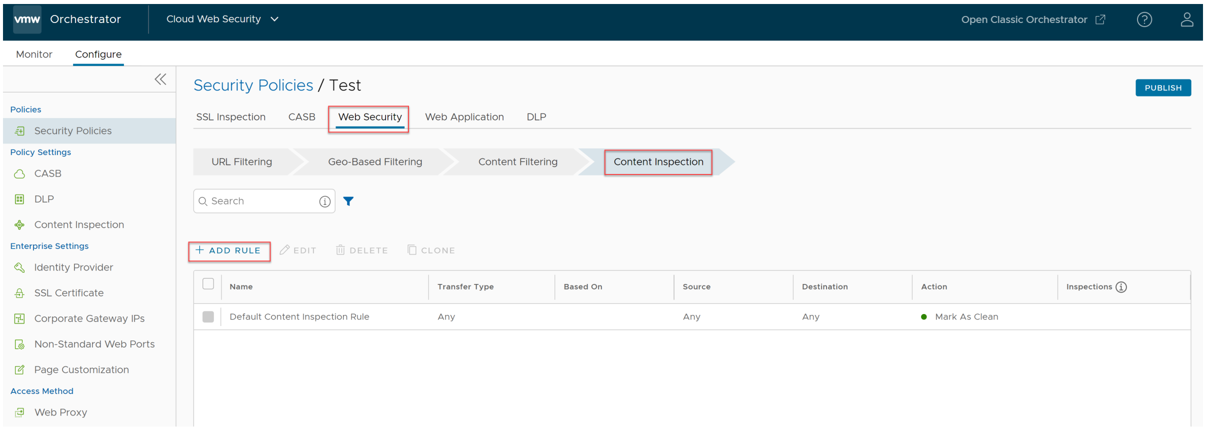
Attention The default content inspection rule for all file types and all sources and destination is to mark them as clean and allow them onto the network.

To configure Content Inspection rule, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

2 Select a security policy to configure a Content Inspection rule.

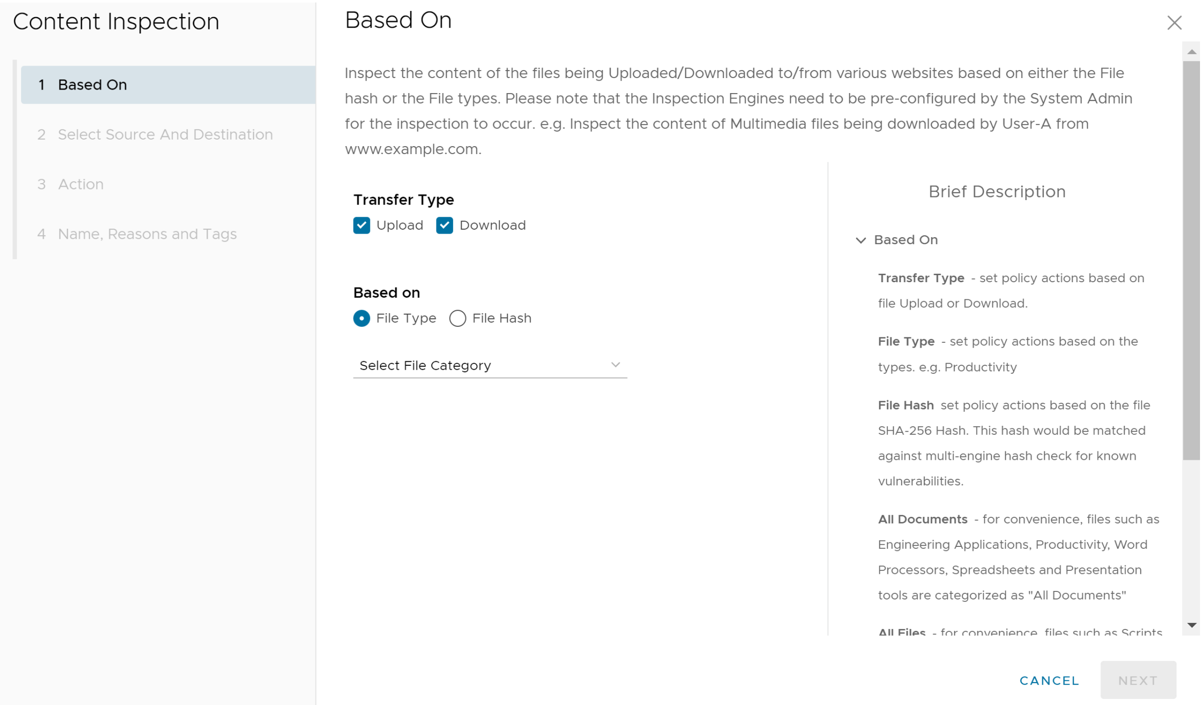
3 In the selected **Security Policies** screen, click the **Web Security** tab.



Name	Transfer Type	Based On	Source	Destination	Action	Inspections
Default Content Inspection Rule	Any		Any	Any	● Mark As Clean	

4 Under the **Content Inspection** tab, click **+ ADD RULE**.

The **Based On** screen appears.



Based On

Inspect the content of the files being Uploaded/Downloaded to/from various websites based on either the File hash or the File types. Please note that the Inspection Engines need to be pre-configured by the System Admin for the inspection to occur. e.g. Inspect the content of Multimedia files being downloaded by User-A from www.example.com.

Transfer Type
☑ Upload ☑ Download

Based on
● File Type ○ File Hash

Select File Category

Brief Description

Based On

Transfer Type - set policy actions based on file Upload or Download.

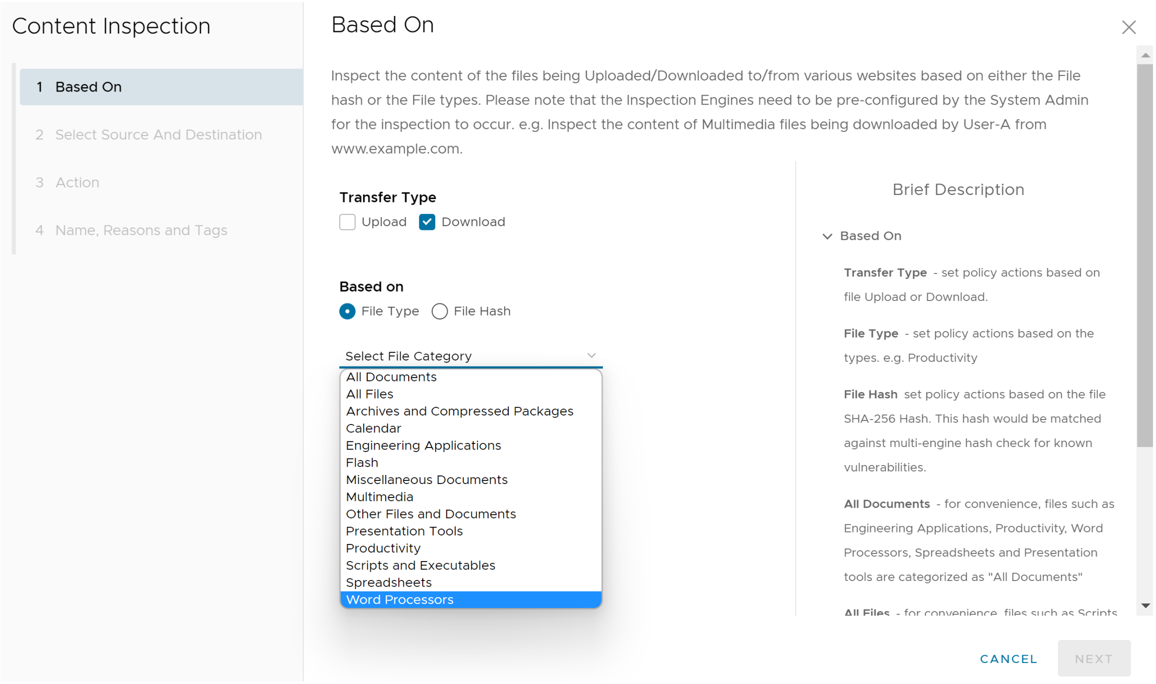
File Type - set policy actions based on the types. e.g. Productivity

File Hash set policy actions based on the file SHA-256 Hash. This hash would be matched against multi-engine hash check for known vulnerabilities.

All Documents - for convenience, files such as Engineering Applications, Productivity, Word Processors, Spreadsheets and Presentation tools are categorized as "All Documents"

5 In the **Based On** screen, configure the following settings to inspect the content of the files being Uploaded/Downloaded to/from various websites based on either the File hash or the File types.:

- For the **Transfer Type**, choose either the **Download** or **Upload** radio button, or choose both types.



Based On

Inspect the content of the files being Uploaded/Downloaded to/from various websites based on either the File hash or the File types. Please note that the Inspection Engines need to be pre-configured by the System Admin for the inspection to occur. e.g. Inspect the content of Multimedia files being downloaded by User-A from www.example.com.

Transfer Type
☐ Upload ☑ Download

Based on
● File Type ○ File Hash

Select File Category
All Documents
All Files
Archives and Compressed Packages
Calendar
Engineering Applications
Flash
Miscellaneous Documents
Multimedia
Other Files and Documents
Presentation Tools
Productivity
Scripts and Executables
Spreadsheets
Word Processors

Brief Description

Based On

Transfer Type - set policy actions based on file Upload or Download.

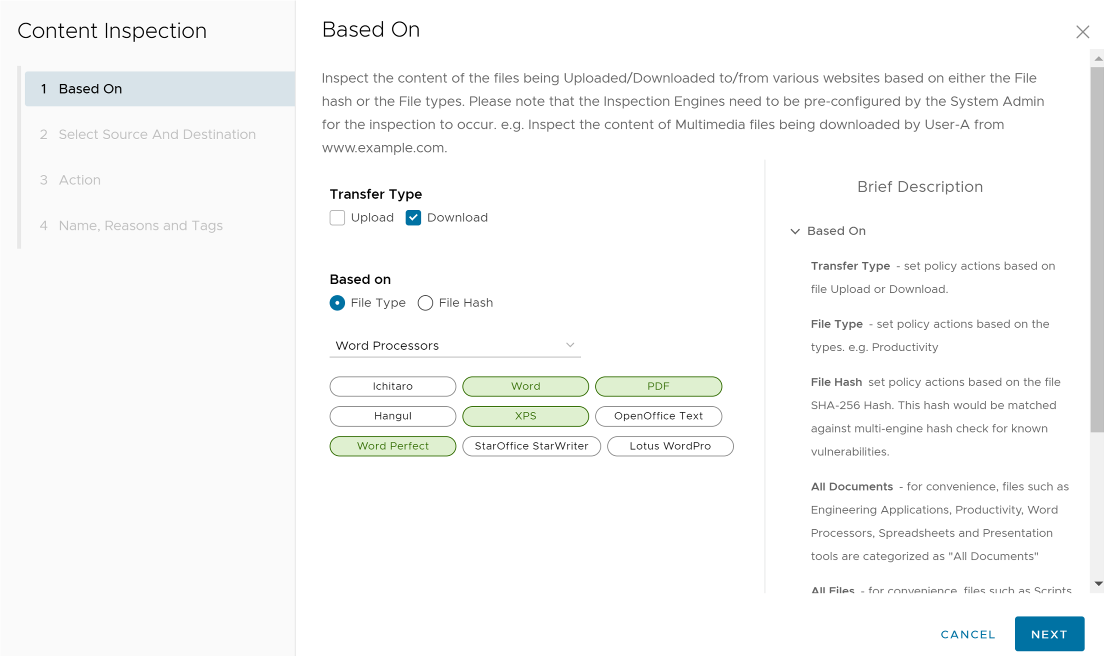
File Type - set policy actions based on the types. e.g. Productivity

File Hash set policy actions based on the file SHA-256 Hash. This hash would be matched against multi-engine hash check for known vulnerabilities.

All Documents - for convenience, files such as Engineering Applications, Productivity, Word Processors, Spreadsheets and Presentation tools are categorized as "All Documents"

- Under **Based on**, select either **File Type** or **File Hash**, which indicates if the inspection will look for files based on File Type or File Hash. (Users cannot choose both).

  1 If users select **File Type**, choose a category from the drop-down menu. For example, users can configure a rule to inspect downloaded files that match the listed Word Processor file types: Word, XPS, OpenOffice Text, and Word Perfect.



Content Inspection

1 Based On

2 Select Source And Destination

3 Action

4 Name, Reasons and Tags

Based On

Inspect the content of the files being Uploaded/Downloaded to/from various websites based on either the File hash or the File types. Please note that the Inspection Engines need to be pre-configured by the System Admin for the inspection to occur. e.g. Inspect the content of Multimedia files being downloaded by User-A from www.example.com.

Transfer Type
☐ Upload ☑ Download

Based on
● File Type ○ File Hash

Word Processors

Ichitaro | Word | PDF
Hangul | XPS | OpenOffice Text
Word Perfect | StarOffice StarWriter | Lotus WordPro

Brief Description

Based On

Transfer Type - set policy actions based on file Upload or Download.

File Type - set policy actions based on the types. e.g. Productivity

File Hash set policy actions based on the file SHA-256 Hash. This hash would be matched against multi-engine hash check for known vulnerabilities.

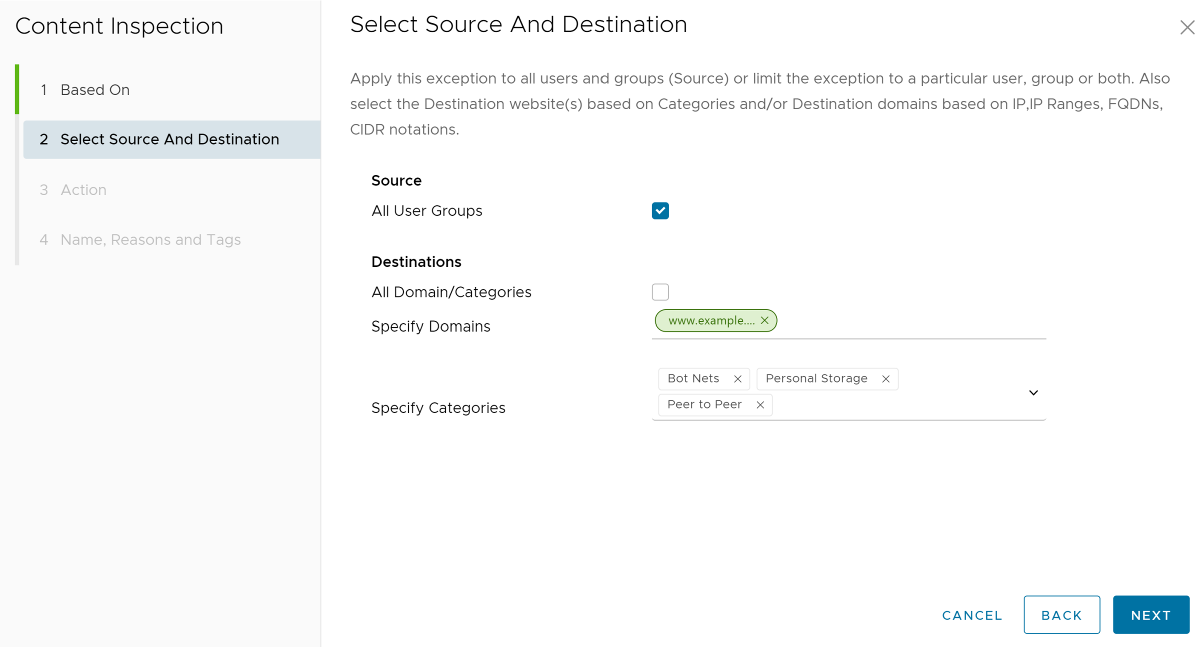
All Documents - for convenience, files such as Engineering Applications, Productivity, Word Processors, Spreadsheets and Presentation tools are categorized as "All Documents"

All Files - for convenience, files such as Scripts

  2 If users select **File Hash**, enter a SHA-256 Hash in the appropriate text box.

- Click **Next**, the **Select Source and Destination** screen appears.

6 In the **Source and Destination** screen appears, select the source and destination to apply the rule.



Content Inspection

1 Based On
2 Select Source And Destination
3 Action
4 Name, Reasons and Tags

Select Source And Destination

Apply this exception to all users and groups (Source) or limit the exception to a particular user, group or both. Also select the Destination website(s) based on Categories and/or Destination domains based on IP,IP Ranges, FQDNs, CIDR notations.

Source

All User Groups ☑

Destinations

All Domain/Categories ☐

Specify Domains: www.example....

Specify Categories: Bot Nets, Personal Storage, Peer to Peer

a Under **Source**, select the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.

b Under **Destinations**, select either **All Domain/Categories** check box to apply the rule to all available domains and categories, or deselect the check box to specify which Domains and Categories to apply to the rule.

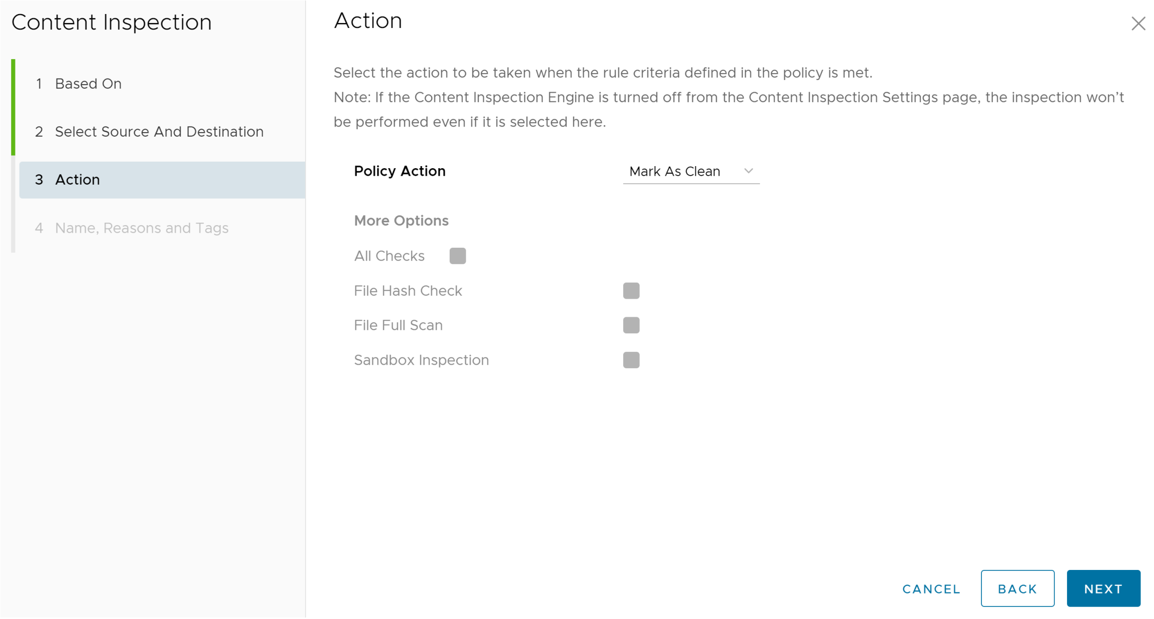
c Click **Next**, the **Action** screen appears.

7 In the **Action** screen, from the **Policy Action** drop-down menu choose any one of the following actions: **Mark As Clean**, **Mark As Infected**, or **Inspect**.

Table 1-2. Policy Action Description

Policy Action	Description
Mark As Clean	The files will automatically be permitted onto the network without inspection.
Mark As Infected	The files will automatically be treated as dangerous and will be dropped and not permitted onto the network.
Inspect	The matching files will be subject up to three different inspection options, and if the file fails the inspection, it will be dropped.

a If users choose either the **Mark As Clean** or **Mark As Infected** policy actions, the Inspection Options (All Checks, File Hash Check, File Full Scan, Sandbox Inspection) are not available.



Action

Select the action to be taken when the rule criteria defined in the policy is met.
Note: If the Content Inspection Engine is turned off from the Content Inspection Settings page, the inspection won't be performed even if it is selected here.

Policy Action: Mark As Clean

More Options

All Checks ☐

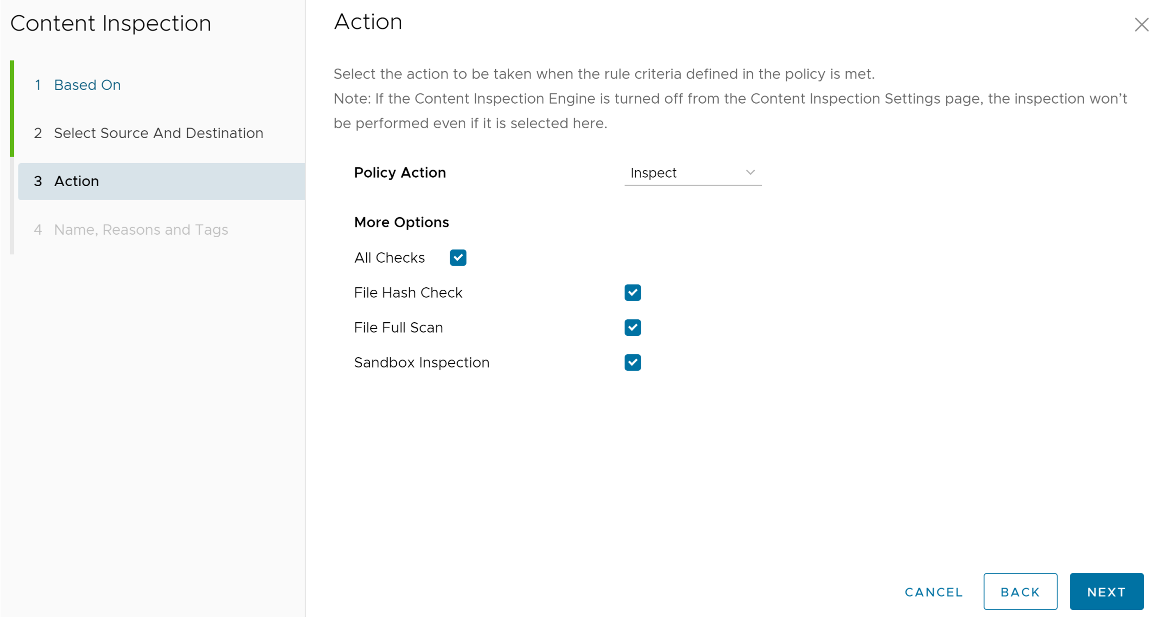
File Hash Check ☐

File Full Scan ☐

Sandbox Inspection ☐

b If users choose the **Inspect** Policy Action, user can select up to three Inspection Options (File Hash Check, File Full Scan, Sandbox Inspection).

Note The **All Checks** option mean all three options (File Hash Check, File Full Scan, Sandbox Inspection) are selected.



Action

Select the action to be taken when the rule criteria defined in the policy is met.
Note: If the Content Inspection Engine is turned off from the Content Inspection Settings page, the inspection won't be performed even if it is selected here.

Policy Action: Inspect

More Options

All Checks ☑

File Hash Check ☑

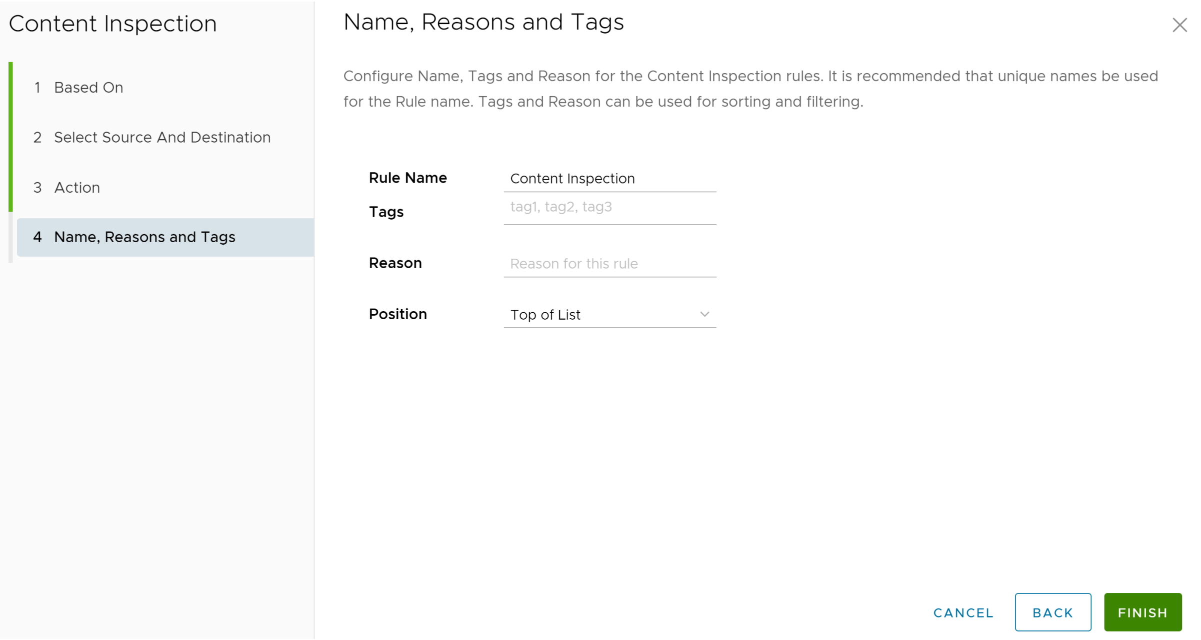
File Full Scan ☑

Sandbox Inspection ☑

Click **Next**, the **Name, Reasons, and Tags** screen appears.

8 In the **Name, Reasons and Tags** screen, configure a unique Rule Name (required), Tags (if used), Reason (if needed), and a Position for the rule on the list of Content Inspection rules (the options are either 'Top of List' or 'Bottom of List').

Note The Position field designates the rule's position on the list of Content Inspection rules.



Configure Name, Tags and Reason for the Content Inspection rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering.

Rule Name: Content Inspection
Tags: tag1, tag2, tag3
Reason: Reason for this rule
Position: Top of List

9 Click **Finish** and the newly created Content Inspection rule appears in the **Content Inspection** list.

10 Users have the following options: configure another rule under Content Filtering, configure a different Security Policy category, or if finished, click the **Publish** button to publish the Security Policy.

11 After publishing the Security Policy, users can Applying a Security Policy.

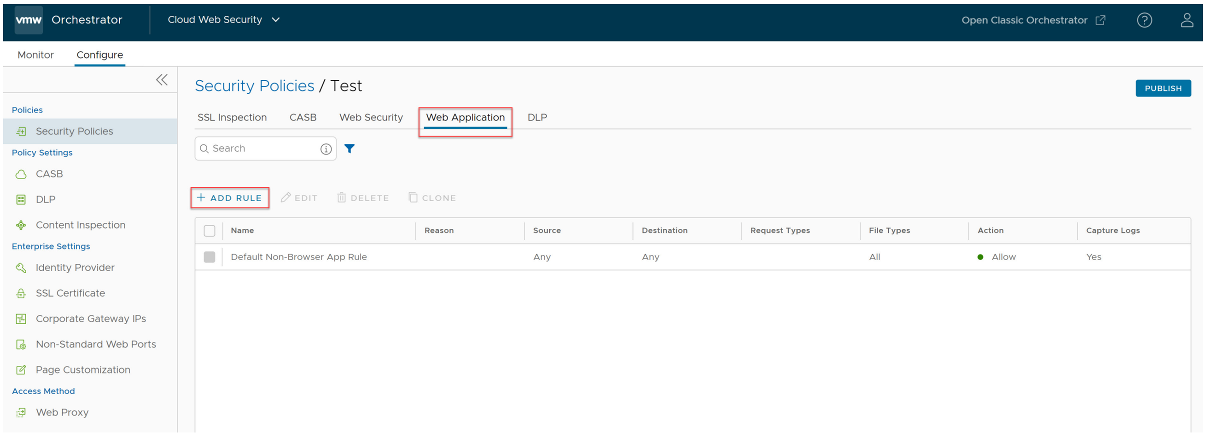
Configure Non-Browser Web Application Rules

VMware Cloud Web Security allows users to configure a CWS Security Policy rule to inspect browser-based web applications like Chrome, Edge, Firefox, Safari, and so on, but the rule would not apply for Non-Browser Web Applications like Slack or Dropbox. Beginning with Release 1.10.0, users have the option to configure rules to inspect browser traffic on Non-Browser Web Applications.

Users can view, add, and remove rules for Non-Browser Web Applications traffic. To configure rules for a Non-Browser Web Application, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

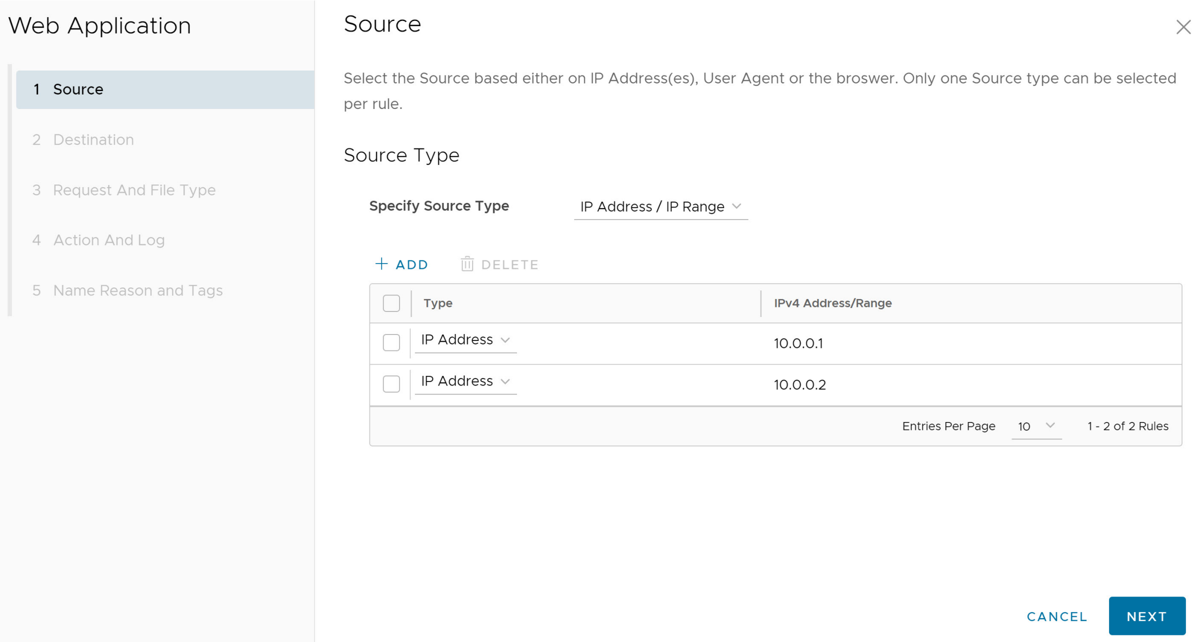
2 Select a security policy to configure Web Applications rule. In the selected **Security Policies** screen, click the **Web Application** tab.



☐	Name	Reason	Source	Destination	Request Types	File Types	Action	Capture Logs
☐	Default Non-Browser App Rule		Any	Any		All	● Allow	Yes

3 Click **+ ADD RULE** and enter all the required details such as Source type, Destination type, Request and File types, Action and Log details to create a new Non-Browser Web Application rule.

4 In the **Source** screen, select the source for which Non-Browser Web Application inspection should apply. Users can select the source based on IP Address/IP Range, User Agent, or Browser as described in the following table.



Select the Source based either on IP Address(es), User Agent or the broswer. Only one Source type can be selected per rule.

Specify Source Type: IP Address / IP Range

☐	Type	IPv4 Address/Range
☐	IP Address	10.0.0.1
☐	IP Address	10.0.0.2

Entries Per Page 10 1 - 2 of 2 Rules

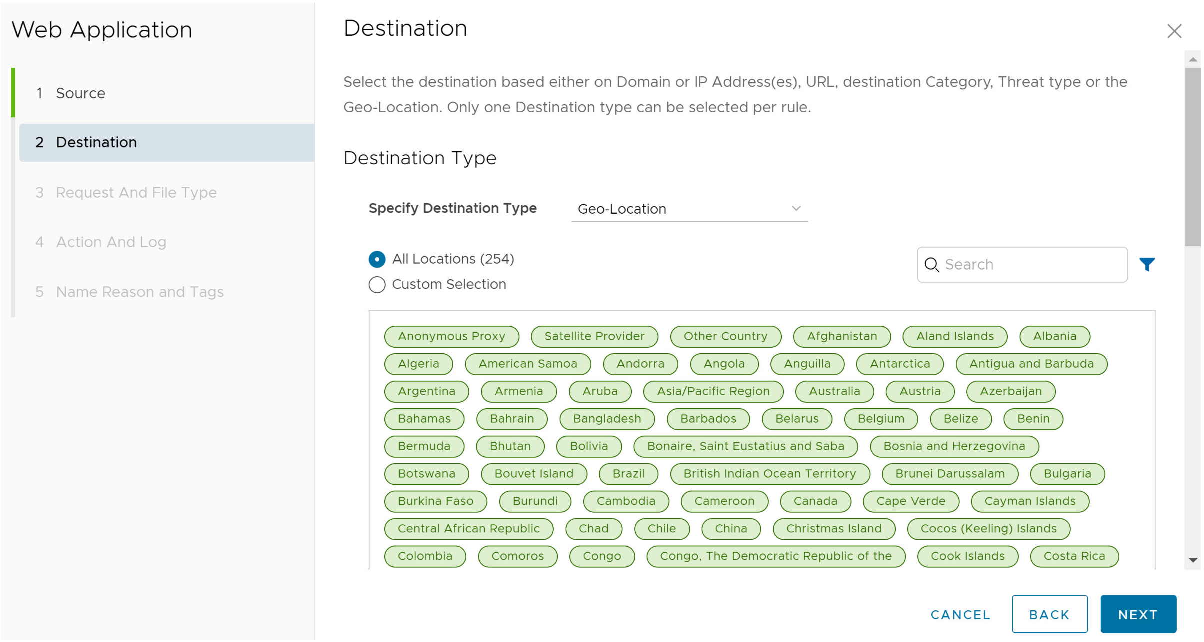
Field	Description
Any	The default setting is "**Any**" and the policy inspects browser traffic on Non-Browser Web Applications from all source types.
IP Address/IP Range	Specify an IP address (for example, 10.0.0.1) or IP range (for example, 10.01.1- 10.0.2.225) to apply the rule.

Field	Description
User Agent	Set policy actions based on the match criteria (text or expression) specified using the following: - Equals - Starts with - Contains - Ends with - RegEx Optionally, users can also include specific Source IP Address/IP range or use the default setting "**Any Source IP Address**".
Browser	Specify the web browsers to apply the rule. Users can set policy actions based on any of the following web browsers: - Google Chrome - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Apple Safari - Samsung Internet Optionally, users can also include specific Source IP Address/IP range or use the default setting "**Any Source IP Address**".

Note Only one Source type can be selected per rule.

Click **Next**. The **Destination** screen appears.

5 In the **Destination** screen, select the destination for which Non-Browser Web Application inspection should apply. Users can select the destination based on Domain, IP Address/IP Range, URL, Category, Threat, or Geo-Location as described in the following table.



Web Application

1 Source

2 Destination

3 Request And File Type

4 Action And Log

5 Name Reason and Tags

Destination

Select the destination based either on Domain or IP Address(es), URL, destination Category, Threat type or the Geo-Location. Only one Destination type can be selected per rule.

Destination Type

Specify Destination Type Geo-Location

● All Locations (254)

○ Custom Selection

Anonymous Proxy, Satellite Provider, Other Country, Afghanistan, Aland Islands, Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, Asia/Pacific Region, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belgium, Belize, Benin, Bermuda, Bhutan, Bolivia, Bonaire, Saint Eustatius and Saba, Bosnia and Herzegovina, Botswana, Bouvet Island, Brazil, British Indian Ocean Territory, Brunei Darussalam, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Canada, Cape Verde, Cayman Islands, Central African Republic, Chad, Chile, China, Christmas Island, Cocos (Keeling) Islands, Colombia, Comoros, Congo, Congo, The Democratic Republic of the, Cook Islands, Costa Rica

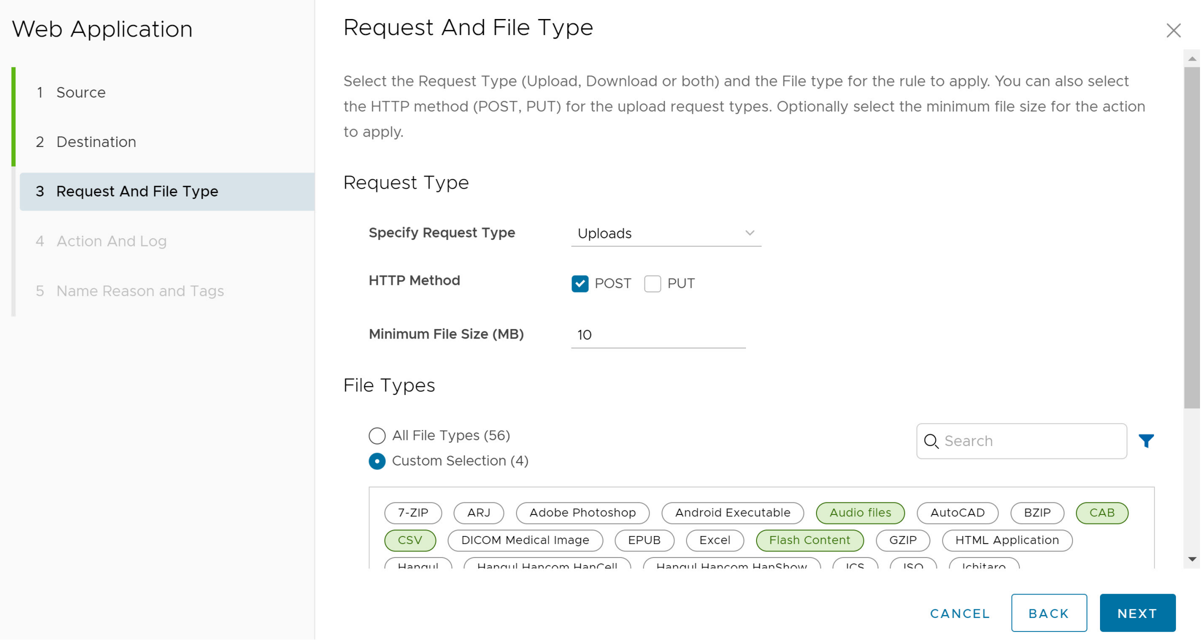
Field	**Description**
Any	The default setting is "**Any**" and the policy inspects browser traffic on Non-Browser Web Applications from all destination types.
Domain/IP Address/IP Range	Specify Fully Qualified Domain Names (FQDN), IP address (for example, 10.0.0.1) or IP range (for example, 10.01.1- 10.0.2.225) to apply the rule.
URL - Regex	Set policy actions for URLs based on the match criteria (text or expression) specified using the following: ■ Equals ■ Starts with ■ RegEx
Category	Select either **All Categories** or **Custom Selection**. The **All Categories** option highlights all available categories and applies them to the rule. The **Custom Selection** option allows users to specify which categories to apply to the rule by clicking on each category.

Field	Description
Threat	Select either **All Threats** or **Custom Selection**. The **All Threats** option highlights all available threats and applies them to the rule. The **Custom Selection** option allows users to specify which threats to apply to the rule by clicking on each threat.
Geo-Location	Select either **All Locations** or **Custom Selection**. The **All Locations** option highlights all available locations and applies them to the rule. The **Custom Selection** option allows users to specify which locations to apply to the rule by clicking on each location.

Note Only one Destination type can be selected per rule.

Click **Next**. The **Request And File Type** screen appears.

6 In the **Request And File Type** screen, select the Request Type (Uploads, Downloads, or Both) and the File Type for the rule to apply. Users can also select the HTTP method (POST, PUT) for the Upload request type. Optionally, users can also enter the minimum file size for the action to apply.



Request And File Type

Select the Request Type (Upload, Download or both) and the File type for the rule to apply. You can also select the HTTP method (POST, PUT) for the upload request types. Optionally select the minimum file size for the action to apply.

Request Type

Specify Request Type: Uploads

HTTP Method: ☑ POST ☐ PUT

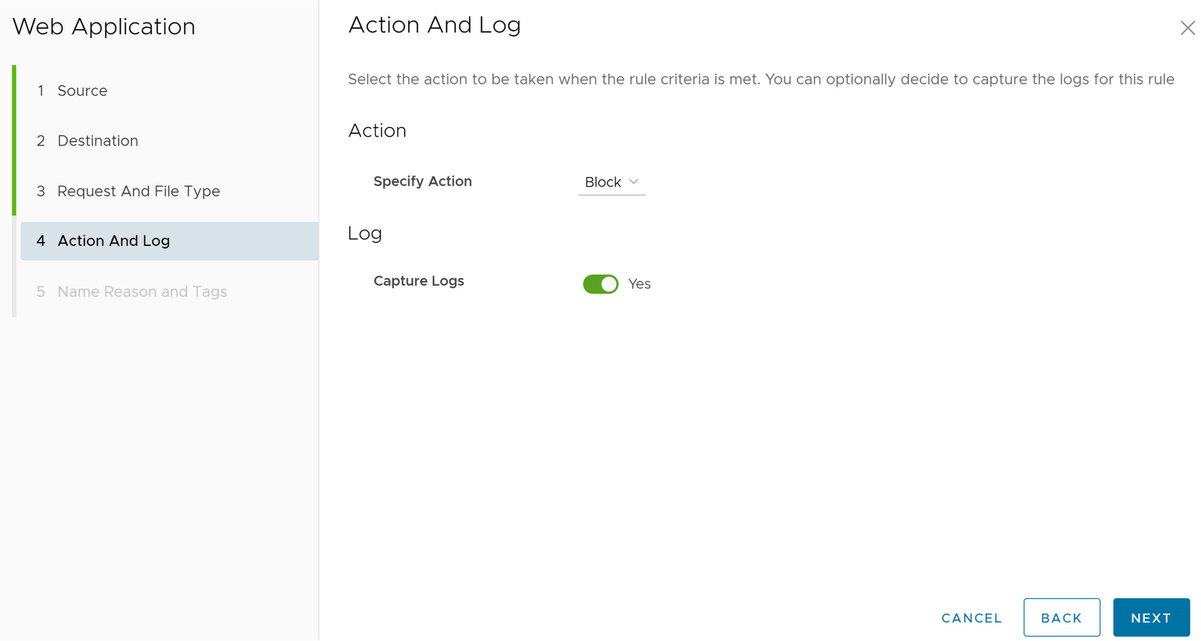
Minimum File Size (MB): 10

File Types

○ All File Types (56)
● Custom Selection (4)

Click **Next**. The **Action and Log** screen appears.

7 In the **Action And Log** screen, select the action (Allow or Block) to be taken if the rule criteria are met. Optionally, users can collect the logs for this rule by turning ON the **Capture Logs** toggle button.



Action And Log

Select the action to be taken when the rule criteria is met. You can optionally decide to capture the logs for this rule

Action

Specify Action: Block

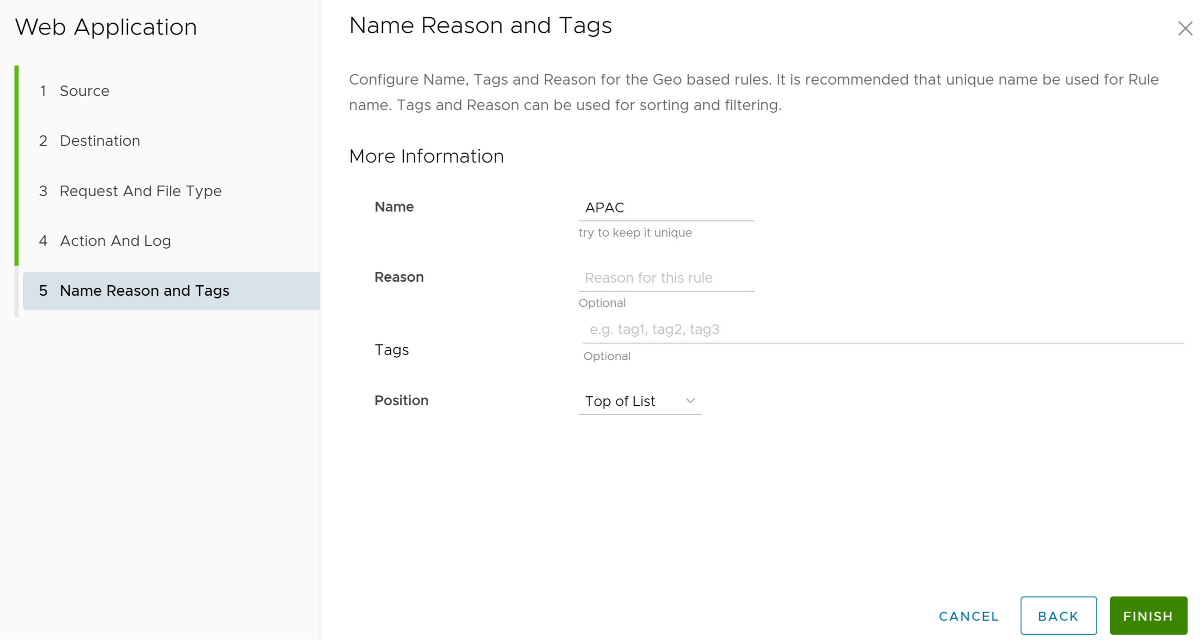
Log

Capture Logs: Yes

Click **Next**. The **Name, Reason and Tags** screen appears.

8 In the **Name, Reason and Tags** screen, configure a unique Rule Name (required), Tags (if used), Reason (if needed), and a Position for the rule on the list of Non-Browser Web Application rules (the options are either 'Top of List' or 'Bottom of List').

Note The Position field designates the rule's position on the list of Web Application rules.



Name Reason and Tags

Configure Name, Tags and Reason for the Geo based rules. It is recommended that unique name be used for Rule name. Tags and Reason can be used for sorting and filtering.

More Information

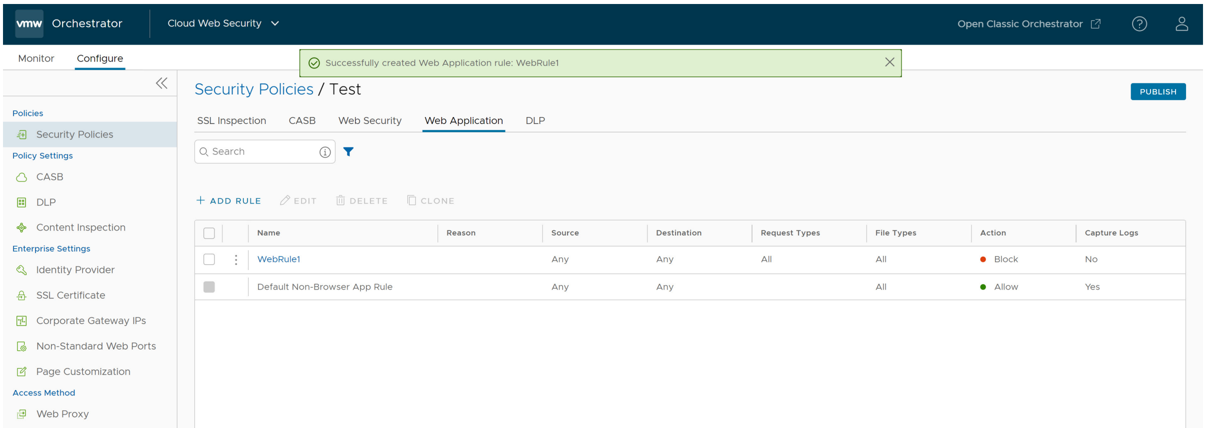
Name: APAC
try to keep it unique

Reason: Reason for this rule
Optional

Tags: e.g. tag1, tag2, tag3
Optional

Position: Top of List

9 Click **Finish** and the newly created Web Application rule appears in the **Web Application** list.



Successfully created Web Application rule: WebRule1

		Name	Reason	Source	Destination	Request Types	File Types	Action	Capture Logs
☐	⋮	WebRule1		Any	Any	All	All	● Block	No
☐		Default Non-Browser App Rule		Any	Any		All	● Allow	Yes

10 For the new Security Policy rule to take effect, select the rule and click the **Publish** button on the upper right-hand corner of the screen.

11 After publishing the Security Policy, users can Apply the Security Policy.

12 For an existing security policy, users can perform the following actions by selecting the check box of the policy:

- **Edit** - Allows to modify an existing policy rule.
- **Clone** - Allows to clone a policy from an existing one.
- **Delete** - Allows to delete a policy.

Configure Data Loss Prevention Rules

Describes in detail how to configure a Data Loss Prevention (DLP) rule for a selected Security Policy.

Before you begin

To configure a Security Policy, users must have first created a Security Policy. For specific instructions on how to create a Security Policy, see Create a Security Policy.

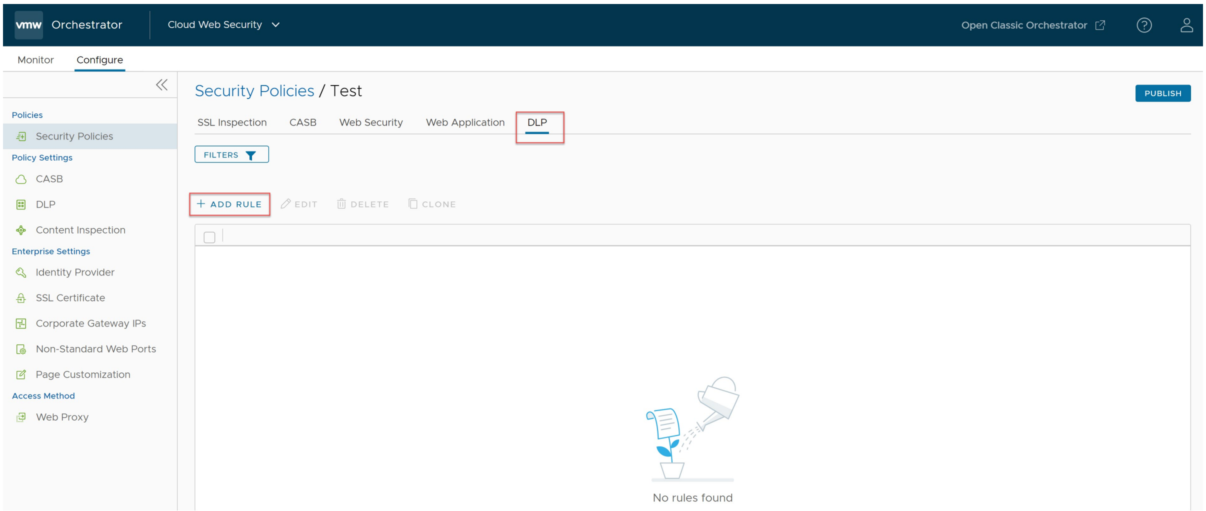
Configuration Steps

To configure a DLP rule, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Security Policies**.

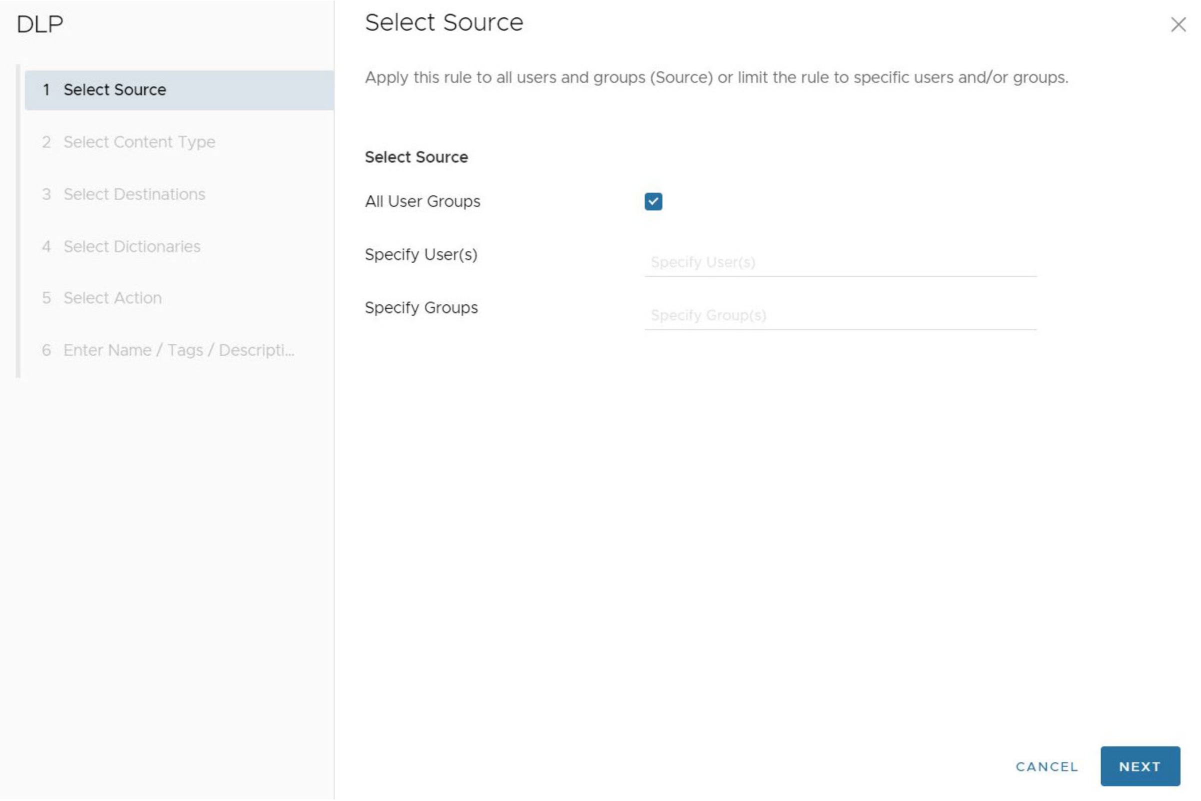
2 Select a security policy to configure DLP rule and then click the **DLP** tab.

3 In the **DLP** tab of the **Security Policies** screen, click **+ ADD RULE**.



The **Select Source** screen appears.

4 In the **Select Source** screen, select the **All Users Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups. By default, **All Users Groups** is selected for the Source.



Select Source

Apply this rule to all users and groups (Source) or limit the rule to specific users and/or groups.

Select Source

All User Groups ☑

Specify User(s): Specify User(s)

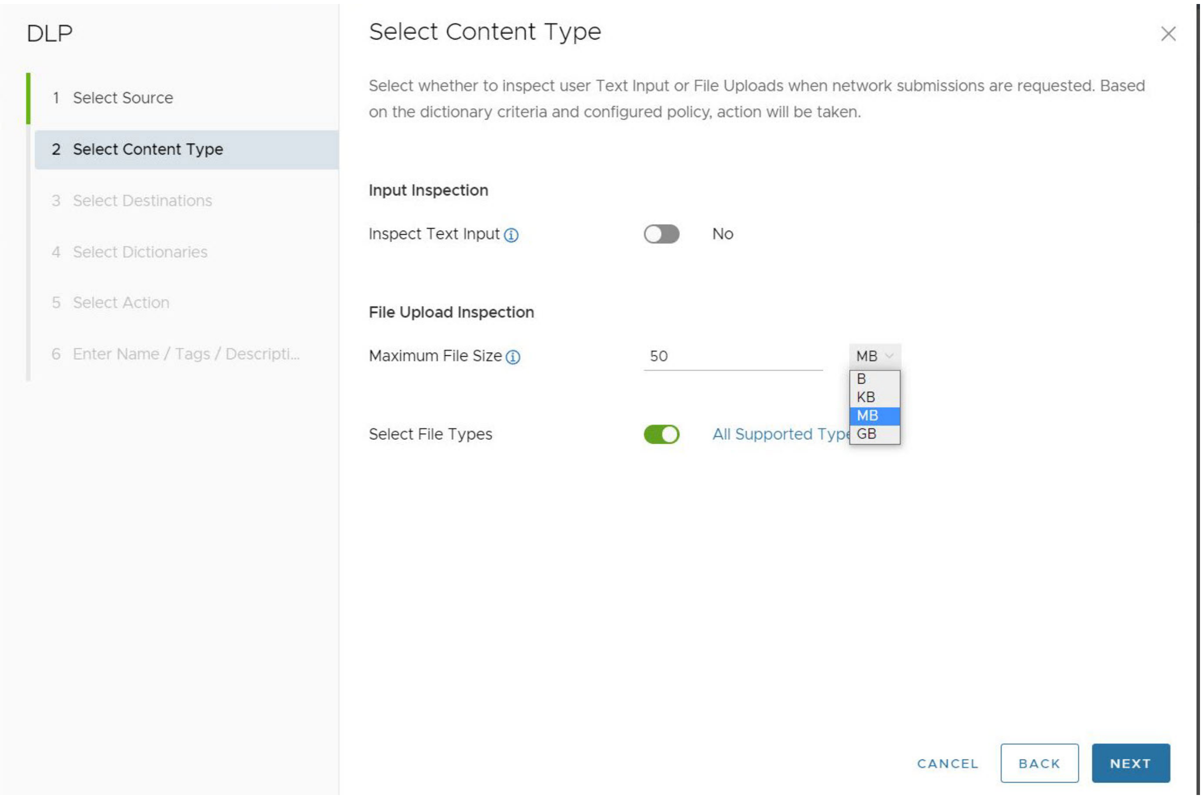
Specify Groups: Specify Group(s)

Note **All Users Groups** is the only option for customers that do not have an Identity Provider (IdP) like Workspace ONE or Azure Active Directory (AD) configured for Cloud Web Security.

Note Cloud Web Security must be configured with an Identity Provider (IdP) like Workspace ONE or Azure Active Directory (AD) for specific Users and Groups to work.

Click **Next**, the **Select Content Type** screen appears.

5 In the **Select Content Type** screen, users can configure the types of content that are triggered by the DLP inspection feature. There are three parameters that can be configured for content type:



DLP

1 Select Source

2 Select Content Type

3 Select Destinations

4 Select Dictionaries

5 Select Action

6 Enter Name / Tags / Descripti...

Select Content Type

Select whether to inspect user Text Input or File Uploads when network submissions are requested. Based on the dictionary criteria and configured policy, action will be taken.

Input Inspection

Inspect Text Input: No

File Upload Inspection

Maximum File Size: 50 MB

Select File Types: All Supported Types

a Choose whether the DLP rule should **Inspect Text Input** or not. The default for this option is **Off**. When toggled to **On**, user Text Input will pass through DLP inspection when network submissions are requested.

Note Text Input is like a form post or text message. Text Input is different from a Text File, which is an actual .txt attached to an upload.

b **Maximum File Size** allows users to choose whether to inspect file uploads by defining a maximum file size to be inspected. The default setting for this option is 50 Megabytes (MB), and users can configure a Maximum File Size value both numerically, and by units of storage: Byte **(B)**, Kilobyte **(KB)**, Megabyte **(MB)**, or Gigabyte **(GB)**. If the uploaded file size is greater than the configured **Maximum File Size** value, the file is not inspected by DLP and is allowed through.

Note The **Maximum File Size** numerical value can be configured as a number between 1 and 1000 on the Orchestrator. The number 0 is not valid for this field.

Important While it is possible to configure extremely small and large values, DLP has a maximum file size limit of 5 GB. Even if users configure a larger value, that value will not be honored beyond 5 GB. DLP also has minimum supported content sizes as follows:

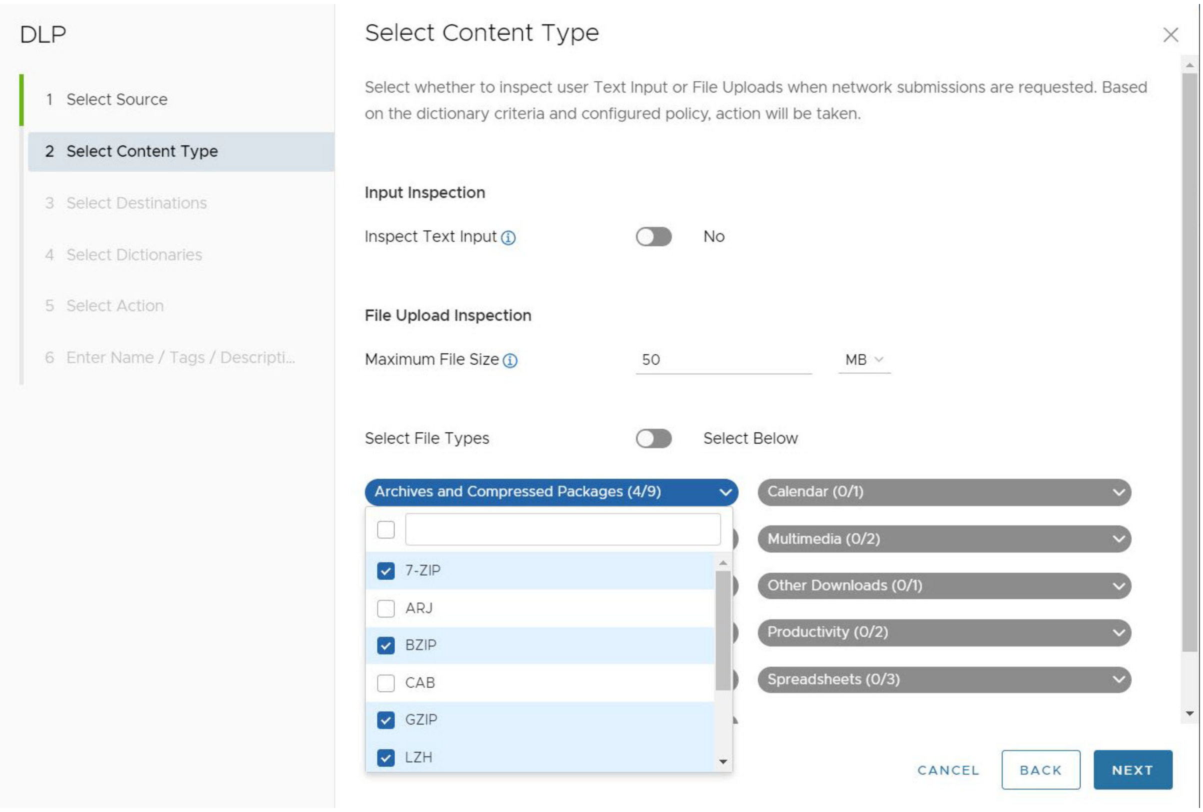
Table 1-3. Minimum Supported Content Sizes

User Input	File Input
1024 Bytes	5120 Bytes

c **Select File Types** allows user to choose specific file types to inspect. The default setting is to inspect **All Supported Types**, 36 file types in total. If users toggle off **All Supported File Types**, they will see a complete menu of all 36 file types sorted by 11 categories:

- **Archives and Compressed Packages (9)**: 7-Zip, ARJ, BZIP, CAB, GZIP, LZH, RAR, TAR, ZIP
- **Calendar (1)**: ICS Meeting Invitation
- **Engineering Applications (2)**: AutoCAD, Visio
- **Multimedia (2)**: Audio Files, Video Files
- **Miscellaneous Documents (1)**: RTF
- **Other Files and Documents (1)**: Other Files and Documents of unknown types
- **Presentation Tools (2)**: OpenOffice Presentation, PowerPoint
- **Productivity (2)**: Microsoft One Note, Microsoft Project
- **Scripts and Executables (6)**: Android Executable, JAR, Linux Executable, Mac Executable, Text-based script files
- **Spreadsheets (3)**: CSV, Excel, OpenOffice Spreadsheet
- **Word Processors (7)**: Hangul, Ichitaro, OpenOffice Text, PDF, Word, Word Perfect, XPS

Users can select several, or all the **File Types** under a file category. If the number of **File Types** selected is less than all the **File Types** available for that category, the file category name will show as blue and display how many **File Types** are selected out of the total available.



Select Content Type

Select whether to inspect user Text Input or File Uploads when network submissions are requested. Based on the dictionary criteria and configured policy, action will be taken.

Input Inspection

Inspect Text Input: No

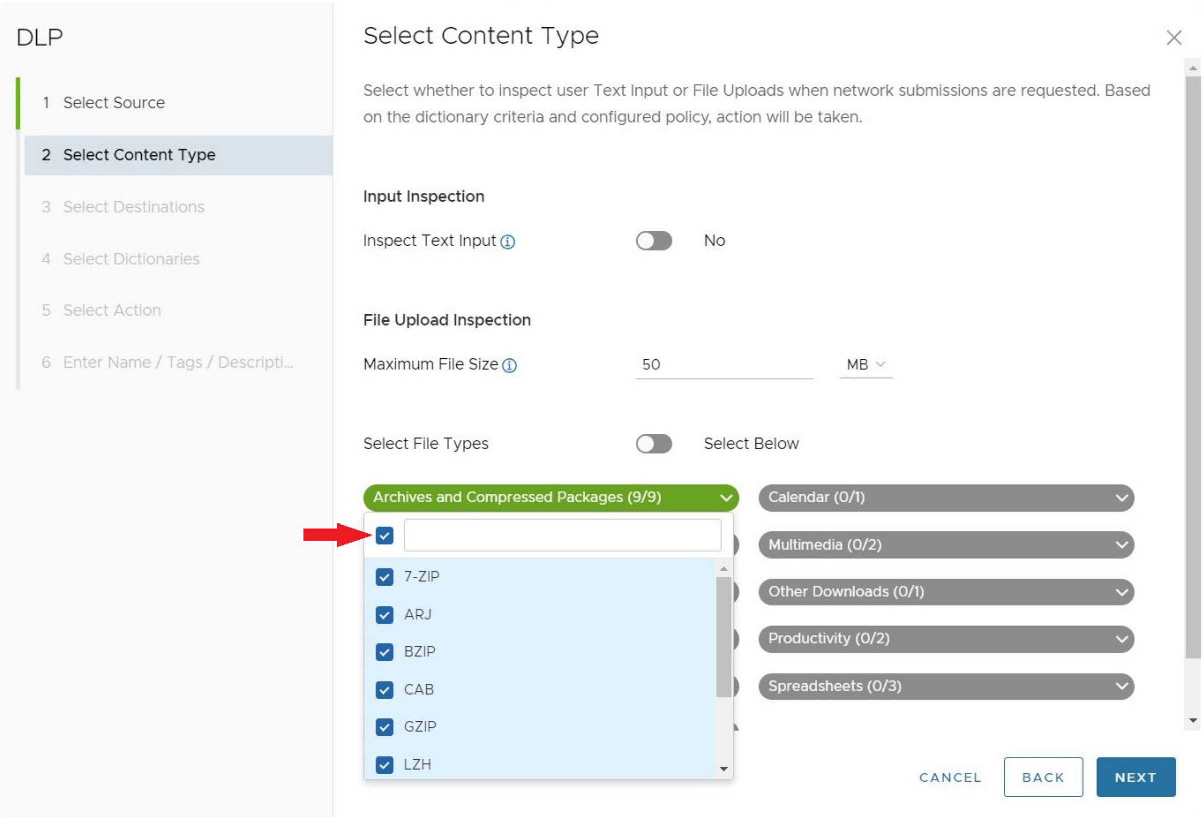
File Upload Inspection

Maximum File Size: 50 MB

Select File Types: Select Below

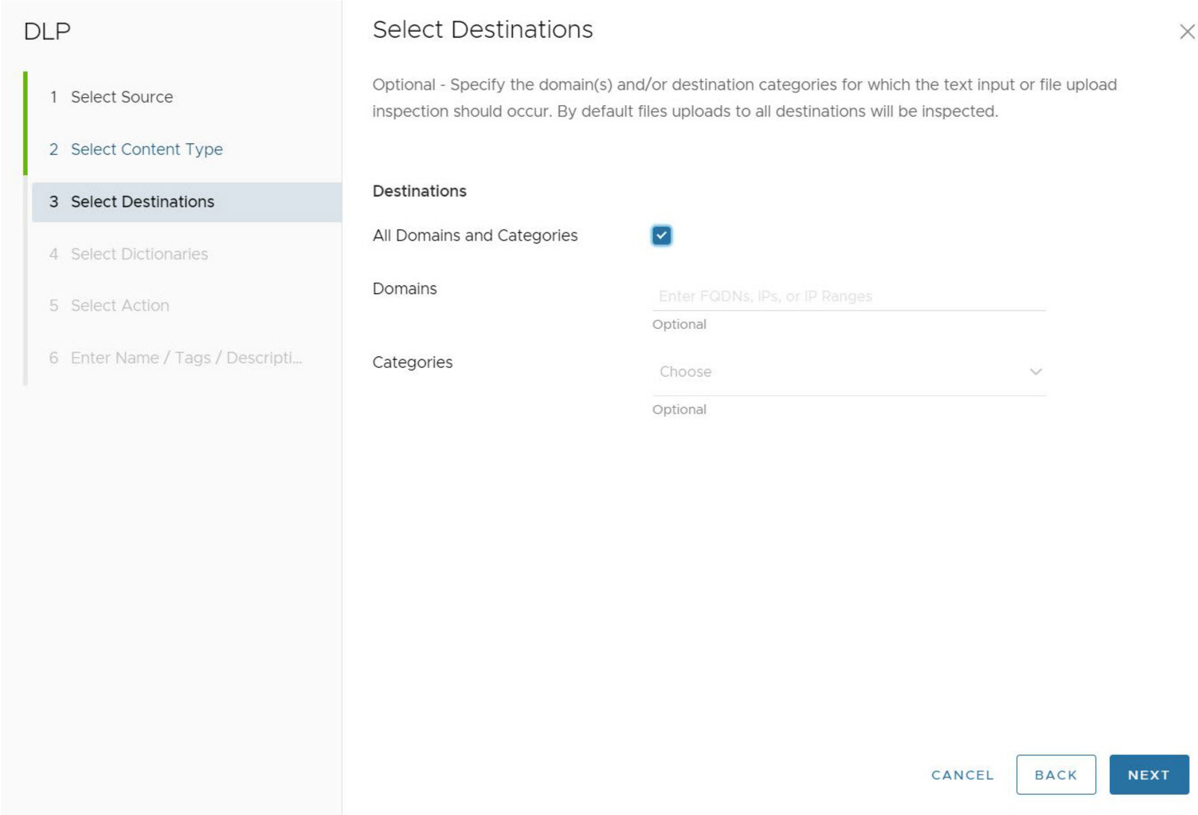
Archives and Compressed Packages (4/9)
- ☐
- ☑ 7-ZIP
- ☐ ARJ
- ☑ BZIP
- ☐ CAB
- ☑ GZIP
- ☑ LZH

If users wish to select all the **File Types** for that category, they can click on the top selection box and all the **File Types** are selected. When this is done, the category header becomes green and shows all **File Types** have been selected for that category.



After selecting the DLP Content types settings for the rule, click **Next**. The **Select Destinations** screen appears.

6 In the **Select Destinations** screen, users can specify the domains and/or categories for which DLP inspection should take place. The default setting is **All Domains and Categories**, which means that DLP inspects all **Domains** and all 84 **Categories**.



Select Destinations

Optional - Specify the domain(s) and/or destination categories for which the text input or file upload inspection should occur. By default files uploads to all destinations will be inspected.

Destinations

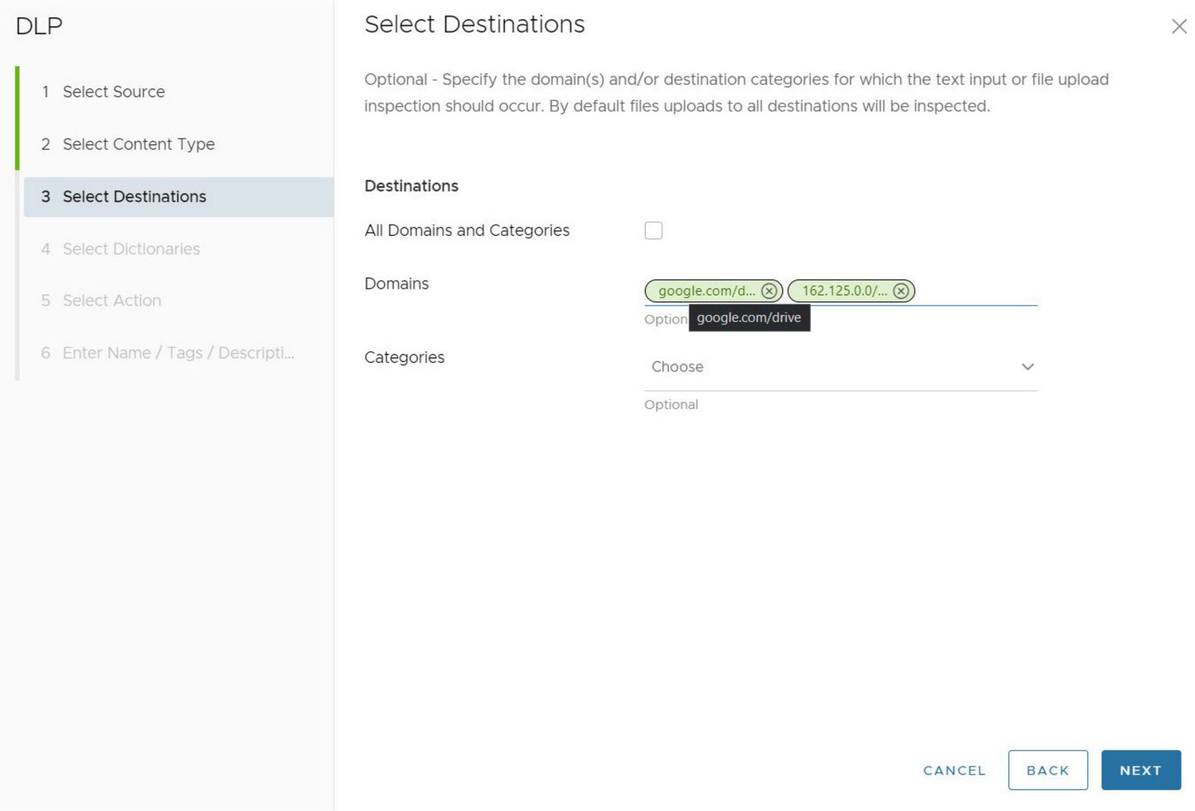
All Domains and Categories ☑

Domains: Enter FQDNs, IPs, or IP Ranges (Optional)

Categories: Choose (Optional)

If users uncheck the box for **All Domains and Categories**, users are required to configure customized **Domains** and/or **Categories**.

For the **Domains** field, users can specify Fully Qualified Domain Names (FQDN), IP Addresses, or IP Ranges that would trigger an Auditor Alert. Users can enter a combination of FQDNs, IP Addresses, and IP Ranges.



DLP

1 Select Source
2 Select Content Type
3 Select Destinations
4 Select Dictionaries
5 Select Action
6 Enter Name / Tags / Descripti...

Select Destinations

Optional - Specify the domain(s) and/or destination categories for which the text input or file upload inspection should occur. By default files uploads to all destinations will be inspected.

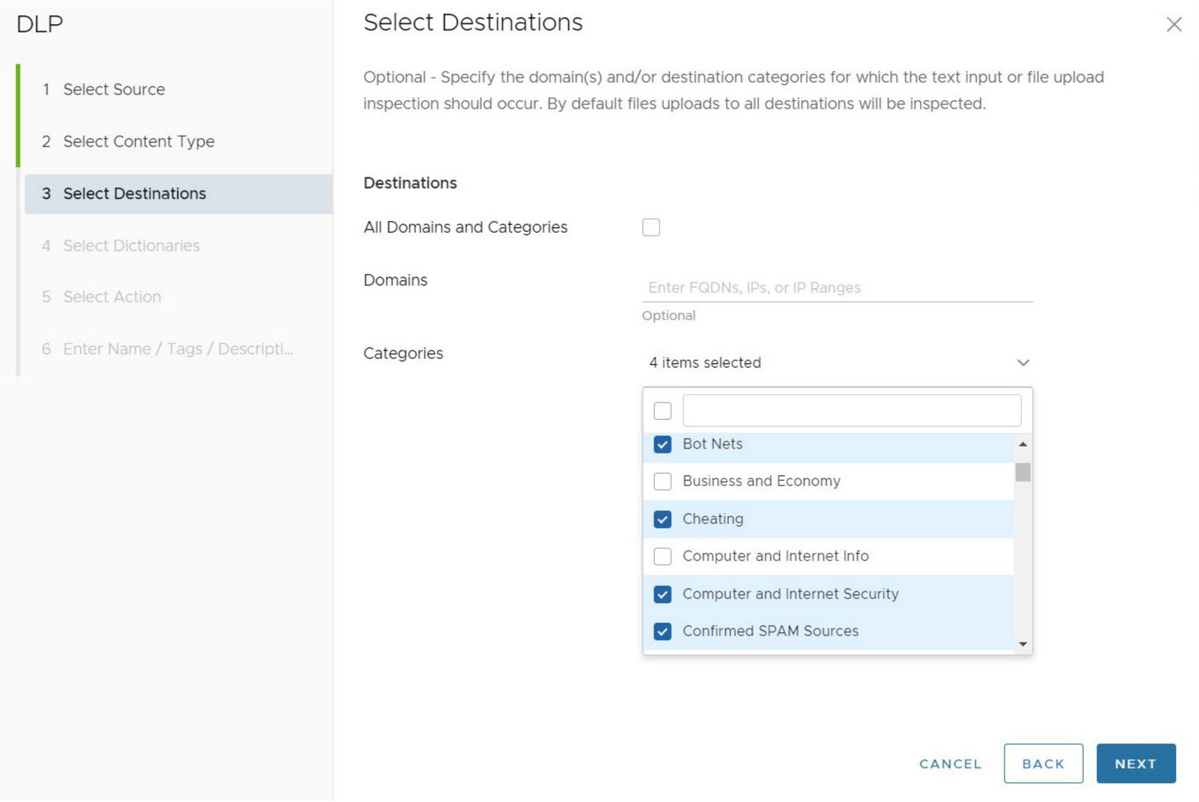
Destinations

All Domains and Categories ☐

Domains: google.com/d... ⊗ 162.125.0.0/... ⊗ (google.com/drive)

Categories: Choose (Optional)

In the **Categories** field, users can choose from up to 84 distinct categories for which a file can match and require a DLP inspection. Users can also select all categories at once by clicking the top left check box.



Select Destinations

Optional - Specify the domain(s) and/or destination categories for which the text input or file upload inspection should occur. By default files uploads to all destinations will be inspected.

Destinations

All Domains and Categories ☐

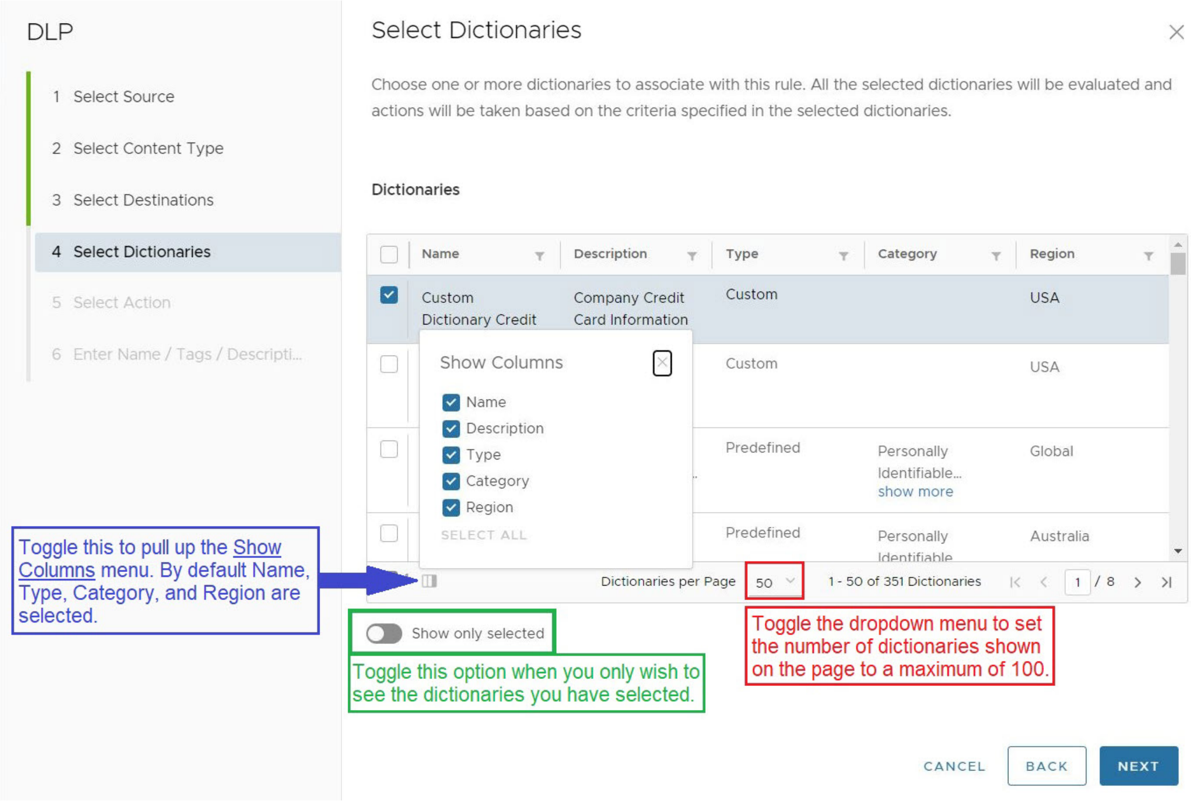
Domains: Enter FQDNs, IPs, or IP Ranges (Optional)

Categories: 4 items selected

☐
☑ Bot Nets
☐ Business and Economy
☑ Cheating
☐ Computer and Internet Info
☑ Computer and Internet Security
☑ Confirmed SPAM Sources

After selecting the DLP destination for the rule, click **Next**. The **Select Dictionaries** screen appears.

7 In the **Select Dictionaries** section, users must choose at least one or more Dictionaries to associate with the rule. The Dictionaries can be Custom, Predefined, or a combination of Custom and Predefined. All selected Dictionaries are evaluated, and action is taken based on the criteria specified in the respective dictionaries.



Select Dictionaries

Choose one or more dictionaries to associate with this rule. All the selected dictionaries will be evaluated and actions will be taken based on the criteria specified in the selected dictionaries.

Dictionaries

☐	Name	Description	Type	Category	Region
☑	Custom Dictionary Credit	Company Credit Card Information	Custom		USA
☐			Custom		USA
☐			Predefined	Personally Identifiable... show more	Global
☐			Predefined	Personally Identifiable	Australia

Show Columns
- ☑ Name
- ☑ Description
- ☑ Type
- ☑ Category
- ☑ Region

Dictionaries per Page 50 | 1 - 50 of 351 Dictionaries | 1 / 8

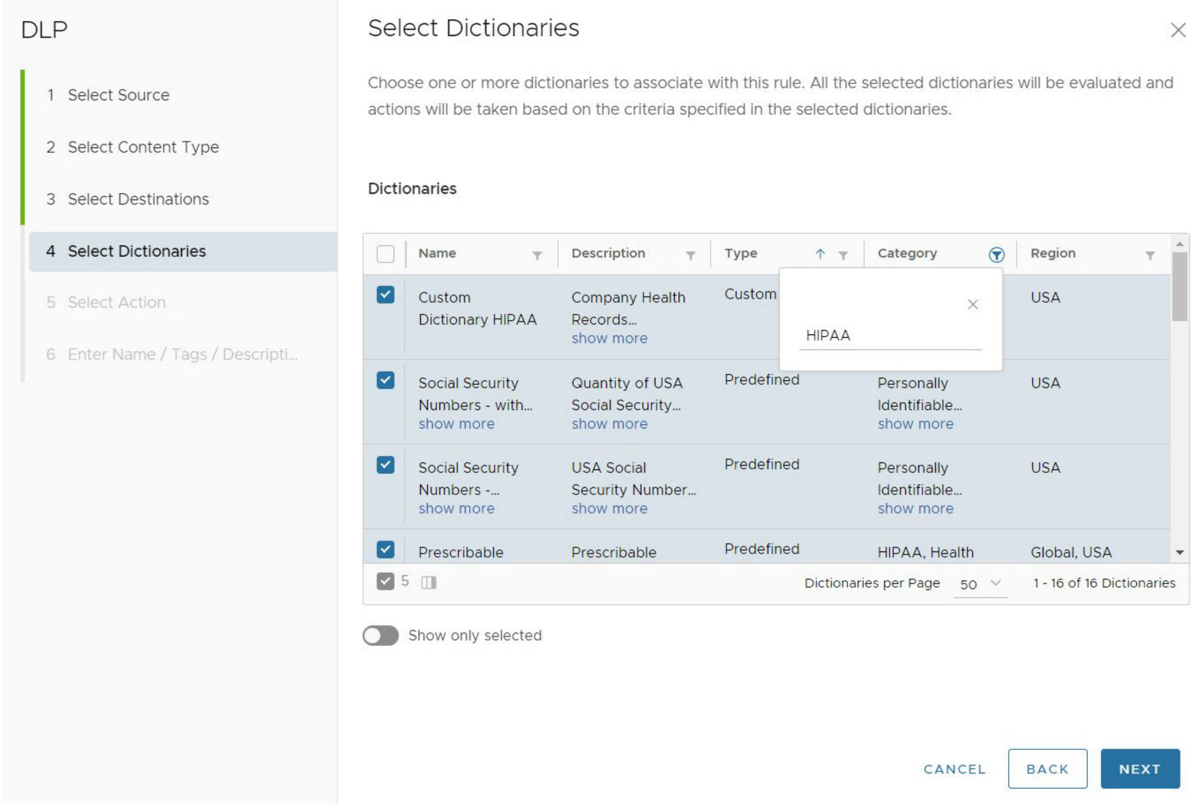
Show only selected

Toggle this to pull up the Show Columns menu. By default Name, Type, Category, and Region are selected.

Toggle this option when you only wish to see the dictionaries you have selected.

Toggle the dropdown menu to set the number of dictionaries shown on the page to a maximum of 100.

There are more than 340 Predefined Dictionaries to choose from in addition to the Custom Dictionaries user may create, users should narrow their Dictionary options using one or more filters located at the top of each column. In this example, the user is filtering for dictionaries that match the Category term "HIPAA" to link up with the Custom Dictionary they already created.



DLP

1 Select Source

2 Select Content Type

3 Select Destinations

4 Select Dictionaries

5 Select Action

6 Enter Name / Tags / Descripti...

Select Dictionaries

Choose one or more dictionaries to associate with this rule. All the selected dictionaries will be evaluated and actions will be taken based on the criteria specified in the selected dictionaries.

Dictionaries

☐	Name	Description	Type	Category	Region
☑	Custom Dictionary HIPAA	Company Health Records... show more	Custom		USA
☑	Social Security Numbers - with... show more	Quantity of USA Social Security... show more	Predefined	Personally Identifiable... show more	USA
☑	Social Security Numbers -... show more	USA Social Security Number... show more	Predefined	Personally Identifiable... show more	USA
☑	Prescribable	Prescribable	Predefined	HIPAA, Health	Global, USA

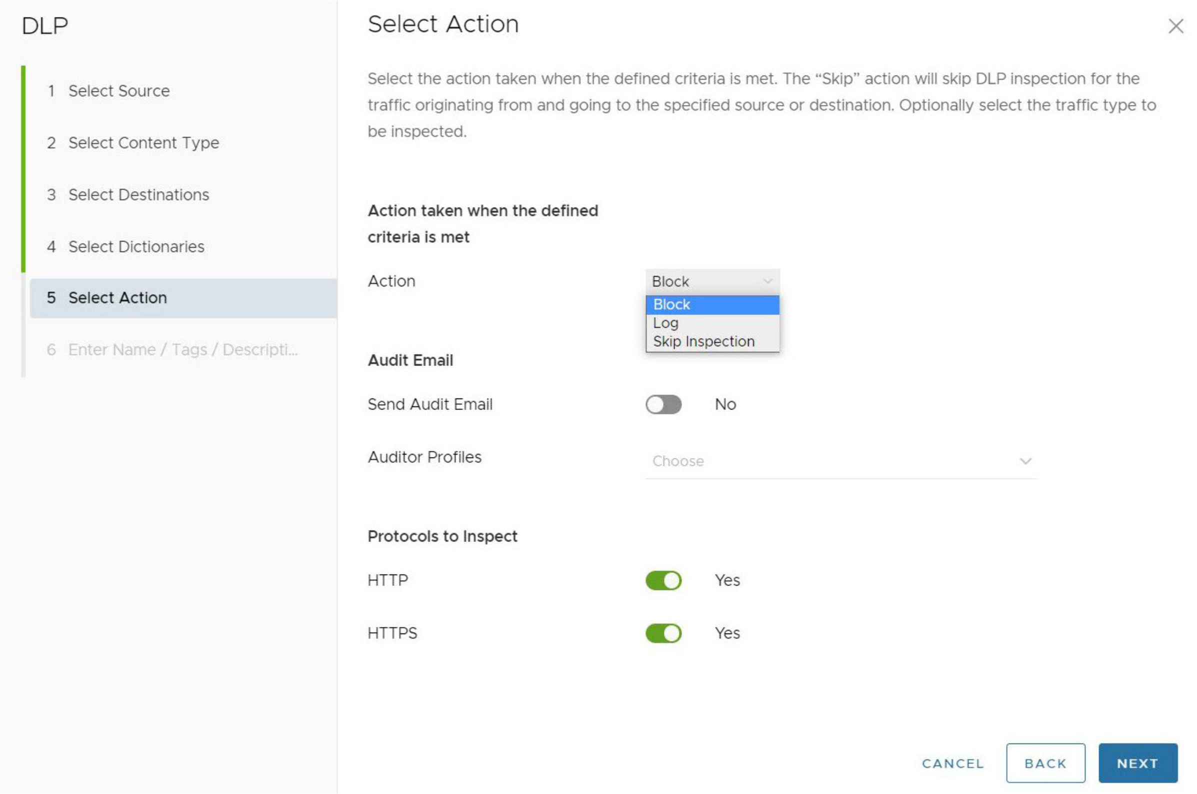
Category filter: HIPAA

☑ 5 Dictionaries per Page 50 1 - 16 of 16 Dictionaries

Show only selected

After selecting the DLP Dictionaries to apply to the rule, click **Next**. The **Select Action** screen appears.

8 In the **Select Action** screen, user can decide what action is taken when the defined criteria are met. The action can be set to **Block**, **Log**, or **Skip Inspection**. The default settings for **Select Action** are **Block**, with no **Audit Email** sent and both **HTTP** and **HTTPS** toggled on as **Protocols to Inspect**.



Select the action taken when the defined criteria is met. The "Skip" action will skip DLP inspection for the traffic originating from and going to the specified source or destination. Optionally select the traffic type to be inspected.

Action taken when the defined criteria is met

Action: Block

Audit Email

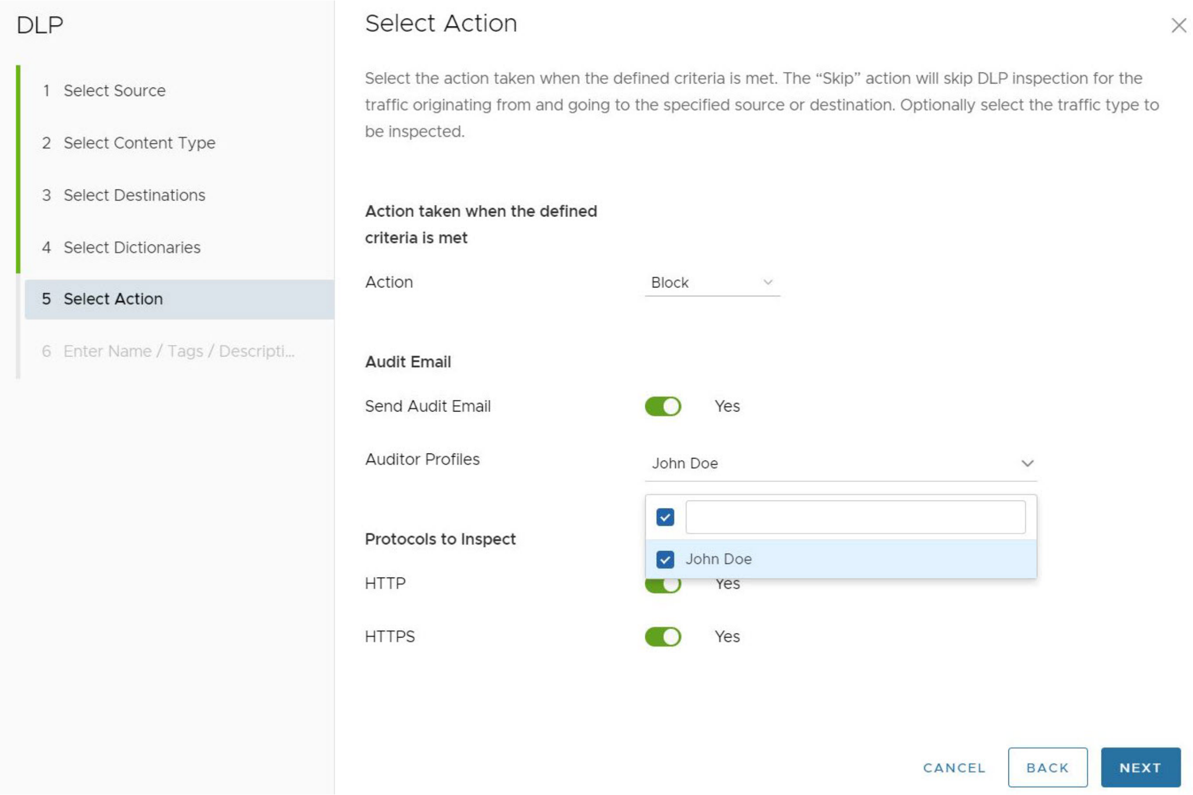
Send Audit Email: No

Protocols to Inspect

HTTP: Yes

HTTPS: Yes

If users toggle the **Send Audit Email** to **Yes**, users will also need to select an **Auditor Profile(s)** who will receive the Audit Email. In this case, the user chooses the Auditor Profile configured earlier in the **Auditors** section.



Select Action

Select the action taken when the defined criteria is met. The “Skip” action will skip DLP inspection for the traffic originating from and going to the specified source or destination. Optionally select the traffic type to be inspected.

Action taken when the defined criteria is met

Action: Block

Audit Email

Send Audit Email: Yes

Auditor Profiles: John Doe

☑ John Doe

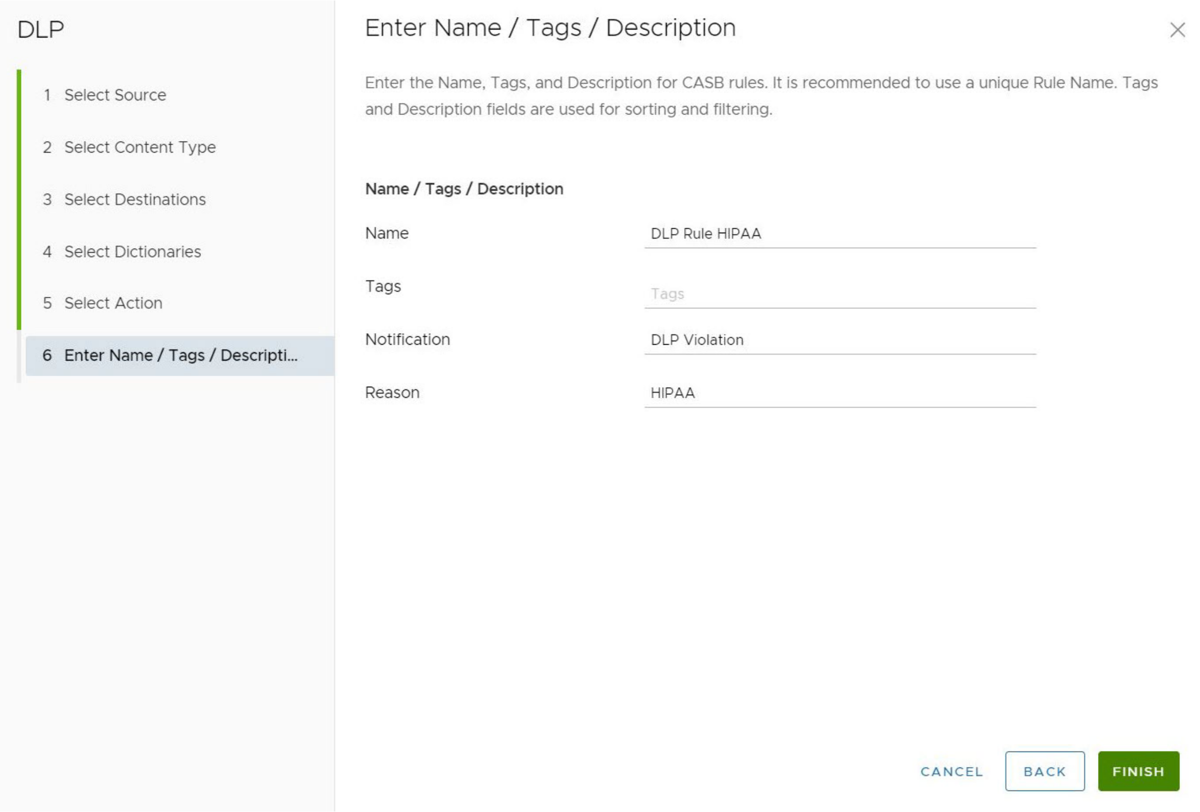
Protocols to Inspect

HTTP: Yes

HTTPS: Yes

After configuring the Action to be taken for the rule, click **Next**.

9 In the **Enter Name /Tags / Description** screen, user must configure a unique **Name** for the DLP Rule. User can also configure **Tags**, **Notification**, and **Reason** for the rule.



Enter Name / Tags / Description

Enter the Name, Tags, and Description for CASB rules. It is recommended to use a unique Rule Name. Tags and Description fields are used for sorting and filtering.

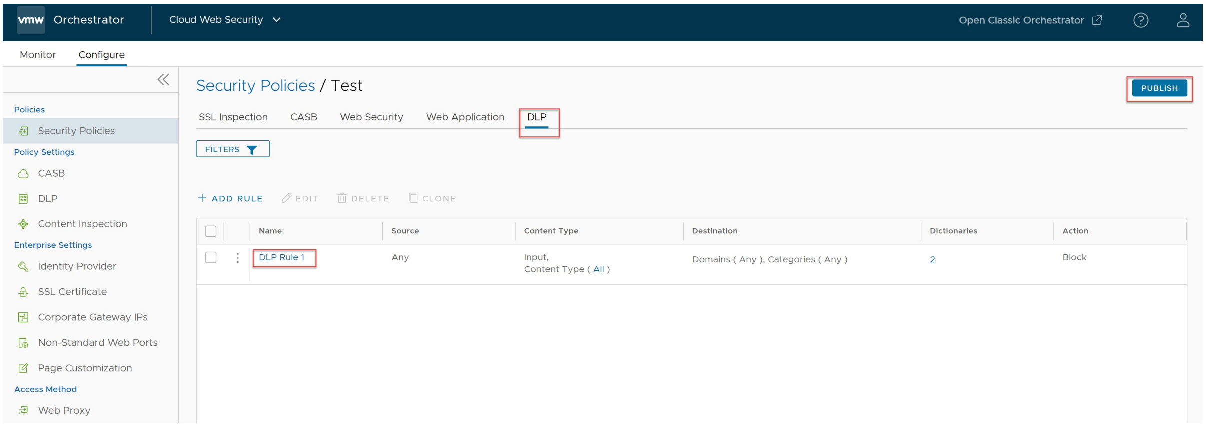
Name / Tags / Description

Name	DLP Rule HIPAA
Tags	Tags
Notification	DLP Violation
Reason	HIPAA

10 Click **Finish**. A DLP rule is created and gets listed on the DLP rule section for the Security Policy.

11 Click **Publish** for the DLP Rule to take effect in this Security Policy.

> **Note** It takes about five minutes for the DLP Rule to take effect from the time users publish it. After publishing the Security Policy, users can Applying a Security Policy.



Security Policies / Test

☐	Name	Source	Content Type	Destination	Dictionaries	Action
☐	DLP Rule 1	Any	Input, Content Type (All)	Domains (Any), Categories (Any)	2	Block

After publishing, a DLP Rule can be edited and republished as needed in the same way that it was first created.

For more information about DLP Enterprise settings, see Chapter 3 Data Loss Prevention.

Cloud Web Security Policy and Rule Limits

This section lists the rule limits for Cloud Web Security policies.

Table 1-4. Default Policy and Rule Limits for Security Policies Created

Feature	Parameter Name	Default Limit	Notes
SSL Exception	Maximum SSL Exception Rules	3000	The maximum number of SSL exceptio
Web Application	Maximum Web Application Rules	4000	Maximum number of Application rules (
Web Proxy	Maximum Number of PAC Files	100	Maximum number of PAC files per tena
Web Security	Maximum Web Security Rules	3000	The maximum number of web exceptio Threats, Content Filters, Content Inspec
Web Security	Maximum Domains per Rule	1000	Maximum number of domains per excep
Web Security	Maximum Users per Rule	1000	Maximum number of users in an excepti
Web Security	Maximum Groups per Rule	250	Maximum number of group entries in a

Applying a Security Policy

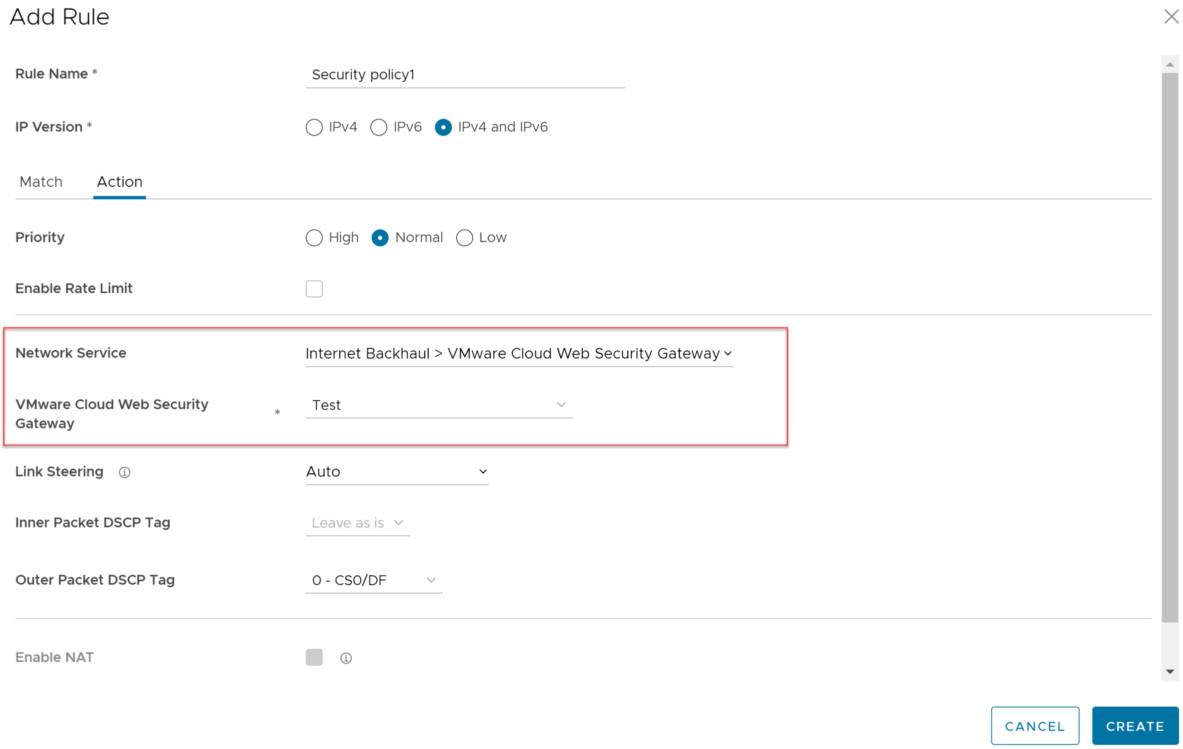
After configuring and publishing a Security Policy, users can then apply the Security Policy to a Profile or an Edge through the use of a Business Policy. Business Policies may be configured at either the Profile or Edge level.

To create a Business Policy rule at the Profile level and apply a Security Policy, follow the steps below:

Procedure

1. From the SD-WAN Orchestrator Enterprise portal, go to **Configure** > **Profiles**. The **Profiles** page displays the existing Profiles.
2. Click the link to a Profile.
3. Click the **Business Policy** tab. From the **Profiles** page, users can navigate to the **Business Policy** page directly by clicking the **View** link in the **Biz. Pol** column of the Profile.

4 Under the **Configure Business Policy** area, click **+ADD**. The **Add Rule** dialog box appears.



Add Rule

Rule Name * Security policy1

IP Version * ○ IPv4 ○ IPv6 ● IPv4 and IPv6

Match Action

Priority ○ High ● Normal ○ Low

Enable Rate Limit ☐

Network Service Internet Backhaul > VMware Cloud Web Security Gateway

VMware Cloud Web Security Gateway * Test

Link Steering Auto

Inner Packet DSCP Tag Leave as is

Outer Packet DSCP Tag 0 - CS0/DF

Enable NAT ☐

5 In the **Rule Name** box, enter a unique name for the rule.

6 Under the **Match** area, configure the match conditions for the traffic flow by defining the matching criteria for the **Source** and **Destination** traffic.

7 Under the **Action** area, configure the actions for the rule as follows:

- Set the **Network Service** to **Internet Backhaul**.
- Click the **VMware Cloud Web Security Gateway** network service and select a published Security Policy to be applied to the Business policy rule.

8 Click **Create**. The selected Security Policy is applied for the selected profile, and it appears under the **Business Policy Rules** area of the Profile Business Policy page.

For more information about Business policies, see the *Configure Business Policy Rule* section in the *VMware SD-WAN Administration Guide* published at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

What to do next

- Chapter 11 Monitor Cloud Web Security

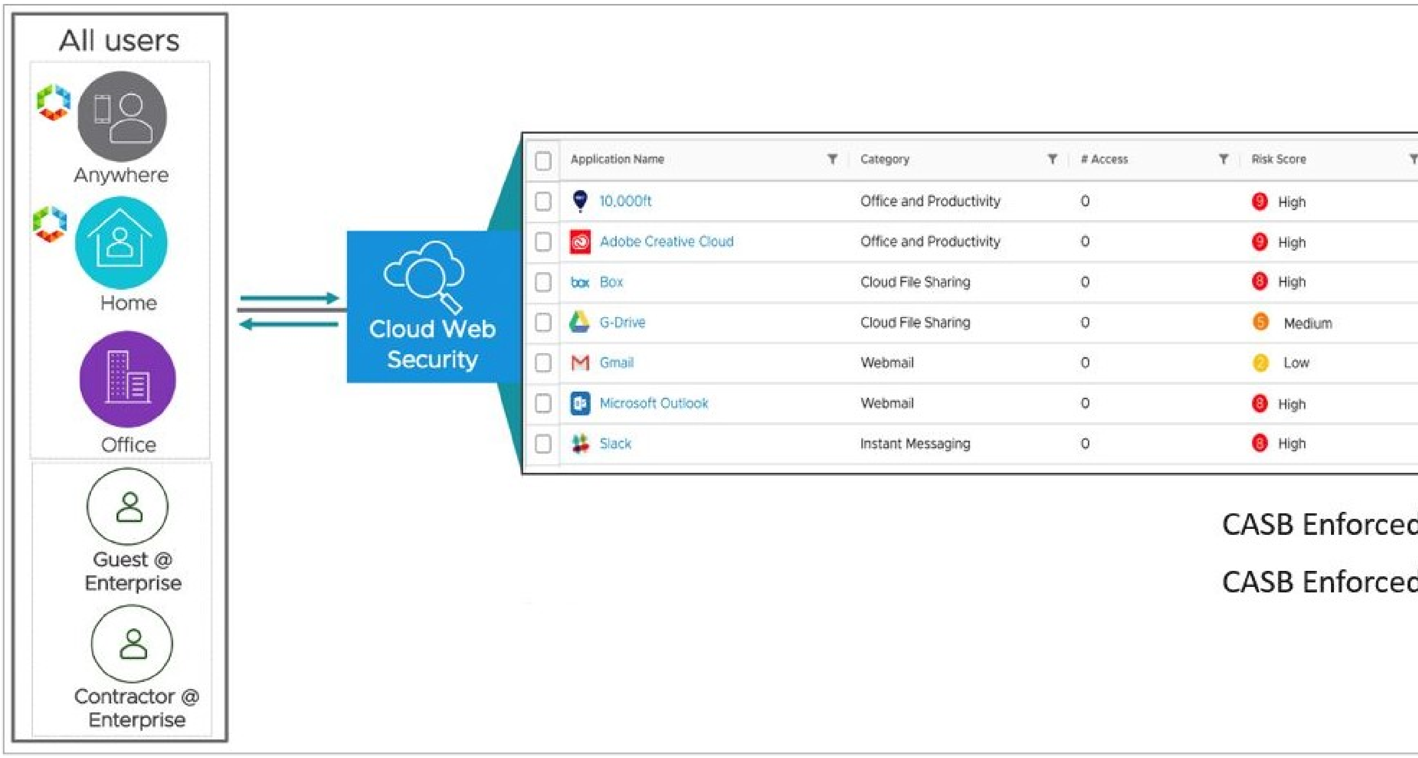
Cloud Access Security Broker

2

This section covers how to use the Cloud Access Security Broker (CASB) feature for the Cloud Web Security service.

Overview

The Cloud Access Security Broker (CASB) feature provides visibility and control on user activities while accessing SaaS applications.



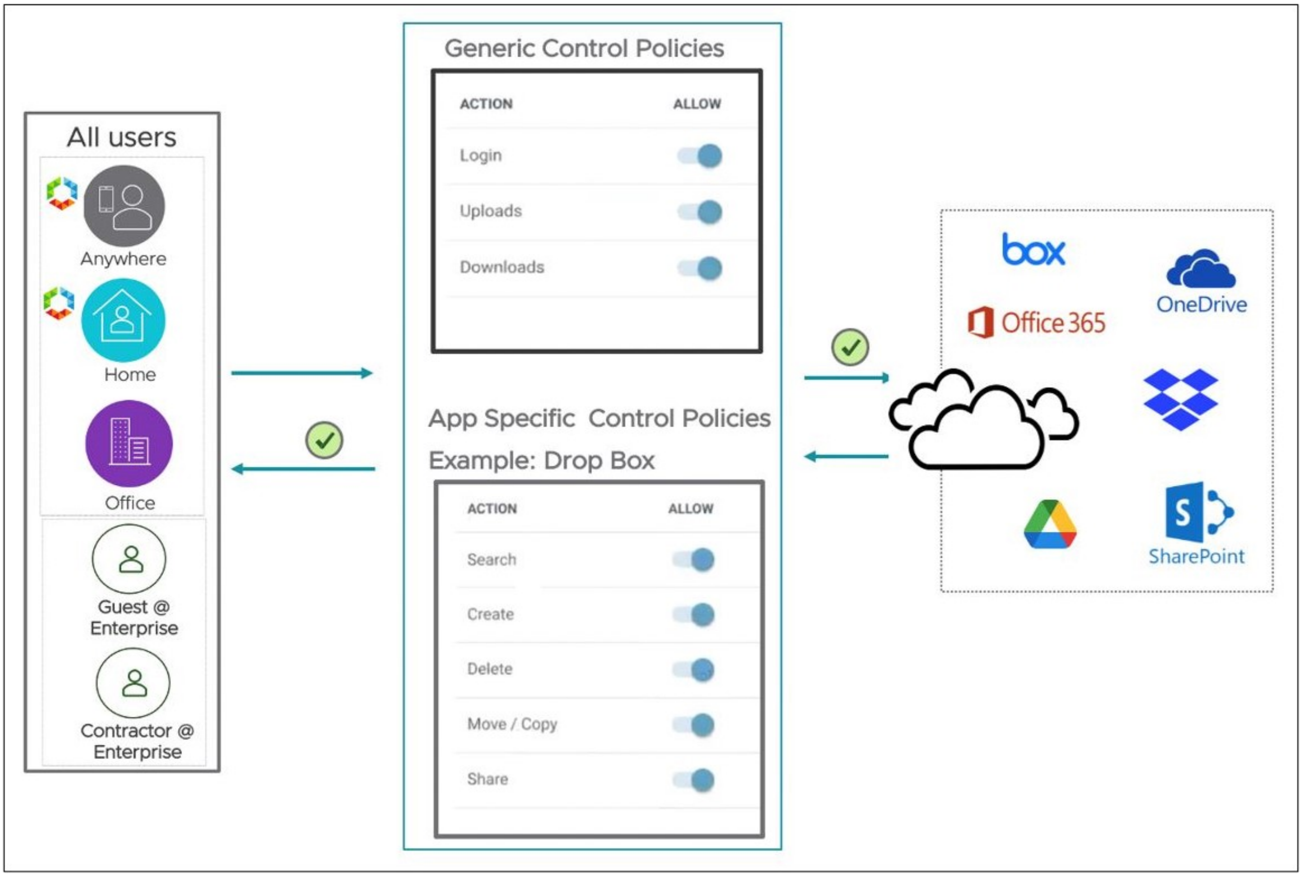
☐	Application Name	Category	# Access	Risk Score
☐	10,000ft	Office and Productivity	0	9 High
☐	Adobe Creative Cloud	Office and Productivity	0	9 High
☐	Box	Cloud File Sharing	0	8 High
☐	G-Drive	Cloud File Sharing	0	5 Medium
☐	Gmail	Webmail	0	2 Low
☐	Microsoft Outlook	Webmail	0	8 High
☐	Slack	Instant Messaging	0	8 High

The CASB feature includes the following capabilities:

Application Visibility (part of both Cloud Web Security Standard and Advanced Edition packages): A customer has the ability to view the different SaaS applications being accessed by users within their network. For each application, a customer using CASB Application Visibility can observe:

- The risk score for each application.
- The number of times users have accessed an application.
- The application's category.

Application Control (part of the Cloud Web Security Advanced Edition package only): A customer has the ability to control specific actions that can be performed on each SaaS application.



Out-of-the-box predefined controls are available for all SaaS applications with application specific controls provided at a per-application level. These controls can be customized and configured per application and based on User and User Group.

For each application, a customer using CASB Application Control can control:

- Initial access to the application site (Allow or Block).
- Additional actions including Login, Upload/Download Content, Search, Edit, Share, Create, Delete, Like, or Post.

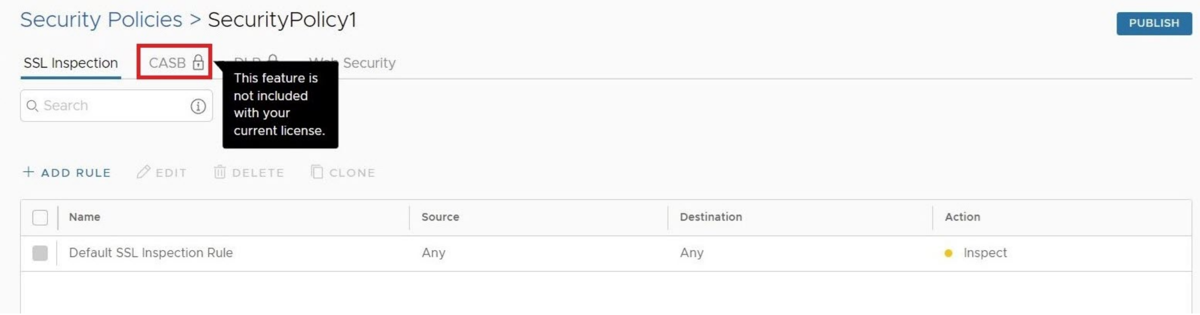
Customers can see the currently available actions for the applications they would like to control.

Prerequisites

Users need the following for access to the Cloud Access Security Broker (CASB) feature with Cloud Web Security:

1. A customer Enterprise on a production VMware Cloud Orchestrator with Cloud Web Security activated.
2. The customer's SD-WAN Edges, the SASE PoPs, and the Orchestrator must all use Release 4.5.0 or later.
3. CASB Application Visibility is useable for all Cloud Web Security customers whether they have a Standard or Advanced package.
4. To access CASB Application Control, a customer must have a Cloud Web Security Advanced package.

   If users navigate to **Cloud Web Security > Configure > Security Policies** and clicks on an existing Policy or create a new Policy, the CASB tab will include a lock icon. This indicates that only CASB Visibility is allowed with the Standard Edition license and that to create CASB Control policies, the Advanced Edition license is required.

   This feature is not included with your current license.

☐	Name	Source	Destination	Action
☐	Default SSL Inspection Rule	Any	Any	● Inspect

5. Optional: An Identity Provider (IdP) if the customer plans to have user-based rules. For more information on configuring either Workspace ONE or Azure Active Directory (AD) as an identity provider, consult the respective guides on the Chapter 4 Single Sign-On page.

CASB Configuration Workflow

Having covered the two key capabilities **Application Visibility** and **Application Control** that comprise the CASB feature, this section will cover the CASB workflow.

Create, Configure, and Apply a Security Policy

For details on Create a Security Policy, Configuring a Security Policy, or Applying a Security Policy a **Security Policy** for the Cloud Web Security service, consult the relevant documentation in the *Cloud Web Security Configuration Guide*.

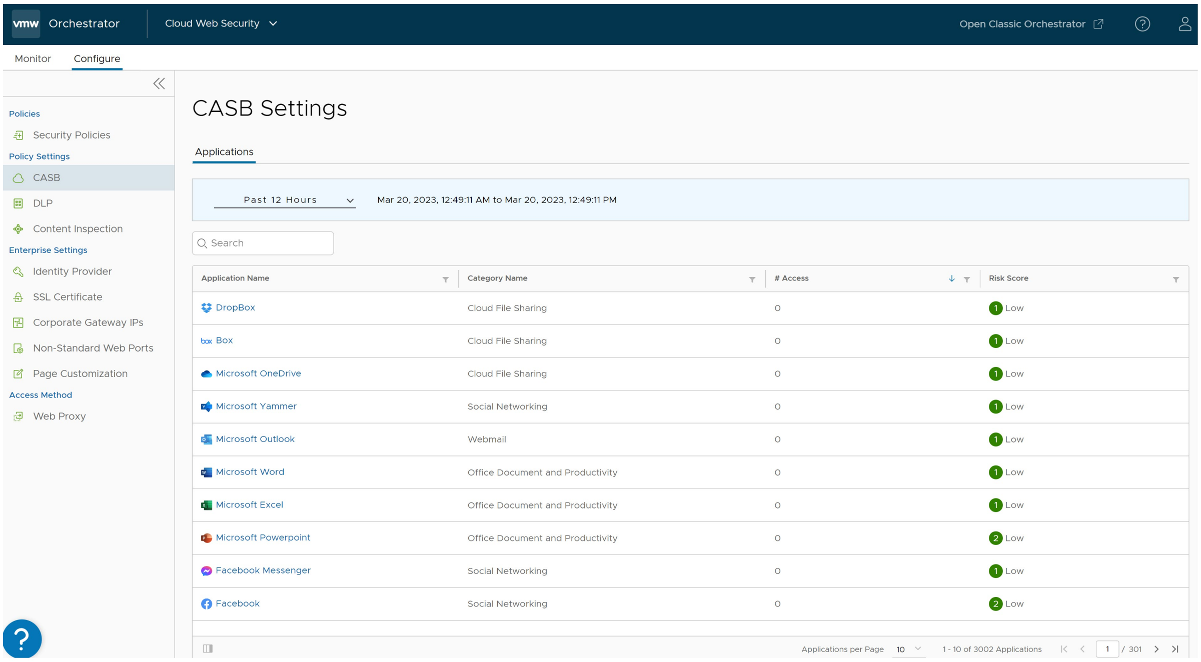
CASB Settings - Application Visibility

After a Security Policy has been associated to a customer segment, traffic from endpoint devices behind the SD-WAN Edge or coming via Secure Access clients are being inspected and monitored if it passes through the Cloud Web Security policy.

1 On the VMware SASE Orchestrator UI, navigate to **Cloud Web Security** > **Configure** > **Policy Settings** > **CASB**.

2 The **CASB Settings** page provides a list of Applications which match a Security Policy Rule and are sorted by default for the highest Number of Access (the number of times a particular application has been accessed within the specified time period).

   - Each Application will also have a Risk Score associated with it: Low (1-3), Medium (4-6), or High (7-9).
   - The **Applications** table can be sorted by Application Name, Category Name, # of times Accessed, or Risk Score by clicking on the column header. Or by clicking the sort icon for a column, users can search for a particular term or number in that column.
   - The CASB Settings page by default displays 20 Applications per Page, users can scroll to the bottom of the page and specify up to 100 Applications per Page. Users can also select a new page of Applications either by clicking one the arrow icons or specifying a specific page in the text box.



CASB Settings

Applications

Past 12 Hours   Mar 20, 2023, 12:49:11 AM to Mar 20, 2023, 12:49:11 PM

Search

Application Name	Category Name	# Access	Risk Score
DropBox	Cloud File Sharing	0	1 Low
Box	Cloud File Sharing	0	1 Low
Microsoft OneDrive	Cloud File Sharing	0	1 Low
Microsoft Yammer	Social Networking	0	1 Low
Microsoft Outlook	Webmail	0	1 Low
Microsoft Word	Office Document and Productivity	0	1 Low
Microsoft Excel	Office Document and Productivity	0	1 Low
Microsoft Powerpoint	Office Document and Productivity	0	2 Low
Facebook Messenger	Social Networking	0	1 Low
Facebook	Social Networking	0	2 Low

Applications per Page 10   1 - 10 of 3002 Applications   1 / 301

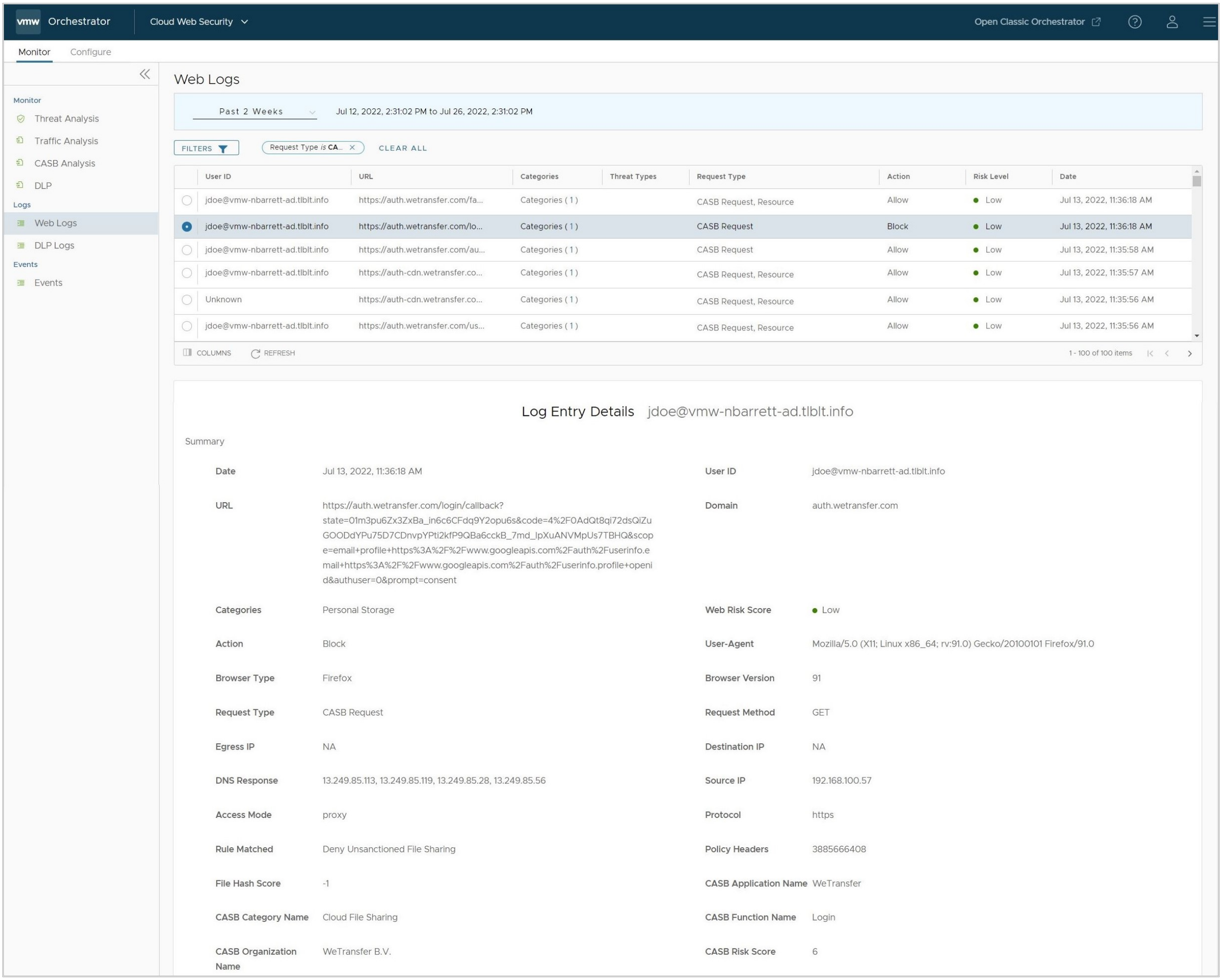
   - As more traffic passes through the Cloud Web Security service, the Applications list may change depending on which websites are being visited. These changes can include application order, number of applications, access events, and risk score.

Create and Apply a CASB Control Rule

To create and apply a CASB Control Rule, see Configure Cloud Access Security Broker Rules.

Verify a CASB Rule is Working

After the Security Policy with the CASB Control Rule is published, go to a website affected by the rule and test the control features to confirm it is working as expected. To verify that the applications have CASB controls configured, use the **Cloud Web Security > Monitor > Web Logs** page. For example, in an instance where users tried to log into the WeTransfer website and was blocked as per the published CASB Control rule. The Web logs show the blocked login attempt.



Jul 12, 2022, 2:31:02 PM to Jul 26, 2022, 2:31:02 PM

	User ID	URL	Categories	Threat Types	Request Type	Action	Risk Level	Date
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/fa...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:36:18 AM
●	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/lo...	Categories (1)		CASB Request	Block	● Low	Jul 13, 2022, 11:36:18 AM
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/au...	Categories (1)		CASB Request	Allow	● Low	Jul 13, 2022, 11:35:58 AM
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth-cdn.wetransfer.co...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:35:57 AM
○	Unknown	https://auth-cdn.wetransfer.co...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:35:56 AM
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/us...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:35:56 AM

Log Entry Details jdoe@vmw-nbarrett-ad.tlblt.info

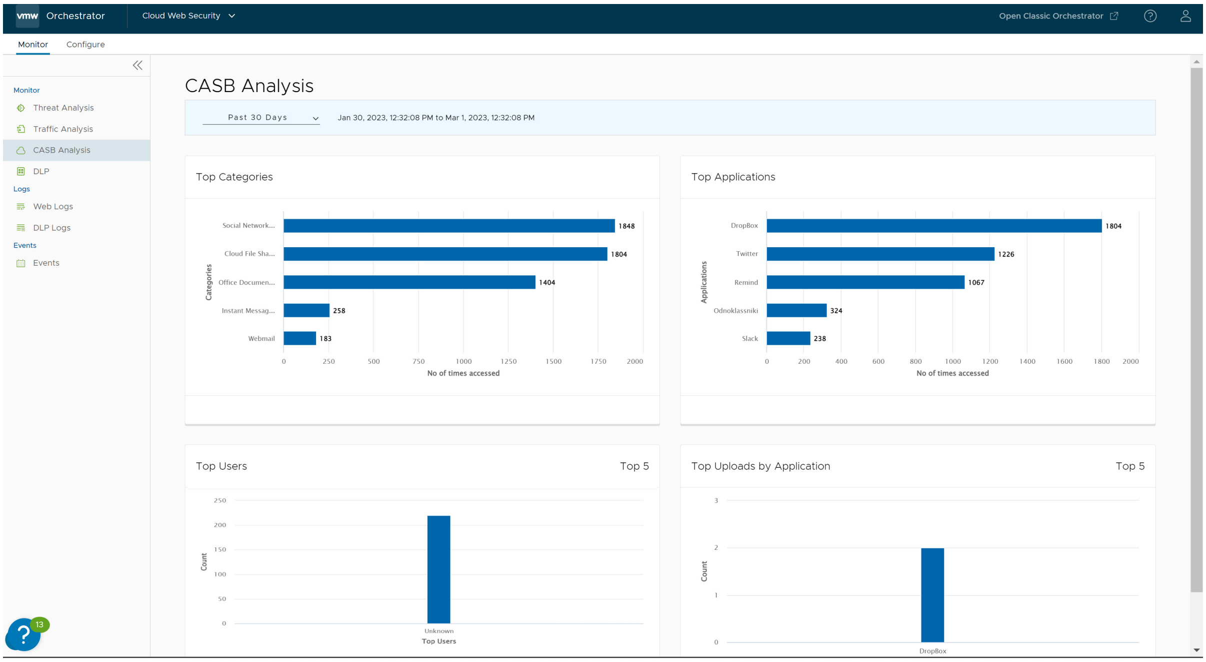
Summary

Date	Jul 13, 2022, 11:36:18 AM	**User ID**	jdoe@vmw-nbarrett-ad.tlblt.info
URL	https://auth.wetransfer.com/login/callback?state=01m3pu6Zx3ZxBa_in6c6CFdq9Y2opu6s&code=4%2F0AdQt8qi72dsQiZuGOODdYPu75D7CDnvpYPti2kfP9QBa6cckB_7md_IpXuANVMpUs7TBHQ&scope=email+profile+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.profile+openid&authuser=0&prompt=consent	**Domain**	auth.wetransfer.com
Categories	Personal Storage	**Web Risk Score**	● Low
Action	Block	**User-Agent**	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Browser Type	Firefox	**Browser Version**	91
Request Type	CASB Request	**Request Method**	GET
Egress IP	NA	**Destination IP**	NA
DNS Response	13.249.85.113, 13.249.85.119, 13.249.85.28, 13.249.85.56	**Source IP**	192.168.100.57
Access Mode	proxy	**Protocol**	https
Rule Matched	Deny Unsanctioned File Sharing	**Policy Headers**	3885666408
File Hash Score	-1	**CASB Application Name**	WeTransfer
CASB Category Name	Cloud File Sharing	**CASB Function Name**	Login
CASB Organization Name	WeTransfer B.V.	**CASB Risk Score**	6

Monitor CASB

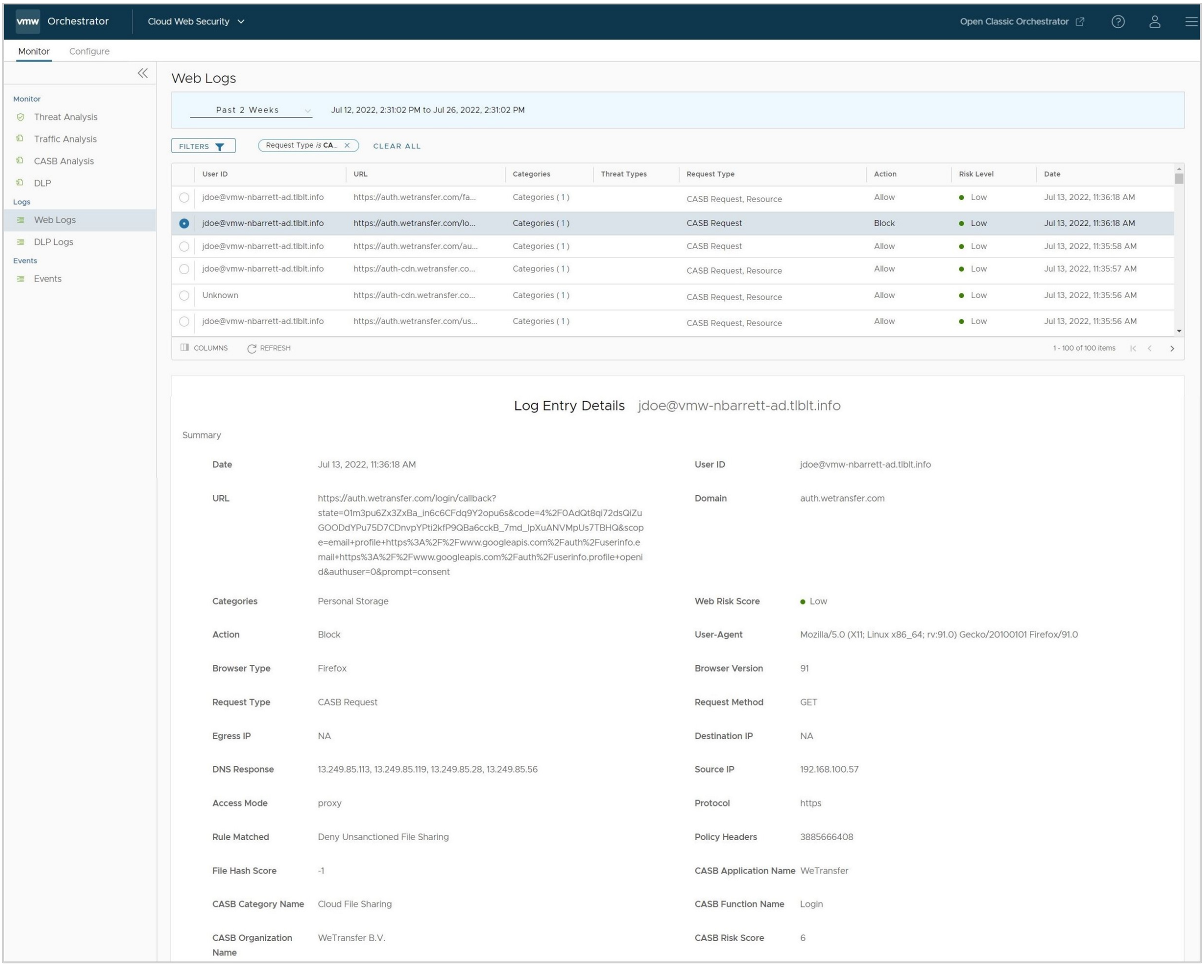
1 Navigate to **Cloud Web Security > Monitor > CASB Analysis**.

2 On the **CASB Analysis** page, users can view a selection of bar charts for Top Categories, Top Applications, Top User, and Top Uploads by Application.



Jan 30, 2023, 12:32:08 PM to Mar 1, 2023, 12:32:08 PM

3 **Web Logs**: **Cloud Web Security > Monitor > Web Logs** page users can learn greater details about an application access event. For any CASB Application event, user can click the bubble associated with that log entry to see the full **Log Entry Details**.



Jul 12, 2022, 2:31:02 PM to Jul 26, 2022, 2:31:02 PM

	User ID	URL	Categories	Threat Types	Request Type	Action	Risk Level	Date
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/fa...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:36:18 AM
●	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/lo...	Categories (1)		CASB Request	Block	● Low	Jul 13, 2022, 11:36:18 AM
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/au...	Categories (1)		CASB Request	Allow	● Low	Jul 13, 2022, 11:35:58 AM
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth-cdn.wetransfer.co...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:35:57 AM
○	Unknown	https://auth-cdn.wetransfer.co...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:35:56 AM
○	jdoe@vmw-nbarrett-ad.tlblt.info	https://auth.wetransfer.com/us...	Categories (1)		CASB Request, Resource	Allow	● Low	Jul 13, 2022, 11:35:56 AM

Log Entry Details jdoe@vmw-nbarrett-ad.tlblt.info

Summary

Date	Jul 13, 2022, 11:36:18 AM	**User ID**	jdoe@vmw-nbarrett-ad.tlblt.info
URL	https://auth.wetransfer.com/login/callback?state=01m3pu6Zx3ZxBa_in6c6CFdq9Y2opu6s&code=4%2F0AdQt8qi72dsQiZuGOODdYPu75D7CDnvpYPti2kfP9QBa6cckB_7md_lpXuANVMpUs7TBHQ&scope=email+profile+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.profile+openid&authuser=0&prompt=consent	**Domain**	auth.wetransfer.com
Categories	Personal Storage	**Web Risk Score**	● Low
Action	Block	**User-Agent**	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Browser Type	Firefox	**Browser Version**	91
Request Type	CASB Request	**Request Method**	GET
Egress IP	NA	**Destination IP**	NA
DNS Response	13.249.85.113, 13.249.85.119, 13.249.85.28, 13.249.85.56	**Source IP**	192.168.100.57
Access Mode	proxy	**Protocol**	https
Rule Matched	Deny Unsanctioned File Sharing	**Policy Headers**	3885666408
File Hash Score	-1	**CASB Application Name**	WeTransfer
CASB Category Name	Cloud File Sharing	**CASB Function Name**	Login
CASB Organization Name	WeTransfer B.V.	**CASB Risk Score**	6

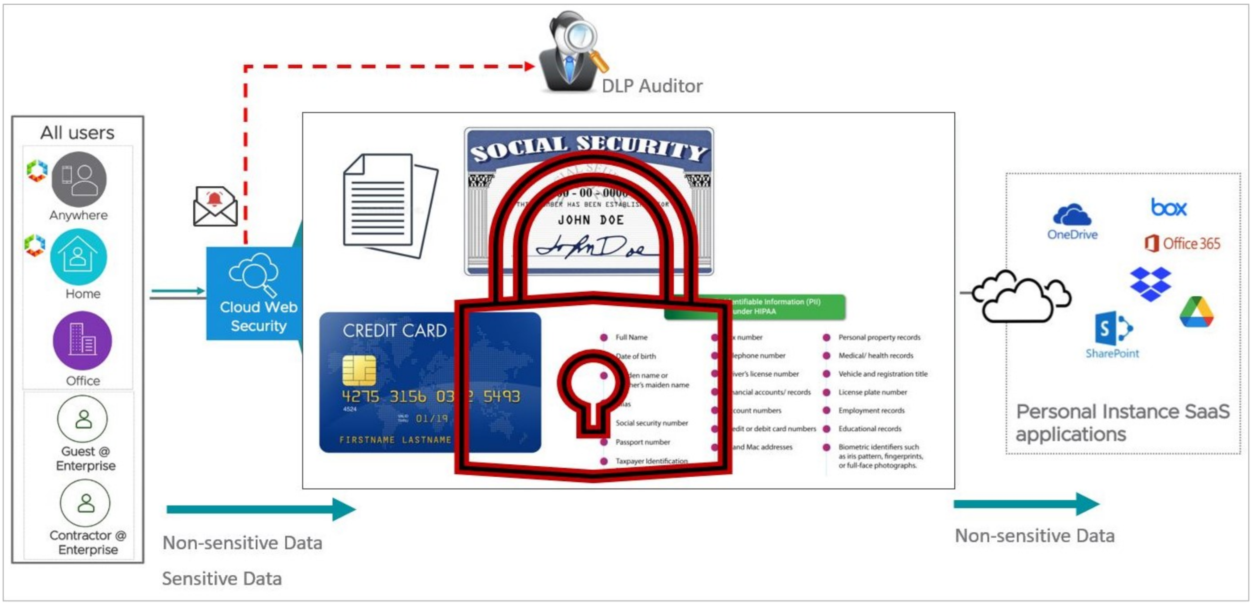
Data Loss Prevention

3

This section covers the core components of Data Loss Prevention (DLP) for the Cloud Web Security service and how they are used to create rules that prevent data leakage for a customer Enterprise. The DLP section concludes with a workflow for configuring a DLP Rule and verifying that the rule works properly.

Overview

The Data Loss Prevention (DLP) feature prevents the unintentional or intentional leakage of sensitive data to the Internet to ensure compliance with HIPAA, PCI, GDPR, and other data privacy laws. The DLP feature inspects file uploads and text entered into Web pages for sensitive data by referencing it. When a DLP inspection discovers sensitive data, the Cloud Web Security administrator can set the action to **skip**, **log**, or **block** while also providing an optional email alert to an Auditor.



While the DLP requirements for every organization are different, the workflow for creating a DLP policy is the same regardless.

The first half describes the two key components of the DLP feature: Dictionaries (predefined and custom), and Auditors. The second half covers the process of creating and applying a DLP rule.

Note For answers to frequently asked questions about DLP, see Data Loss Prevention Frequently Asked Questions.

Prerequisites

Users need the following for access to the Data Loss Prevention (DLP) feature with Cloud Web Security:

1. A customer enterprise on a production VMware SASE Orchestrator with Cloud Web Security activated. Both the Edges and Orchestrator must use VMware Release 4.5.0 or later.
2. A customer must have a Cloud Web Security Advanced package to access the DLP feature.

   Important A customer with a Cloud Web Security Standard package would not be able to access DLP and a locked icon would appear next to all DLP options on the Orchestrator UI.

Overview of DLP Dictionaries

A DLP Dictionary uses matching expressions to identify sensitive data. For example, credit card numbers and social security numbers follow a specific format. And dictionaries can match against those patterns and determine if sensitive data is or is not present in a file upload or text input.

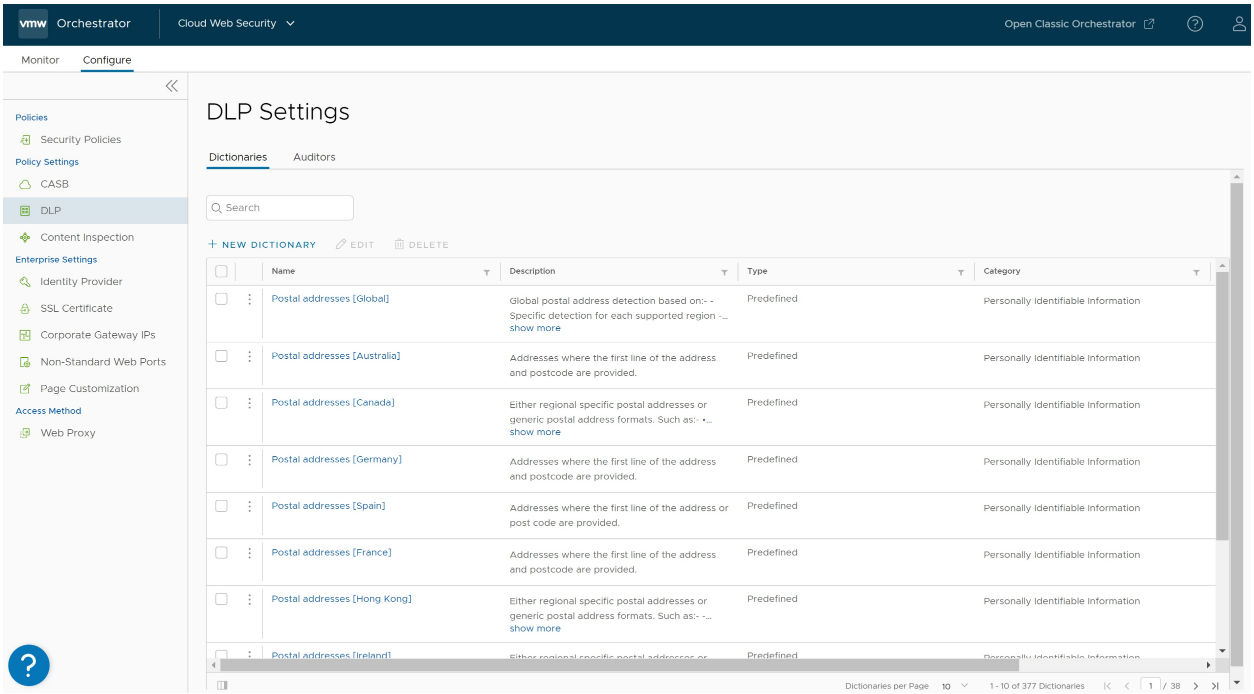
Predefined Dictionaries

Cloud Web Security predefined data dictionaries are a combination of pattern matching, checksums, context scoring, and fuzzy logic to identify sensitive data. Cloud Web Security has more than 340 predefined data dictionaries covering the following major data categories:

- Document Classification
- Financial Data
- Health Care
- HIPAA
- Item Identifiers
- PCI DSS
- PII

Additionally, the predefined data dictionaries are region-specific to ensure correct pattern matching is applied across the globe. Data dictionaries can be set to 29 different countries or regions. Of those 29, two are reserved for **Global** and **Other**. These two options allow categorizing multinational data or data that does not neatly fit into a country or region category.

Users can explore dictionaries on the VMware SASE Orchestrator by going to the **Cloud Web Security** section and navigating to **Configure > Policy Settings > DLP > Dictionaries**



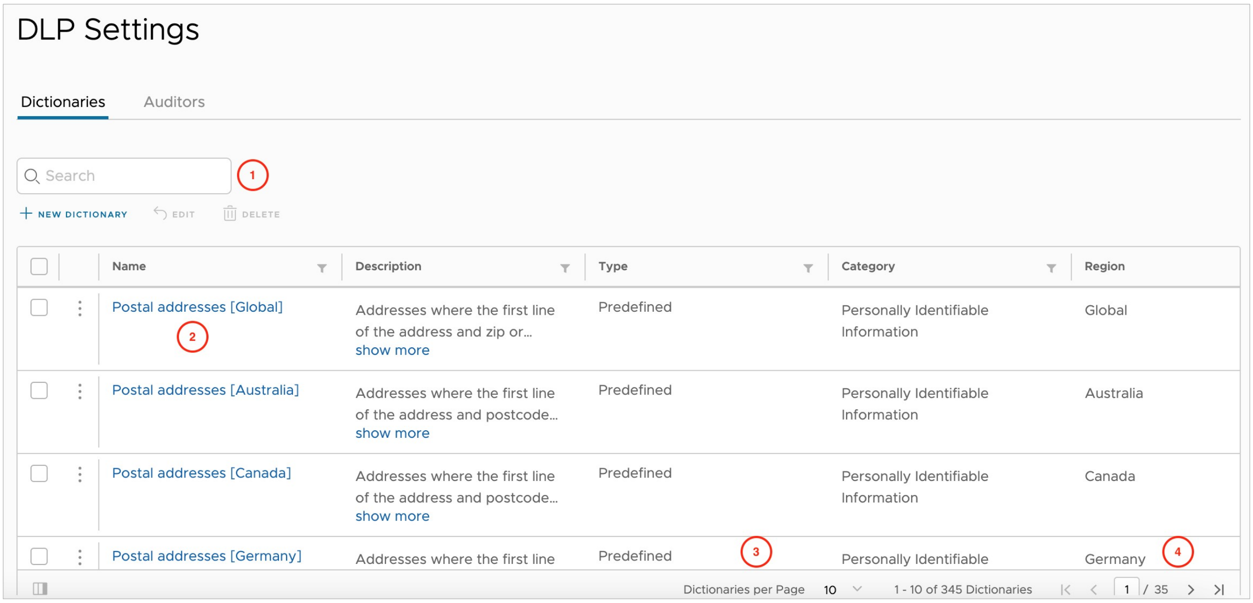
Name	Description	Type	Category
Postal addresses [Global]	Global postal address detection based on:- - Specific detection for each supported region -… show more	Predefined	Personally Identifiable Information
Postal addresses [Australia]	Addresses where the first line of the address and postcode are provided.	Predefined	Personally Identifiable Information
Postal addresses [Canada]	Either regional specific postal addresses or generic postal address formats. Such as:- •… show more	Predefined	Personally Identifiable Information
Postal addresses [Germany]	Addresses where the first line of the address and postcode are provided.	Predefined	Personally Identifiable Information
Postal addresses [Spain]	Addresses where the first line of the address or post code are provided.	Predefined	Personally Identifiable Information
Postal addresses [France]	Addresses where the first line of the address and postcode are provided.	Predefined	Personally Identifiable Information
Postal addresses [Hong Kong]	Either regional specific postal addresses or generic postal address formats. Such as:- -… show more	Predefined	Personally Identifiable Information
Postal addresses [Ireland]	Either regional specific postal addresses or	Predefined	Personally Identifiable Information

Dictionaries per Page 10 1 - 10 of 377 Dictionaries 1 / 38

On this page, users are shown all the dictionaries available for use in DLP policy. The dictionaries are organized in a table containing names, descriptions, types, categories, and region fields.

- **Name** is used to identify the dictionary for use in policy.
- **Description** provides a high-level overview of what the dictionary matches.
- **Type** distinguishes two different dictionary types:
  - Predefined
  - Custom
- **Category** includes:
  - Canadian Health Service
  - Document Classification
  - Financial Data, HIPAA
  - HIPAA/Health Care
  - Health Care
  - Item Identifiers
  - Other
  - PCI DSS
  - Personally Identifiable Information

  - UK National Health Service
- **Region** represents the geography the dictionary applies to, which includes:
  - Australia
  - Belgium
  - Brazil
  - Canada
  - Denmark
  - Finland
  - France
  - Germany
  - Global
  - Hong Kong
  - India
  - Indonesia
  - Ireland
  - Italy
  - Japan
  - Malaysia
  - Netherlands
  - New York
  - New Zealand
  - Norway
  - Other
  - Poland
  - Singapore
  - South Africa
  - Spain
  - Sweden
  - United Kingdom (UK)
  - United States of America (USA)



☐		Name	Description	Type	Category	Region
☐	⋮	Postal addresses [Global]	Addresses where the first line of the address and zip or... show more	Predefined	Personally Identifiable Information	Global
☐	⋮	Postal addresses [Australia]	Addresses where the first line of the address and postcode... show more	Predefined	Personally Identifiable Information	Australia
☐	⋮	Postal addresses [Canada]	Addresses where the first line of the address and postcode... show more	Predefined	Personally Identifiable Information	Canada
☐	⋮	Postal addresses [Germany]	Addresses where the first line	Predefined	Personally Identifiable	Germany

Dictionaries per Page 10 1 - 10 of 345 Dictionaries 1 / 35

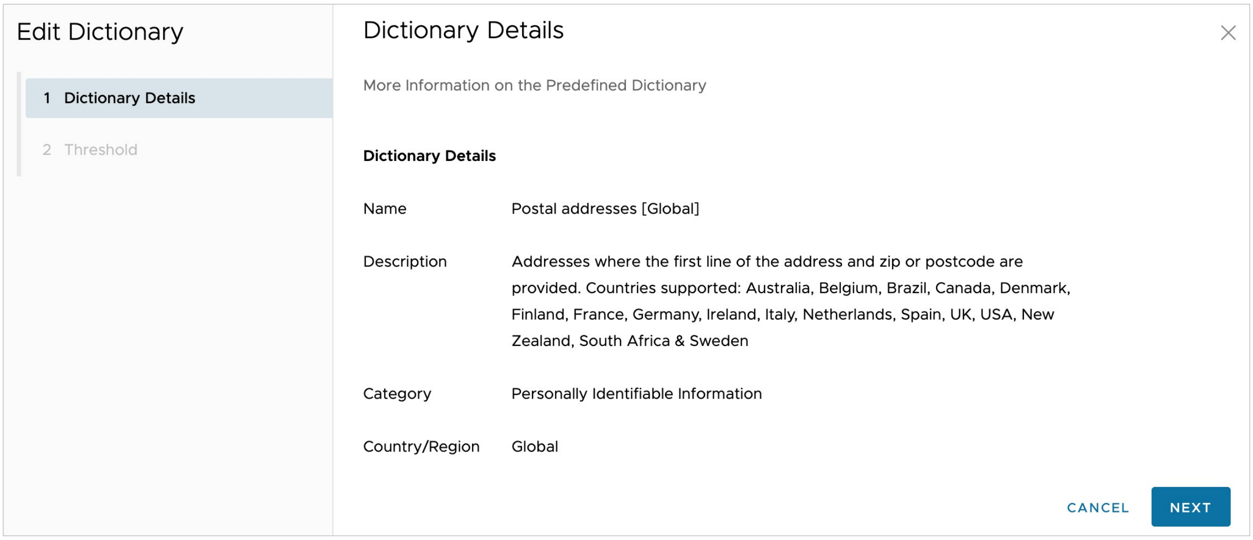
1 The **Search** bar applies to all fields on the Dictionaries page and can be used to quickly display specific dictionaries users are interested in viewing.

2 Each row contains a dictionary that can be clicked to explore further.

3 The **Dictionaries per Page** can display up to 100 entries on a single page.

4 **Page Navigation** buttons are provided for going back or skipping ahead.

To continue this examination, find the **Postal addresses [Global]** dictionary and click on the blue text to bring up the **Edit Dictionary** screen.



More Information on the Predefined Dictionary

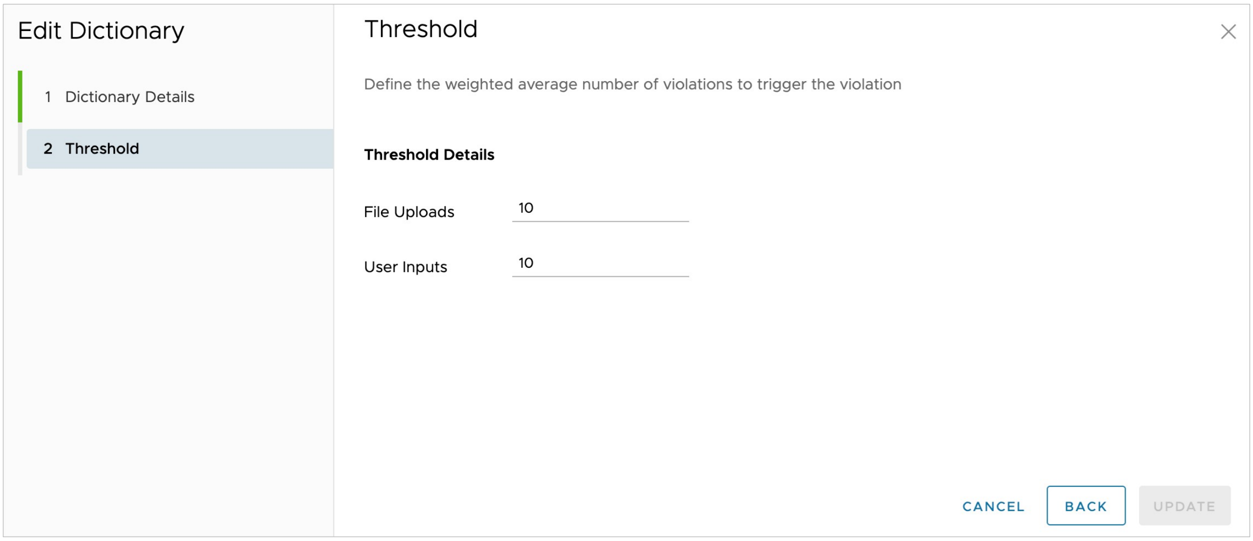
Dictionary Details

Name	Postal addresses [Global]
Description	Addresses where the first line of the address and zip or postcode are provided. Countries supported: Australia, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Ireland, Italy, Netherlands, Spain, UK, USA, New Zealand, South Africa & Sweden
Category	Personally Identifiable Information
Country/Region	Global

While the fields on this page have already been discussed, there is one that warrants further explanation. The **Description** provides the details needed to know whether this dictionary is appropriate for your policy. The exact mechanisms used to identify data are proprietary and confidential. However, users can be assured that pattern matching uses advanced techniques to ensure accuracy across the numerous categories and regions dictionaries support.

Note The method used with predefined dictionaries of triggering a DLP violation based on a sensitivity level and DLP engine heuristics is in contrast to the method used for a Custom Dictionary, which uses a specific repeat count. There are more details on that method in the Custom Dictionary section.

Clicking on the **Next** button in the modal brings users to the **Threshold** settings. It is not recommended to adjust the **Threshold Details** from their default values unless necessary.



Edit Dictionary

1 Dictionary Details

2 Threshold

Threshold

Define the weighted average number of violations to trigger the violation

Threshold Details

File Uploads: 10

User Inputs: 10

The screenshot above shows the **weighted average number** of violations for both **File Uploads** and **User Inputs** is set to **10**. For predefined dictionaries, do not think of this as a simple occurrence count but rather a computational scoring of all information discovered in a document. This scoring mechanism helps to reduce the number of false positives observed when using this data dictionary. When finished viewing this modal, click **Cancel**. Please note that if users made changes to any editable values, users would need to click **Update** to preserve those changes.

Custom Dictionaries

Cloud Web Security DLP Custom Dictionaries give users the flexibility to create data dictionaries pertinent to their organization. As with predefined dictionaries, customer dictionaries start by having users add four fields:

- Name
- Description
- Category

- Country/Region

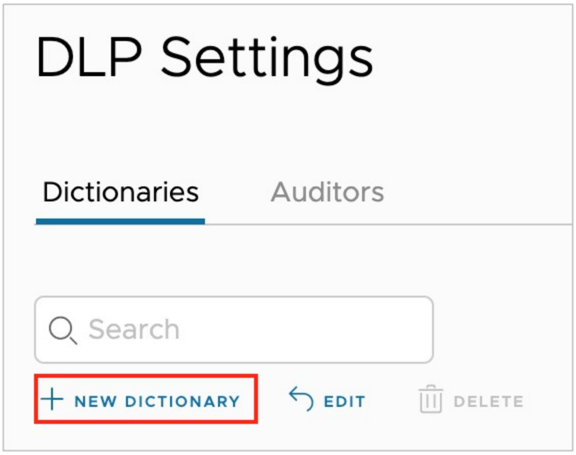
These are the same four fields shown for predefined dictionaries, but with the ability to set each value to what is relevant for the dictionary users are creating.

For identifying data, customer dictionaries employ two methods:

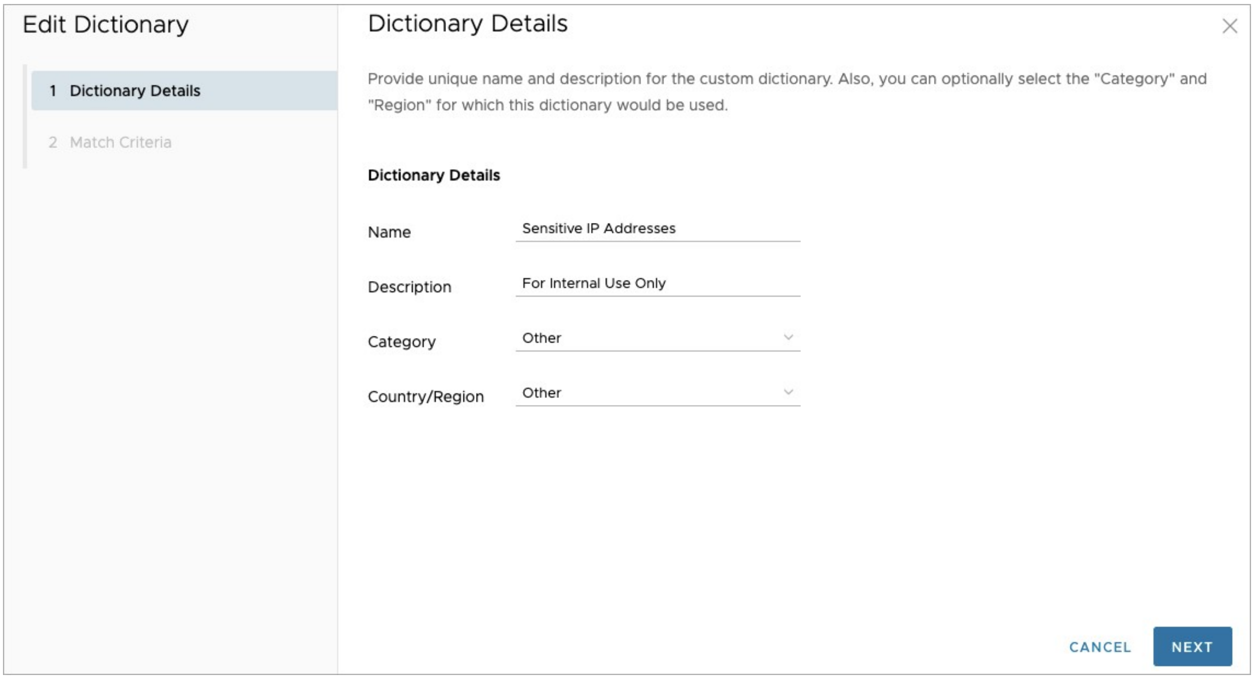
- **String** is used to match an exact combination of alphanumeric and special characters. It can be set to match or ignore casing.
- **Expression** uses Perl regular expressions (regex) to find data patterns that are otherwise difficult to find with a simple string.

There are numerous resources on the Internet for learning more about regular expressions. One such resource is https://perldoc.perl.org/perlre. Here users can find multiple examples of different pattern matching syntax for regexes.

To create a Custom Dictionary, click the **New Dictionary** button from **Configure > Policy Settings > DLP > Dictionaries** page.



The Dictionary Details screen prompts users to enter values for **Name**, **Description**, **Category**, and **Country/Region**.



Dictionary Details

Provide unique name and description for the custom dictionary. Also, you can optionally select the "Category" and "Region" for which this dictionary would be used.

Dictionary Details

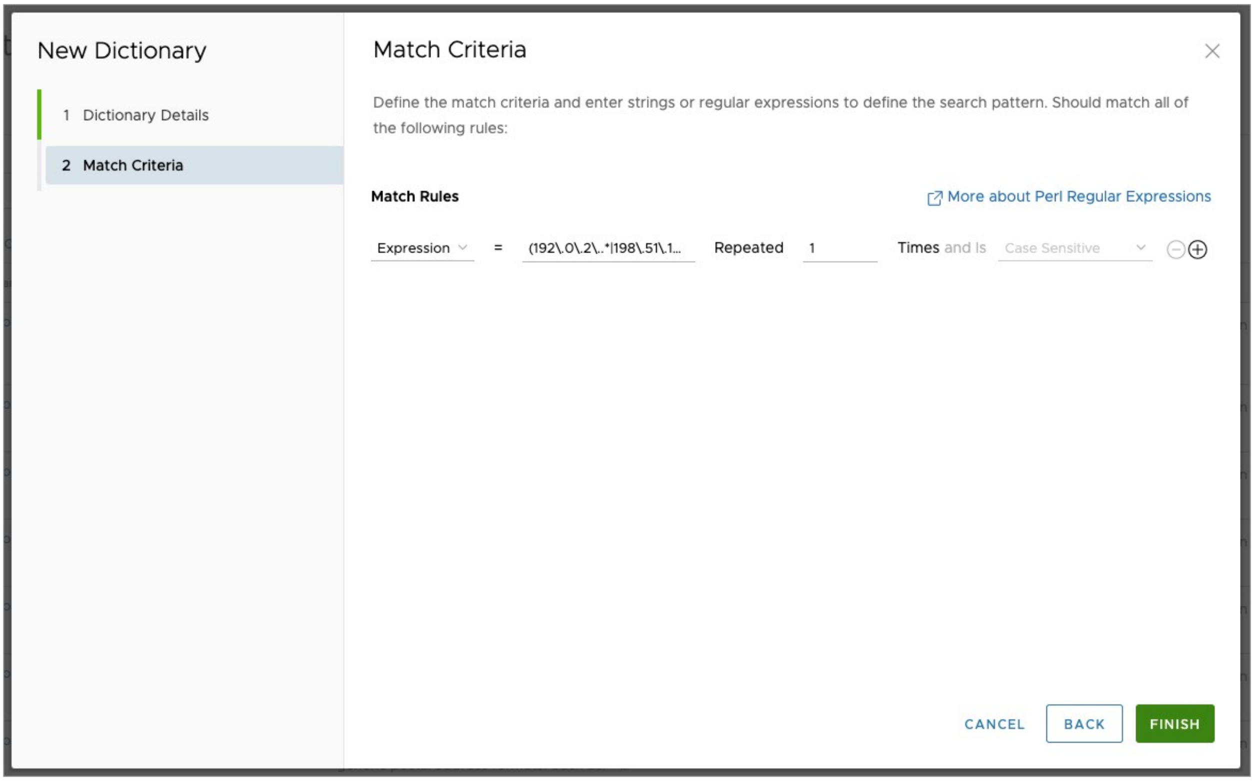
Name: Sensitive IP Addresses

Description: For Internal Use Only

Category: Other

Country/Region: Other

The screenshot above indicates that this dictionary is meant to identify **Sensitive IP Addresses** and is **For Internal Use Only**. The selection of **Other** for both category and country/region indicate that the data matched by this dictionary either does not fit into one of the preexisting categories, or the additional metadata is not necessary.



Match Criteria

Define the match criteria and enter strings or regular expressions to define the search pattern. Should match all of the following rules:

Match Rules

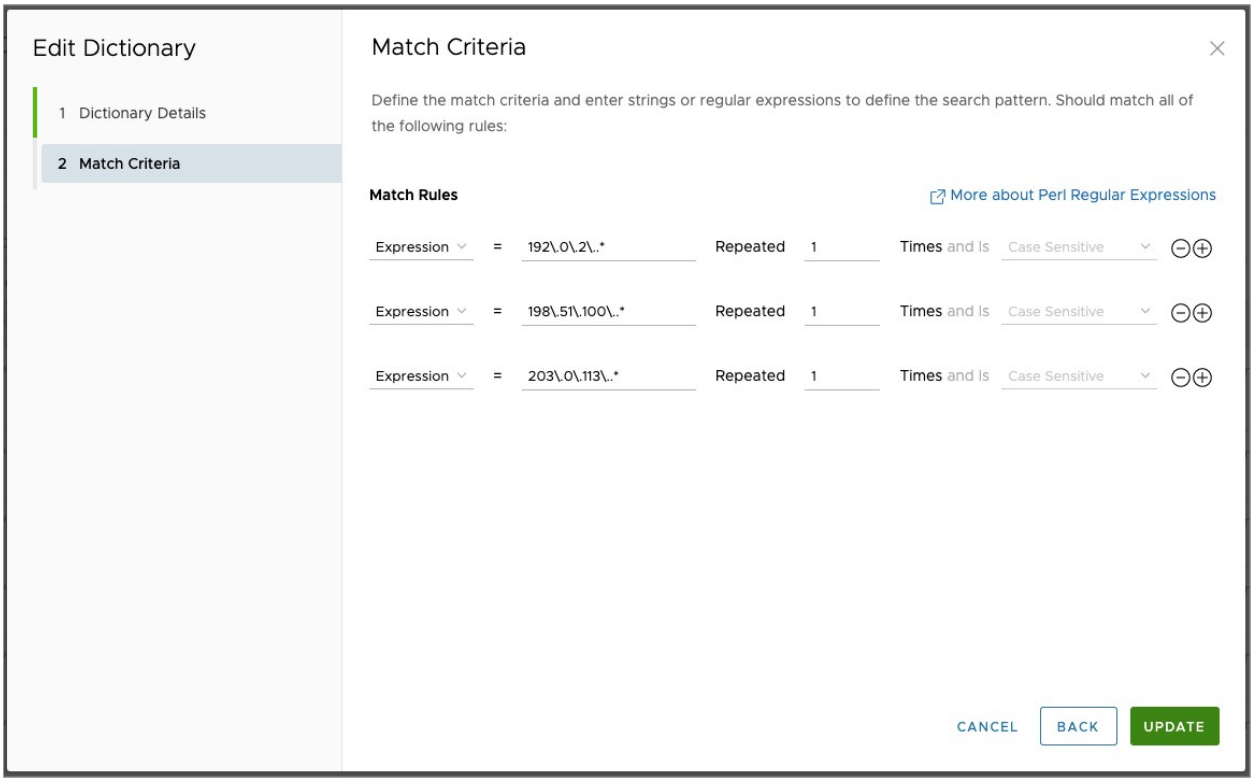
Expression = (192\.0\.2\..*|198\.51\.1... Repeated 1 Times and Is Case Sensitive

For the **Match Data** screen, the example configuration is based on the IP address ranges 192.0.2.0/24, 198.151.100.0/24, and 203.0.133.0/24 (RFC 5737), the sensitive data the company needs to protect. The regex used to look for any IP addresses in those ranges is: **(192\.0\.2\..*|198\.51\.100\..*|203\.0\.113\..*)**

The regex is read as, "Match a string if it contains 192.0.2. OR 198.51.100. OR 203.0.113." And the **Repeated** value is set to **1**, indicating that discovering this pattern one or more times will trigger the dictionary.

Note While a Custom Dictionary uses a specific repeat count to trigger a DLP violation, for a Predefined Dictionary the threshold to trigger the DLP violation is based on a sensitivity level and DLP engine heuristics.

The regex is not broken up over several lines using the **Plus Icon** to add another row because the dictionary logic across multiple rows is a logical AND. Had the **Match Criteria** been defined in this manner, the dictionary would trigger only when all three IP address ranges were present in a document.



Edit Dictionary

1 Dictionary Details

2 Match Criteria

Match Criteria

Define the match criteria and enter strings or regular expressions to define the search pattern. Should match all of the following rules:

Match Rules

More about Perl Regular Expressions

Expression = 192\.0\.2\..* Repeated 1 Times and Is Case Sensitive

Expression = 198\.51\.100\..* Repeated 1 Times and Is Case Sensitive

Expression = 203\.0\.113\..* Repeated 1 Times and Is Case Sensitive

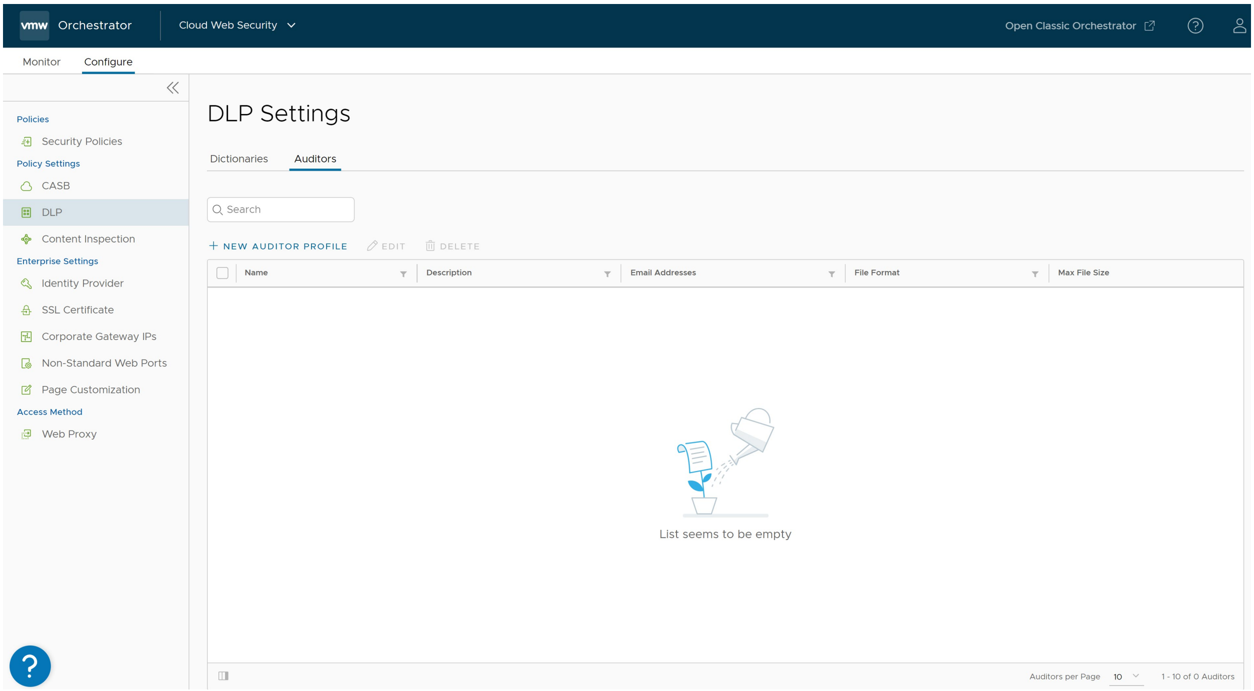
After configuring the Custom Dictionary settings, click **Finish** to make the dictionary available for use in Cloud Web Security.

Auditors

An Auditor is someone in the organization designated to follow up on any incidents that pertain to the attempted exfiltration of data, whether intentional or accidental. This individual can be notified via email from the Orchestrator that a DLP rule has been violated. The email sent to the Auditor contains the name of the DLP rule, user's input or file name that contained sensitive data, the destination to which the user was trying to send the data, and the person's username that tried to expose the data. Optionally, user's input or file can be sent to the Auditor, either in its original format, as a ZIP file, or an encrypted ZIP file.

Users can add, edit, delete, and view auditors by logging into Cloud Web Security and navigating to:

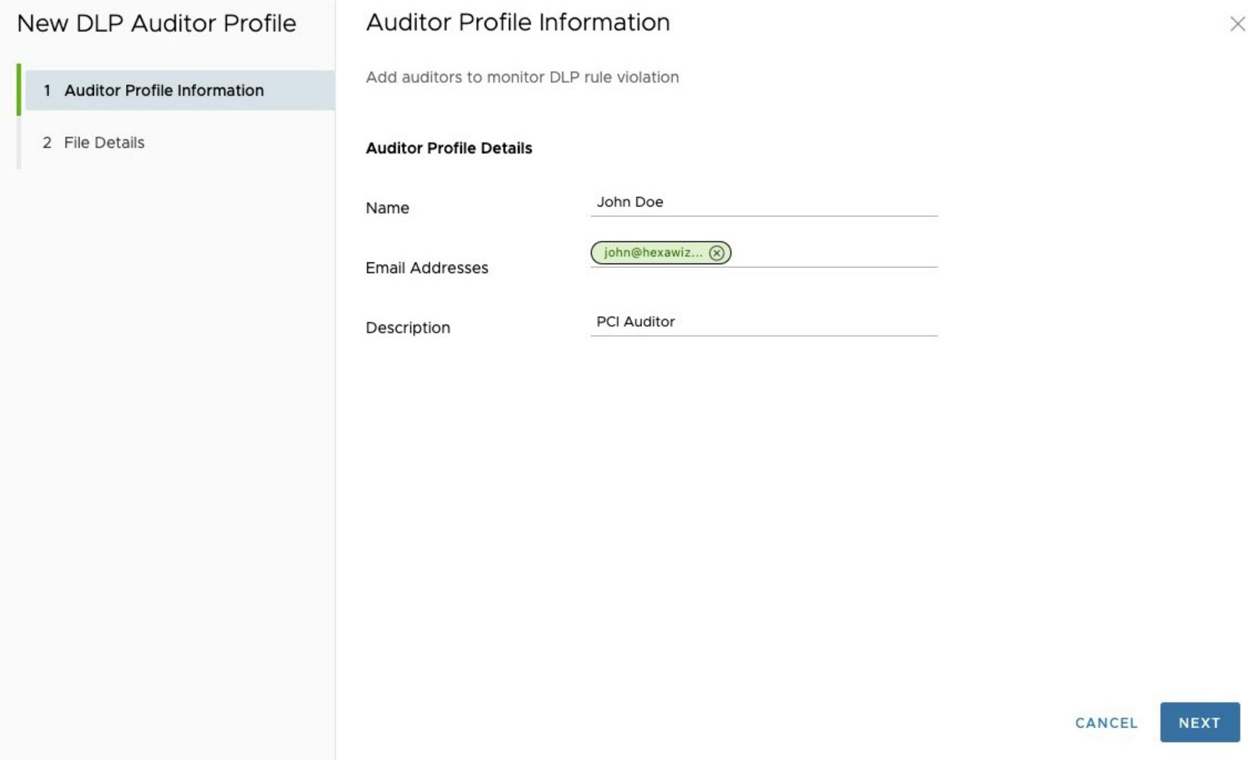
Configure > **Policy Settings** > **DLP** > **Auditors**



List seems to be empty

In the Auditors screen, users can see that there are currently no auditors in the system. To add the first Auditor, select **+ NEW AUDITOR PROFILE**. A pop-up will prompt users to provide the following information:

- **Name (mandatory)** is the name of Auditor.
- **Email Address (mandatory)** is a valid email address account for the individual.
- **Description (optional)** is any relevant information users would want to provide about the Auditor. For example, "PCI Auditor" if the Auditor's primary function is to monitor for PCI violations.



New DLP Auditor Profile

1 Auditor Profile Information

2 File Details

Auditor Profile Information

Add auditors to monitor DLP rule violation

Auditor Profile Details

Name: John Doe

Email Addresses: john@hexawiz...

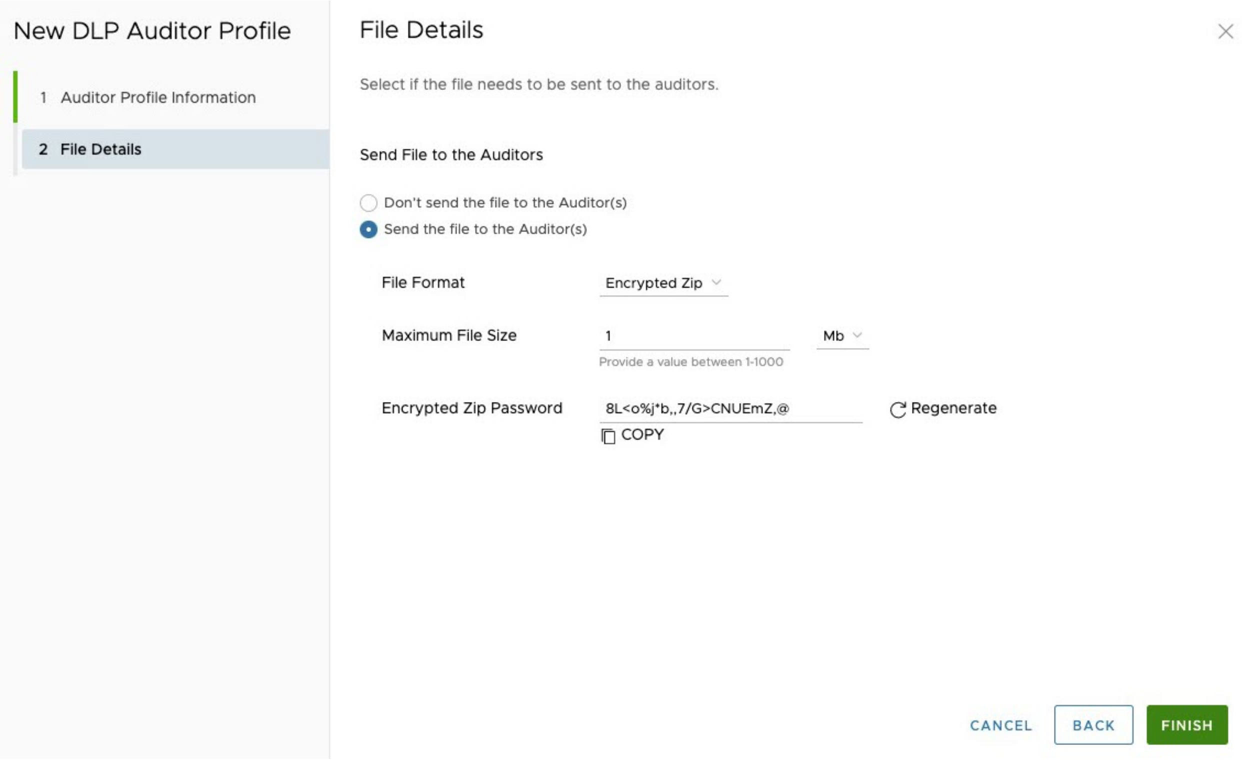
Description: PCI Auditor

The next page will ask users for **File Details**. This page is completely optional, but it provides users with the option to send the offending file to the DLP Auditor for their review. Configuration options include:

- **Send File to the Auditors**, with the default behavior being to not send the file to the Auditor(s).
- **File Format** becomes available when users select **Send the file to the Auditor(s)**. Users have the option of selecting the Original File, Zip, or Encrypted Zip. Since this file will contain sensitive information, it is recommended to use the Encrypted Zip option.
  - **Maximum File Size** is the maximum size of the attachment included with the email that is sent by the system. The limit can be set for up to 1GB, but it is recommended to match their organization's email file size restrictions.

    Important If a file size exceeds the **Maximum File Size** value, then that file is bypassed. In other words, the file is not attached to the DLP violation alert, and the alert is sent without the file.

  - **Encrypted Zip Password** is autogenerated by the system and can be regenerated if compromised. Users can also configure their own password if desired.



File Details

Select if the file needs to be sent to the auditors.

Send File to the Auditors

○ Don't send the file to the Auditor(s)
● Send the file to the Auditor(s)

File Format: Encrypted Zip
Maximum File Size: 1 Mb
Provide a value between 1-1000
Encrypted Zip Password: 8L<o%j*b,,7/G>CNUEmZ,@
COPY
Regenerate

Click the **Finish** button to save the New DLP Auditor Profile configuration. The Auditor entry appears in the DLP Settings Auditor page. Optionally, users can view, edit, or delete the Auditor entry.

DLP Configuration workflow

Having covered the two key components that comprise the Data Loss Prevention (DLP) feature, this section will cover the overall DLP workflow.

Create, Configure, and Apply a Security Policy

A DLP rule is part of a **Security Policy** and thus prior to configuring a DLP rule, there must first be a Security Policy. For details on Create a Security Policy, Configuring a Security Policy, or Applying a Security Policy a **Security Policy** for the Cloud Web Security service, consult the relevant documentation in the *Cloud Web Security Configuration Guide*.

Create and Apply a DLP Rule

To create and apply a DLP Rule, see Configure Data Loss Prevention Rules.

Verify a DLP Rule is Working

There are three criteria which together confirm that a DLP rule is configured properly and working as expected:

- Cloud Web Security blocks the exfiltration of sensitive data that matches a DLP Rule.
- Cloud Web Security detects and logs the attempt to exfiltrate sensitive data.
- Cloud Web Security sends an email alert to a DLP Auditor when the rule is triggered.

To verify the effectiveness of a DLP rule, do the following:

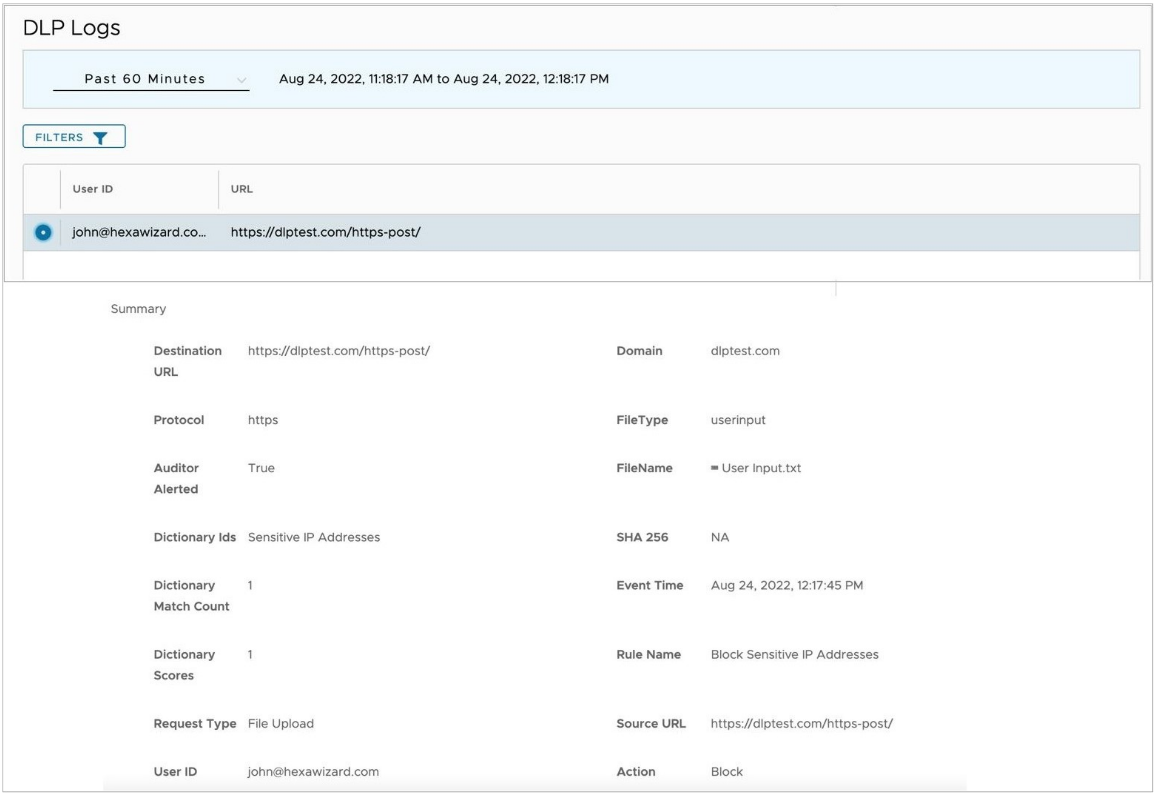
1. From an endpoint device (Windows, MacOS, iOS, or Android) that sits behind an SD-WAN Edge, login to a file hosting service (for example, Apple iCloud, Dropbox, Google Drive, Microsoft OneDrive or similar).
2. If the rule includes a Custom Dictionary, upload a Text Input, Text File, or PDF which matches the criteria set in the DLP Rule.

   Note Text Input is like a form post or text message. A Text File is an actual .txt attached to an upload.

3. Alternatively, use any of the Predefined Dictionaries and their respective thresholds for PII data, Social Security numbers, Bank Account numbers, or something similar.

   Note With Predefined Dictionaries, the threshold to trigger the DLP violation is based on the combination of a sensitivity level and DLP engine heuristics. This contrasts with the Custom Dictionary which uses a specific repeat count.

4. The text file/input or file upload is blocked.
5. Verify in the DLP logs that the block action has been logged.
   a. The following is a sample log for a Text Input block in DLP Test which matches a Custom Dictionary the DLP Rule uses.



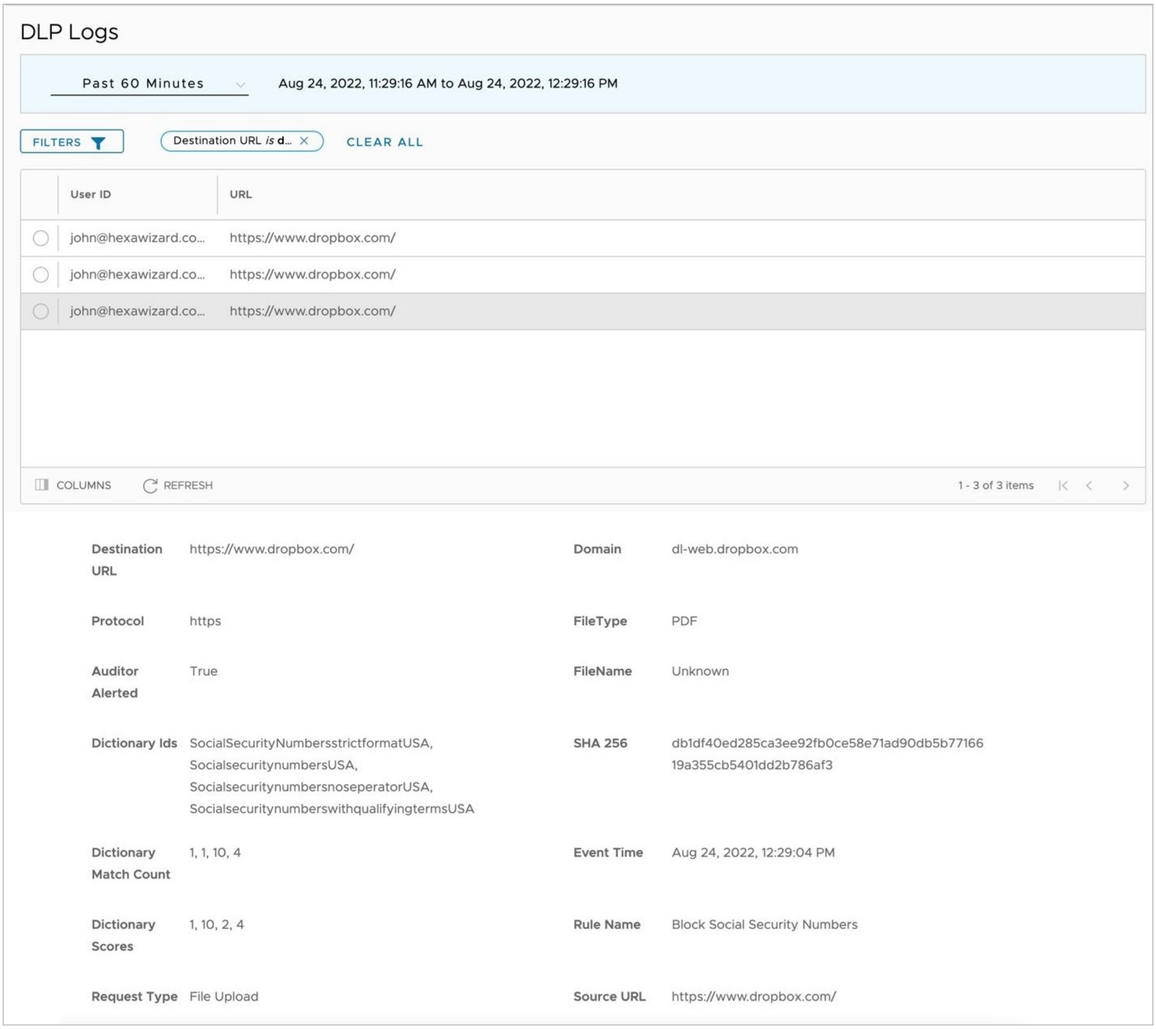
Aug 24, 2022, 11:18:17 AM to Aug 24, 2022, 12:18:17 PM

	User ID	URL
●	john@hexawizard.co...	https://dlptest.com/https-post/

Summary

Destination URL	https://dlptest.com/https-post/	**Domain**	dlptest.com
Protocol	https	**FileType**	userinput
Auditor Alerted	True	**FileName**	User Input.txt
Dictionary Ids	Sensitive IP Addresses	**SHA 256**	NA
Dictionary Match Count	1	**Event Time**	Aug 24, 2022, 12:17:45 PM
Dictionary Scores	1	**Rule Name**	Block Sensitive IP Addresses
Request Type	File Upload	**Source URL**	https://dlptest.com/https-post/
User ID	john@hexawizard.com	**Action**	Block

b The following is a sample log for a PDF file blocked in Dropbox for a Social Security number match from a Predefined Dictionary.



DLP Logs

Aug 24, 2022, 11:29:16 AM to Aug 24, 2022, 12:29:16 PM

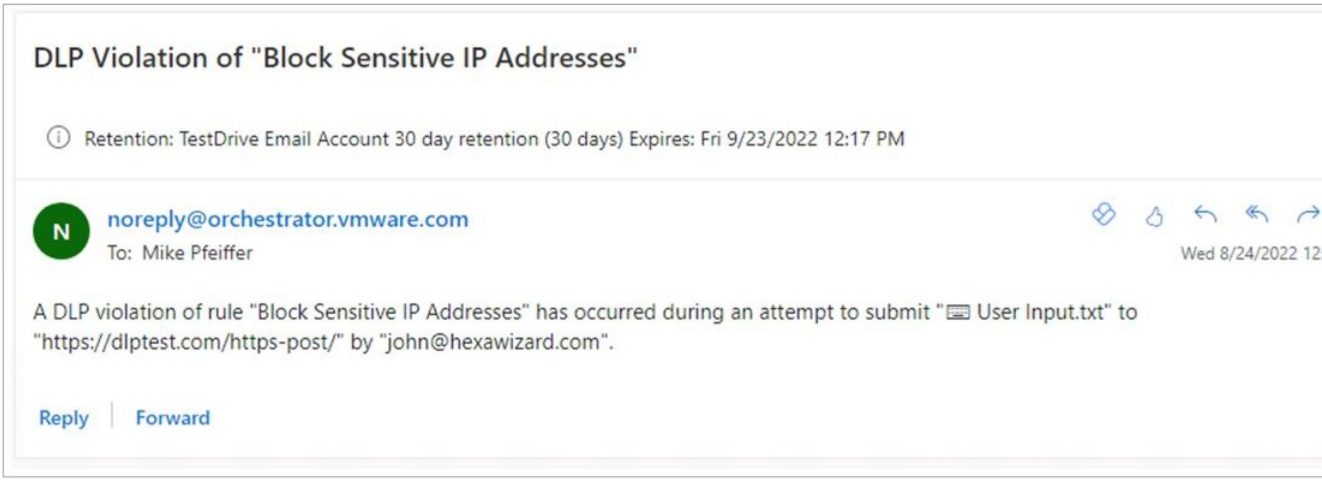
	User ID	URL
○	john@hexawizard.co...	https://www.dropbox.com/
○	john@hexawizard.co...	https://www.dropbox.com/
○	john@hexawizard.co...	https://www.dropbox.com/

1 - 3 of 3 items

Destination URL	https://www.dropbox.com/	**Domain**	dl-web.dropbox.com
Protocol	https	**FileType**	PDF
Auditor Alerted	True	**FileName**	Unknown
Dictionary Ids	SocialSecurityNumbersstrictformatUSA, SocialsecuritynumbersUSA, SocialsecuritynumbersnoseperatorUSA, SocialsecuritynumberswithqualifyingtermsUSA	**SHA 256**	db1df40ed285ca3ee92fb0ce58e71ad90db5b77166 19a355cb5401dd2b786af3
Dictionary Match Count	1, 1, 10, 4	**Event Time**	Aug 24, 2022, 12:29:04 PM
Dictionary Scores	1, 10, 2, 4	**Rule Name**	Block Social Security Numbers
Request Type	File Upload	**Source URL**	https://www.dropbox.com/

6 Verify that a DLP Auditor has received an alert email based on the DLP Rule and the action configured for this rule.

   a The following is a sample email for a Text Input block in DLP Test for a Custom Dictionary the DLP Rule uses.



DLP Violation of "Block Sensitive IP Addresses"

Retention: TestDrive Email Account 30 day retention (30 days) Expires: Fri 9/23/2022 12:17 PM

noreply@orchestrator.vmware.com

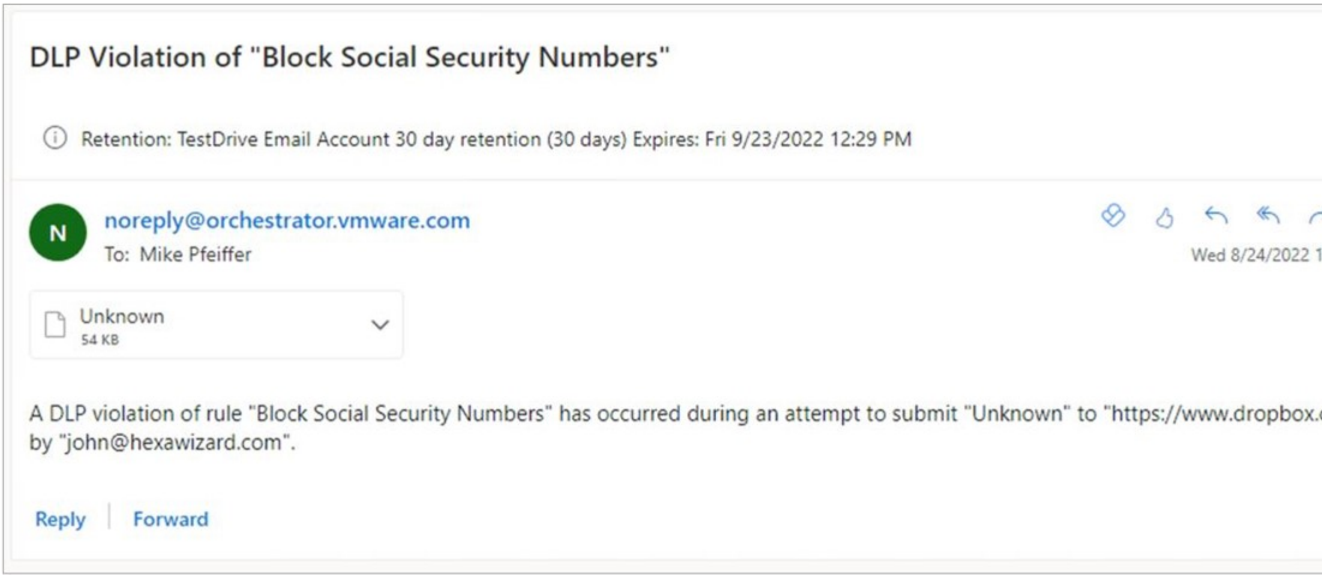
To: Mike Pfeiffer

Wed 8/24/2022 12

A DLP violation of rule "Block Sensitive IP Addresses" has occurred during an attempt to submit "⌨ User Input.txt" to "https://dlptest.com/https-post/" by "john@hexawizard.com".

b The following is a sample email for a PDF file blocked in Dropbox for a Social Security number match from a Predefined Dictionary.

Note Non-text files may appear with an "Unknown" file name. As a result, the attached file in the Auditor email would also show as "Unknown".



DLP Violation of "Block Social Security Numbers"

Retention: TestDrive Email Account 30 day retention (30 days) Expires: Fri 9/23/2022 12:29 PM

noreply@orchestrator.vmware.com

To: Mike Pfeiffer

Wed 8/24/2022 1

Unknown
54 KB

A DLP violation of rule "Block Social Security Numbers" has occurred during an attempt to submit "Unknown" to "https://www.dropbox.
by "john@hexawizard.com".

Read the following topics next:

- Data Loss Prevention Frequently Asked Questions

Data Loss Prevention Frequently Asked Questions

This section provides answers to frequently asked questions about **Data Loss Prevention (DLP)** feature of Cloud Web Security service.

1 **What is DLP?**

   Data Loss Prevention (also known as Data Leak Prevention) detects potential data breaches or data ex-filtration transmissions.

2 **Which requests are not supported by Cloud Web Security DLP?**

   Domains that are subject to an SSL Exception or included in your PAC (Proxy Auto-Configuration) file will not be analyzed by DLP.

3 **What file types can be scanned by Cloud Web Security DLP?**

   Cloud Web Security can inspect all file types. The file types to be inspected can be defined in each DLP rule. The file type is identified by Media/MIME type, magic number, and file extension. Certain file types such as images cannot be scanned by DLP.

4 **Are there any size limits with Cloud Web Security DLP?**

In the DLP policy, there is a maximum file size that can be defined in the DLP rule for file uploads. The maximum supported file size defined is currently set at 5 GB.

Table 3-1. Minimum Supported Content Sizes

User Input	File Input
1024 Bytes	5120 Bytes

5 **Does Cloud Web Security DLP work with zip files and encrypted zip files?**

Yes, DLP will extract and scan the file contained within the zip. For encrypted zip files, users will be prompted to enter the password.

6 **I am uploading some test data, why is Cloud Web Security DLP not detecting the data leakage?**

A common cause of reports is the use of artificially generated data when testing DLP functionality. We did a lot of research to ensure DLP does not detect items that merely look like what is being searched for. Therefore, artificial test data is often not real enough for us to detect.

For example, we are sometimes contacted for failing to detect test credit card numbers. This is typically due to the artificial card numbers having invalid check digits, the start digits being invalid or the spacing being incorrect for the brand of card.

7 **How do the DLP files get scanned? Is it all kept in RAM or is it written to disk at all?**

The DLP scanning happens inside a short lived/single use container which is locked down to have minimal access to the main VM and no network etc., The file is briefly written to disk so that the file system inside the container can get to the file (and only that file). It is deleted as soon as the scan completes along with the entire container's file system, usually within a few seconds.

Single Sign-On

4

You can use Single-Sign-On to log in with an Identity Provider using SAML. You can find out how to set up these Single-Sign-On solutions in the following guides.

Notes about Single Sign-On

The following are important caveats about Cloud Web Security Single Sign On.

1. The Cloud Web Security backend re-authentication value is set to 30 days by default.
2. Every time you change the policy, you need to log in again with your browser (otherwise the old authentication cookie will stay the same).
3. You can trigger a re-authentication by clearing the cache on your browser, restarting your browser or opening a new incognito mode session.
4. Please also note that it may take up to an hour for the group changes in your IdP to show up correctly in logs or for group based rules to work. This is because the group memberships are stored for an hour.

Read the following topics next:

- Configuring Azure Active Directory (AD) as an Identity Provider (IdP) with VMware Cloud Web Security
- Configuring Workspace ONE Access as an Identity Provider (IdP) with VMware Cloud Web Security

Configuring Azure Active Directory (AD) as an Identity Provider (IdP) with VMware Cloud Web Security

This section covers configuring Azure Active Directory (AD) as an Identity Provider (IdP) for Cloud Web Security. This allows Cloud Web Security policies to be configured to match on a username or groups as well as log the user access in the Web and DLP logs. We first cover the Azure AD configuration, and then the VMware Cloud Orchestrator configuration.

Prerequisites

Users need the following to configure an Azure Active Directory as an identity provider with Cloud Web Security:

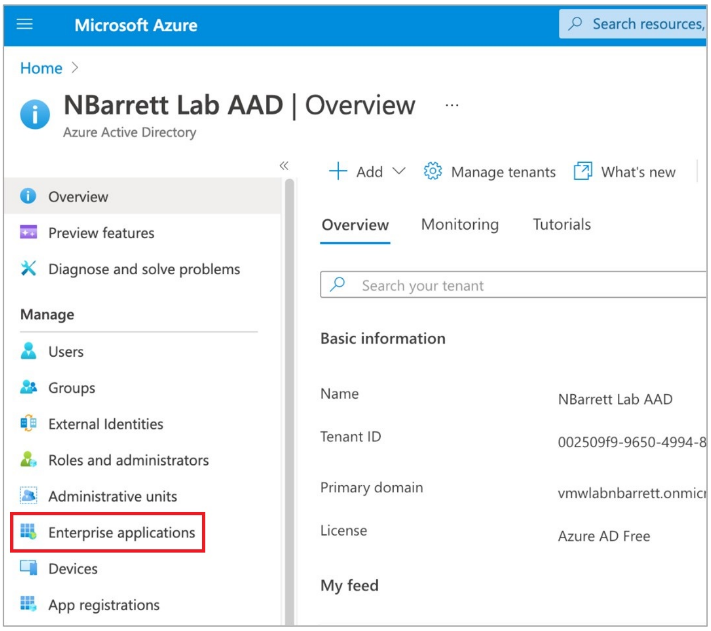
1. An Azure account
2. An Azure Active Directory (AD) tenant

   Tip The process for creating an Azure AD tenant is documented here.

3. A customer Enterprise on a production VMware Cloud Orchestrator with Cloud Web Security activated. The Orchestrator must use Release 4.5.0 or later.

Azure Configuration

1. Log into the Azure portal https://portal.azure.com/ using either your Enterprise credentials or a local user to your Azure AD tenant.
2. Access the **Azure Active Directory** service by searching for active directory in the top search bar.
3. Click on **Enterprise Applications** in the left-hand side panel:



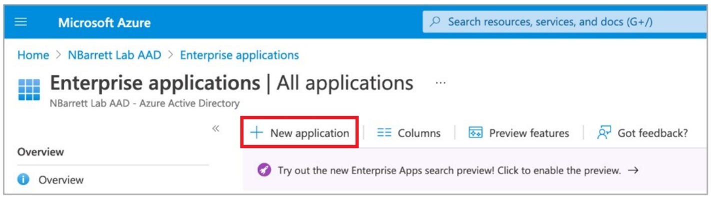
Name NBarrett Lab AAD

Tenant ID 002509f9-9650-4994-8

Primary domain vmwlabnbarrett.onmicr

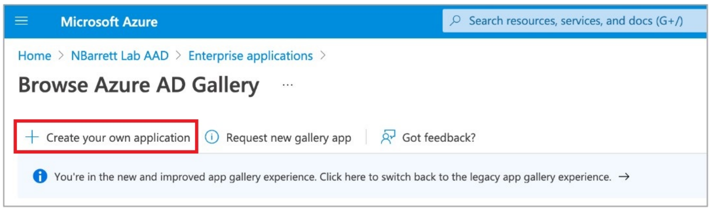
License Azure AD Free

4. Click on **New application** at the top of the **Enterprise Applications** panel:


Microsoft Azure
Search resources, services, and docs (G+/)
Home > NBarrett Lab AAD > Enterprise applications
Enterprise applications | All applications ...
NBarrett Lab AAD - Azure Active Directory
«
+ New application
Columns
Preview features
Got feedback?
Overview
Overview

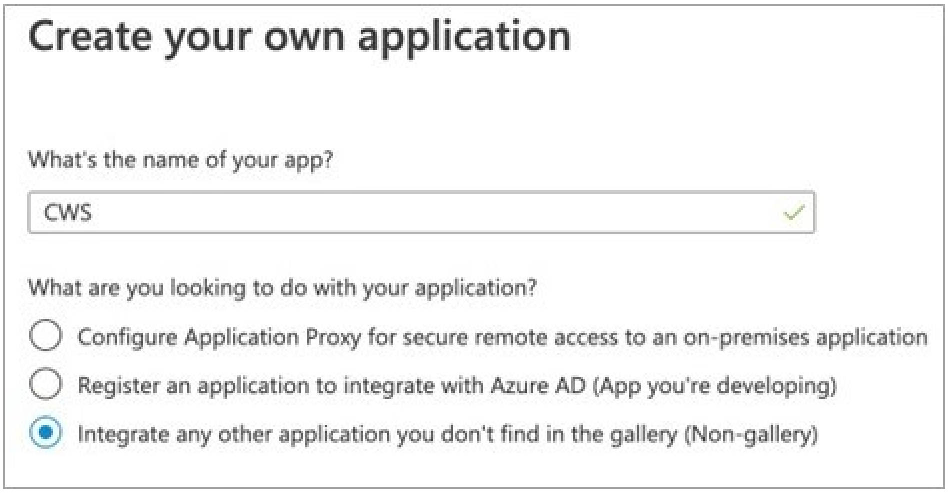
Try out the new Enterprise Apps search preview! Click to enable the preview. →

5 Click on **Create Your Own Application** at the top of the **New Application** panel.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > NBarrett Lab AAD > Enterprise applications >
Browse Azure AD Gallery
+ Create your own application
Request new gallery app
Got feedback?

You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

6 Enter a name (for example, CWS) and ensure that the **Non-gallery** radio option is selected.



Create your own application

What's the name of your app?

CWS

What are you looking to do with your application?

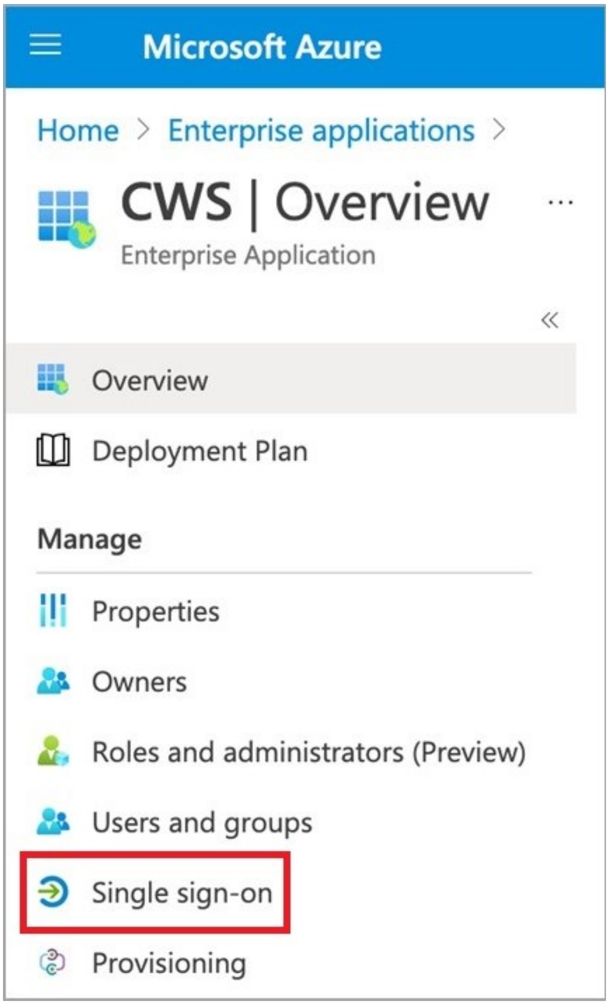
○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

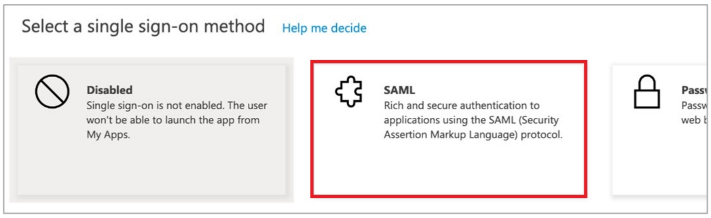
● Integrate any other application you don't find in the gallery (Non-gallery)

7 Click **Create** at the bottom of the **Create Your Own Application** form.

8 Click on the **Single sign-on** panel using the left-side panel of your Cloud Web Security (CWS) Enterprise application page.



9 Click **SAML** (Security Assertion Markup Language) as your **single sign-on method** of choice.



Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

10 Fill in section (1) using the upper-right edit pencil icon as shown below. After entering all the required details, click **Save** at the top of the pop-over pane.

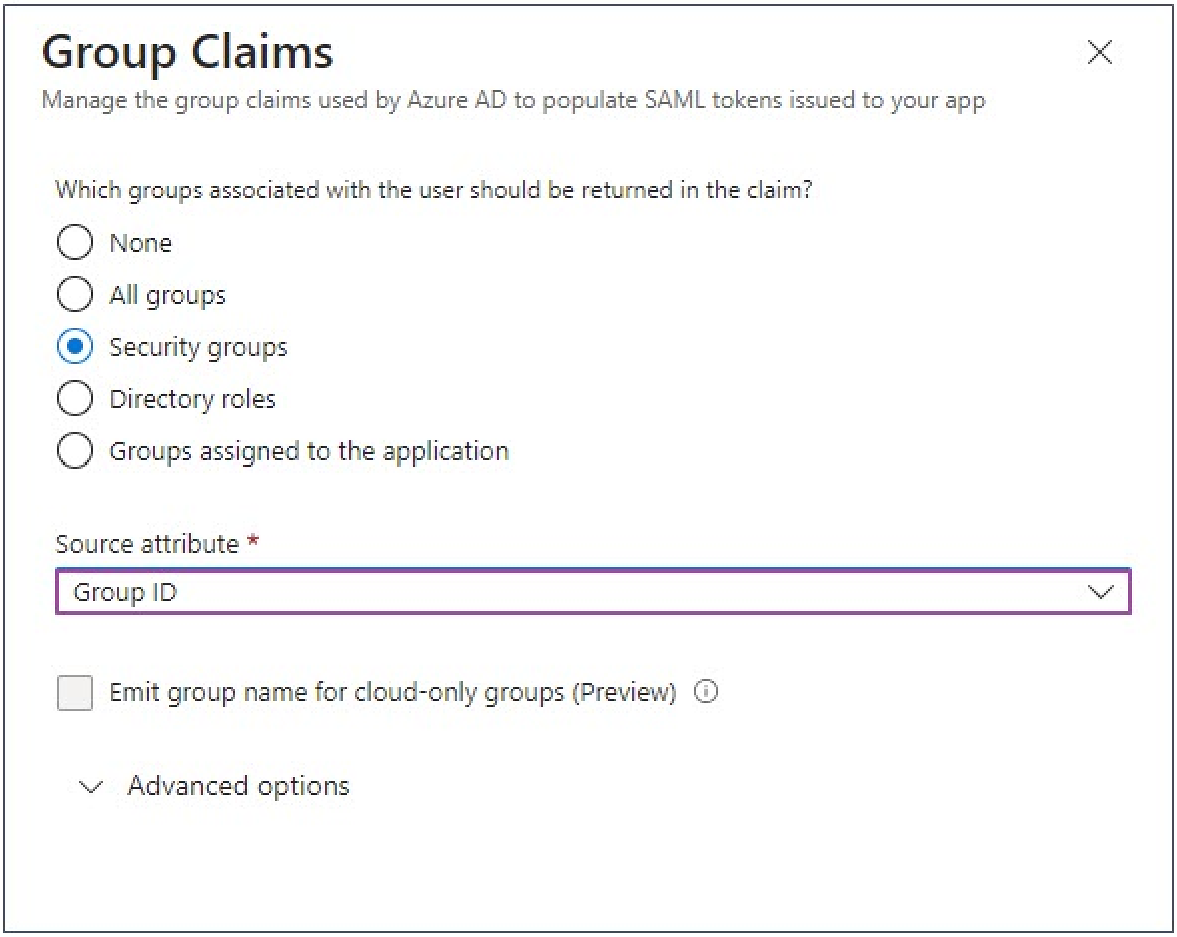
Field Name	Field Value	Field Description
Identifier (Entity ID)	https://safe-cws-sase.vmware.com/safeview-auth-server/saml/metadata	Azure AD allows multiple values. Set it to this value and select t **Default** check box for it. This is the Entity ID that Cloud Web Se will present itself as in the SAML **AuthRequest** message.
Reply URL (ACS URL)	https://safe-cws-sase.vmware.com/safeview-auth-server/saml	This is the URL that Azure AD will redirect the SAML assertion payload to. This is how Cloud Web Security learns that users ar authenticated successfully.
Sign-on URL	https://safe-cws-sase.vmware.com/safeview-auth-server/saml	This is used for Azure AD initiating authentication into Cloud We Security (versus Cloud Web Security redirecting to Azure AD). not typically used.

11 Copy the following items from section (3) and (4) into a text editor (for example, Windows Notepad or Mac TextEdit).

Field Name	Field Description
Section (3) - Certificate (Base64)	This is the public key of the key-pair used by Azure AD to sign SAML assertions. It allows Cloud Web Security to validate the assertions were truly created by this Azure AD integration. Download this fil and keep its contents handy. It should start with -----BEGIN CERTIFICATE----- and end with -----END CERTIFICATE-----.
Section (4) - Azure AD Identifier	This is the SAML **entityID** for the Azure AD IdP. In the payload of the Reply URL (see step 10), this indicates to Cloud Web Security that the SAML assertion came from this Azure AD integration.
Section (4) - Login URL	This is the Azure AD login URL that Cloud Web Security will redirect to in order to allow users to logi Azure AD (if they are not already logged in).

12 Click on the pencil icon in the upper-right corner of **User Attributes & Claims**.

13 Add a **Group Claim** using the following setting. Select the “Group ID” as source attribute.



Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

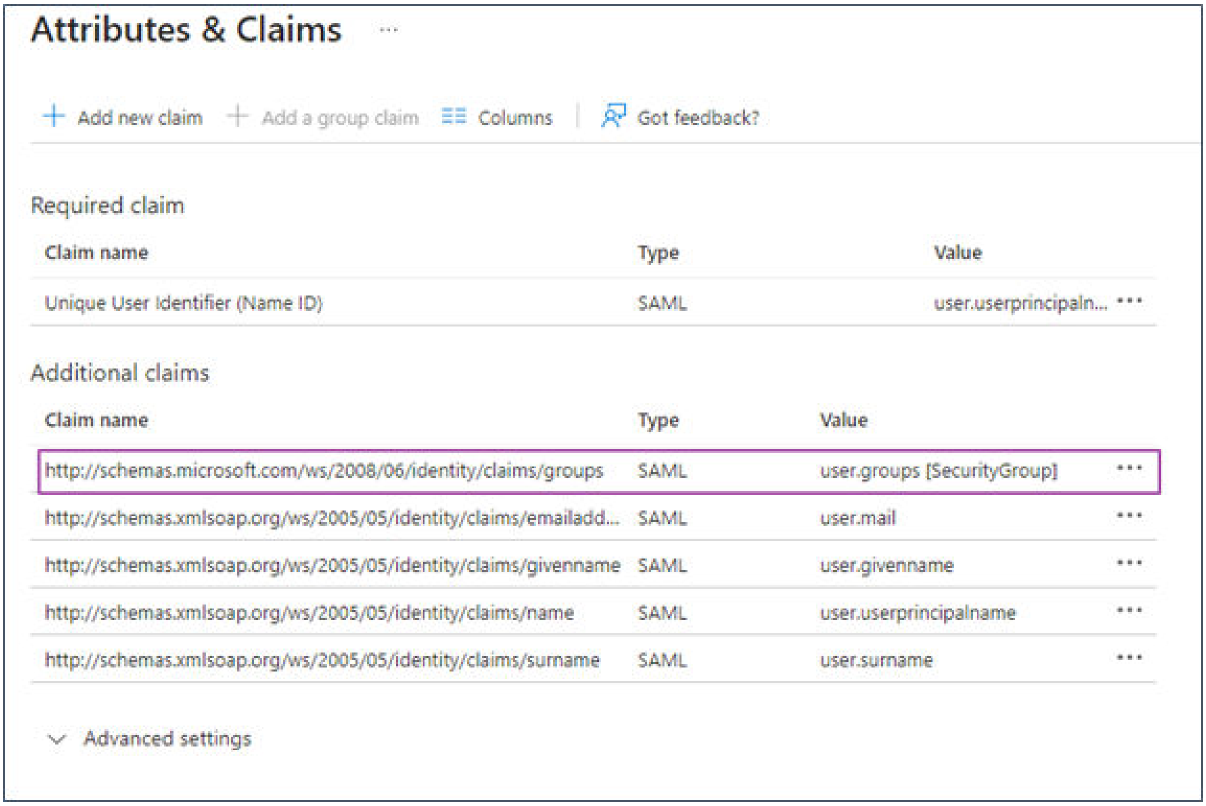
○ None
○ All groups
● Security groups
○ Directory roles
○ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups (Preview)

In the **Attribute & Claims** window, the group claim is added.



Required claim

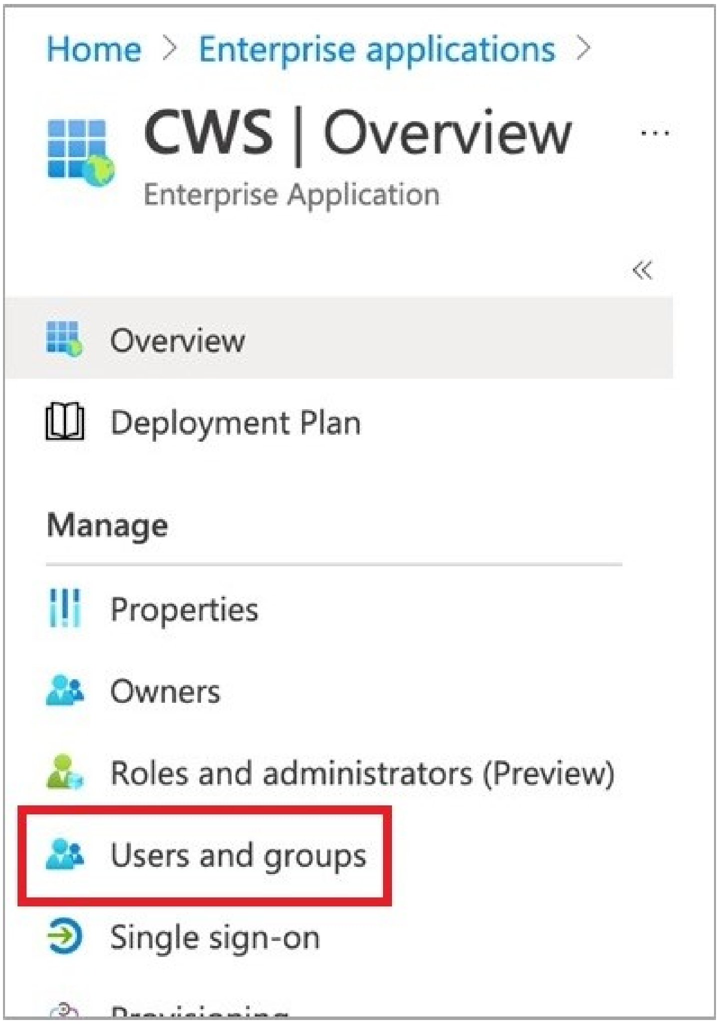
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipaln... ···

Additional claims

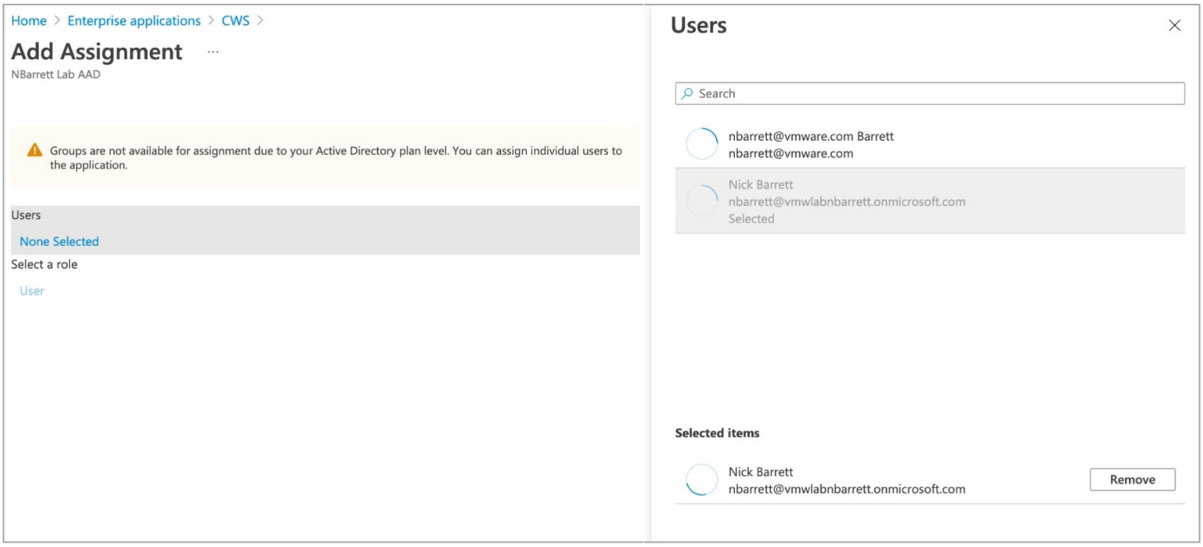
Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [SecurityGroup] ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ···
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ···

14 The Azure AD SAML configuration is now complete.

15 Click into the **Users and Groups** section of the Cloud Web Security **Enterprise applications** page.



16 Select users and/or groups that should be allowed access into the Cloud Web Security application. Then click **Assign**.



Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

nbarrett@vmware.com Barrett
nbarrett@vmware.com

Nick Barrett
nbarrett@vmwlabnbarrett.onmicrosoft.com
Selected

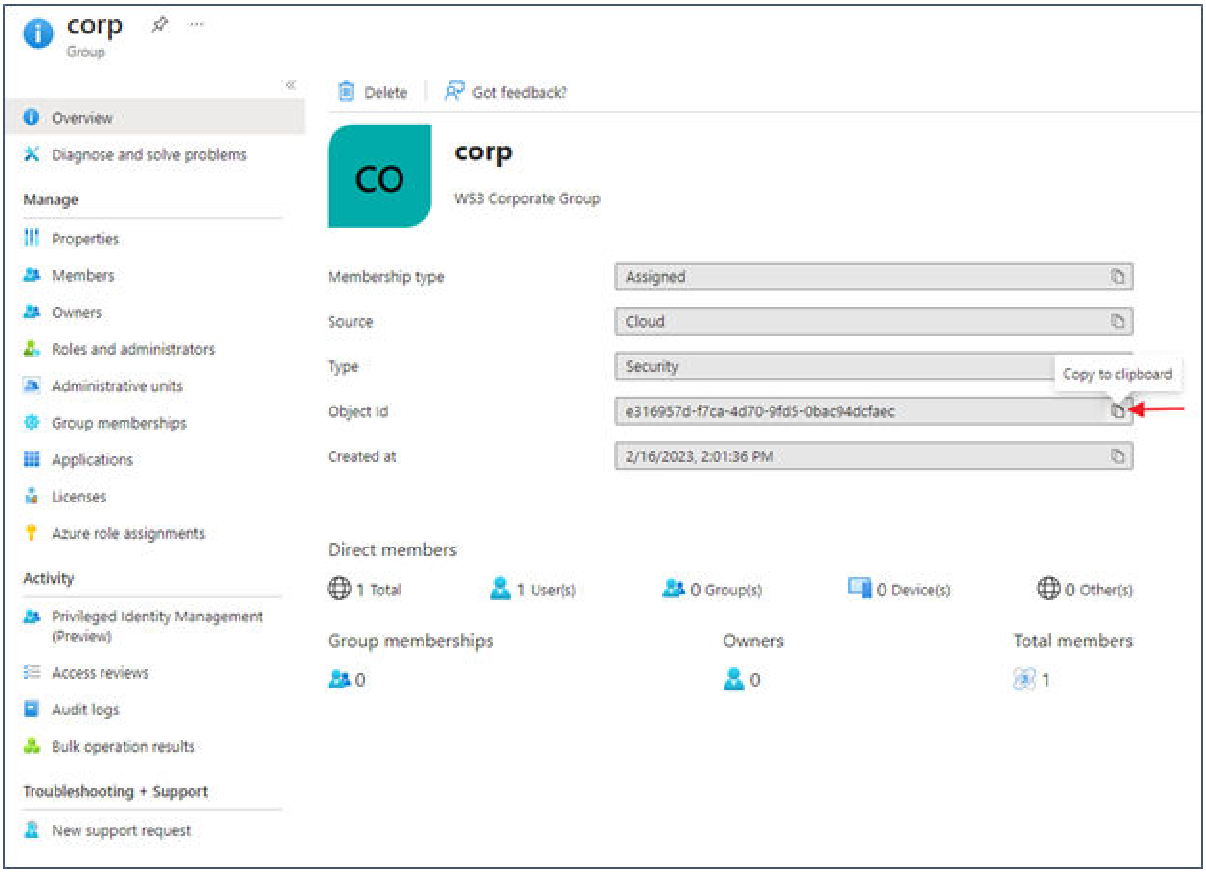
Nick Barrett
nbarrett@vmwlabnbarrett.onmicrosoft.com

Important

- If this step is not done, users will be shown an error that the application is not approved for them when they attempt to authenticate in the Cloud Web Security workflow.
- Groups are only an option if users have an upgraded Azure Active Directory P1 or P2 tenant. The default AD plan level will only allow assigning individual users to the application.

17 In the Azure portal, navigate to **Azure Active Directory** > **Groups** and select the group name to display the group properties. Copy the **Object ID** value from the Azure Group.

Note To use the Azure Group in the CWS Policy, you would need to obtain the Object ID for an Azure Group.



Membership type: Assigned

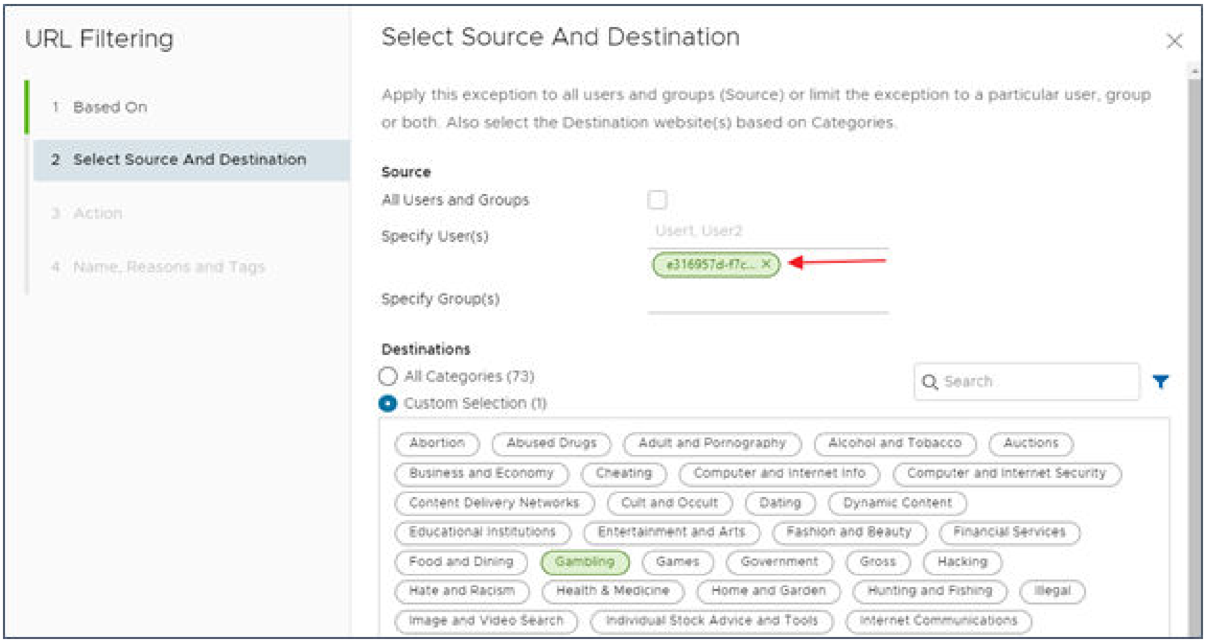
Source: Cloud

Type: Security

Object Id: e316957d-f7ca-4d70-9fd5-0bac94dcfaec

Created at: 2/16/2023, 2:01:36 PM

Use the **Object ID** to specify the Azure Group you would want to match on in a CWS policy. In the following example, the Azure AD group “**corp**” is matched on a URL filtering policy for the **Gambling** category.


URL Filtering
1 Based On
2 Select Source And Destination
3 Action
4 Name, Reasons and Tags
Select Source And Destination
×

Apply this exception to all users and groups (Source) or limit the exception to a particular user, group or both. Also select the Destination website(s) based on Categories.

Source

All Users and Groups ☐

Specify User(s): User1, User2

e316957d-f7c... ×

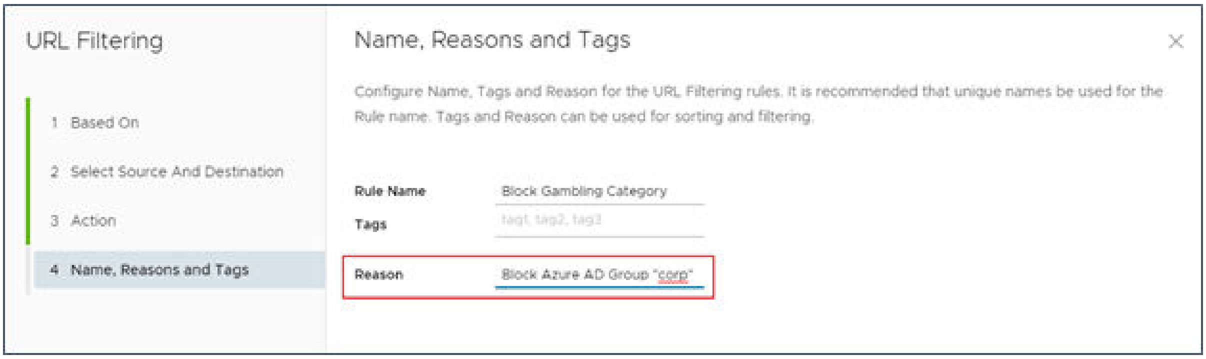
Specify Group(s)

Destinations

○ All Categories (73)

● Custom Selection (1)

To avoid confusion, it is also advisable to include information in the **Reason** field of the CWS policy that references back to the original Azure Group name. In the following example, refer to “**corp**” group or create a tag.



Configure Name, Tags and Reason for the URL Filtering rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering.

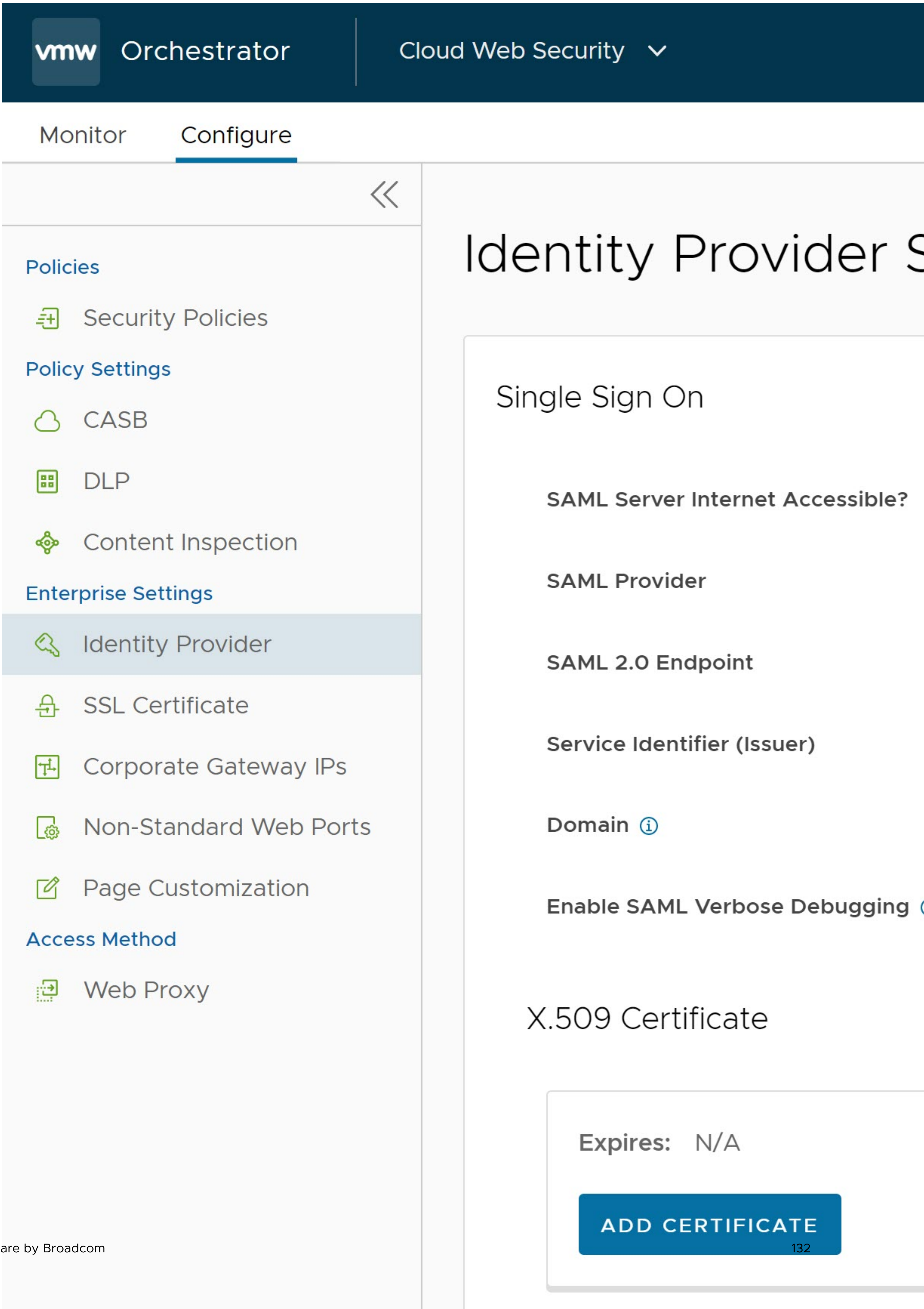
Rule Name: Block Gambling Category

Tags: tag1, tag2, tag3

Reason: Block Azure AD Group "corp"

VMware Cloud Orchestrator Configuration

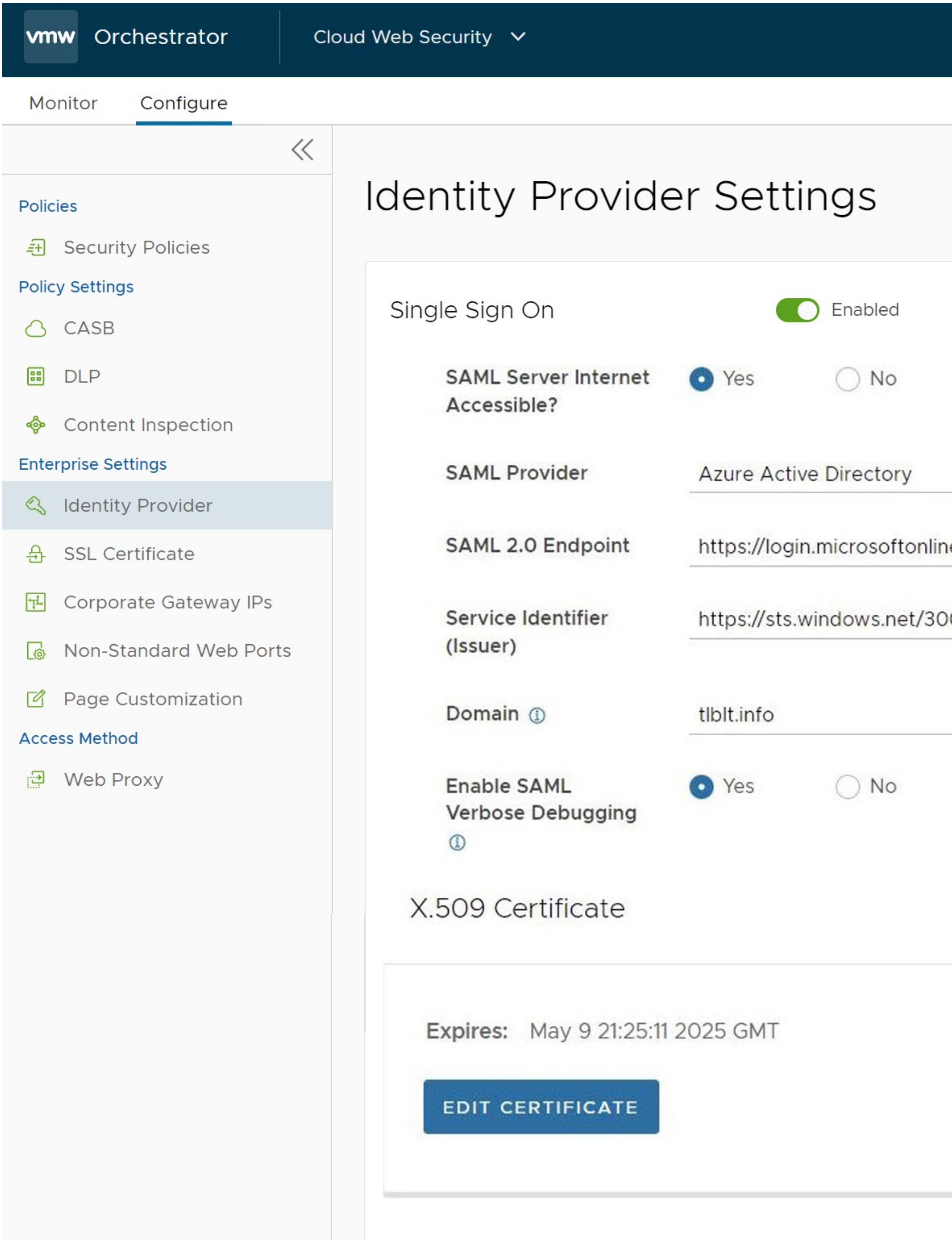
1. Log onto the Orchestrator UI.
2. Go to **Cloud Web Security** > **Configure** > **Enterprise Settings** > **Identity Provider**. The **Identity Provider Settings** page appears.
3. Toggle **Single Sign On** to **Enabled**.


vmw Orchestrator
Cloud Web Security
Monitor
Configure
Policies
Security Policies
Policy Settings
CASB
DLP
Content Inspection
Enterprise Settings
Identity Provider
SSL Certificate
Corporate Gateway IPs
Non-Standard Web Ports
Page Customization
Access Method
Web Proxy
Identity Provider S
Single Sign On
SAML Server Internet Accessible?
SAML Provider
SAML 2.0 Endpoint
Service Identifier (Issuer)
Domain
Enable SAML Verbose Debugging
X.509 Certificate
ADD CERTIFICATE

Expires: N/A

4 Configure the following details:

   - For **SAML Server Internet Accessible** select **Yes**
   - For **SAML Provider** select **Azure Active Directory**
   - For **SAML 2.0 Endpoint**, copy the **Login URL** from your notepad application as per step 11 of the Azure AD configuration.
   - For **Service Identifier (Issuer)**, copy the **Azure AD Identifier** from your notepad application as per step 11 of the Azure AD configuration.
   - Activate **SAML Verbose Debugging** if needed.
     - This turns on debugging messages for a period of 2 hours, after which the debugging is deactivated automatically.
     - The SAML debug messages can be viewed in the Chrome Developer console.



Identity Provider Settings

Single Sign On Enabled

SAML Server Internet Accessible? ● Yes ○ No

SAML Provider: Azure Active Directory

SAML 2.0 Endpoint: https://login.microsoftonline

Service Identifier (Issuer): https://sts.windows.net/30

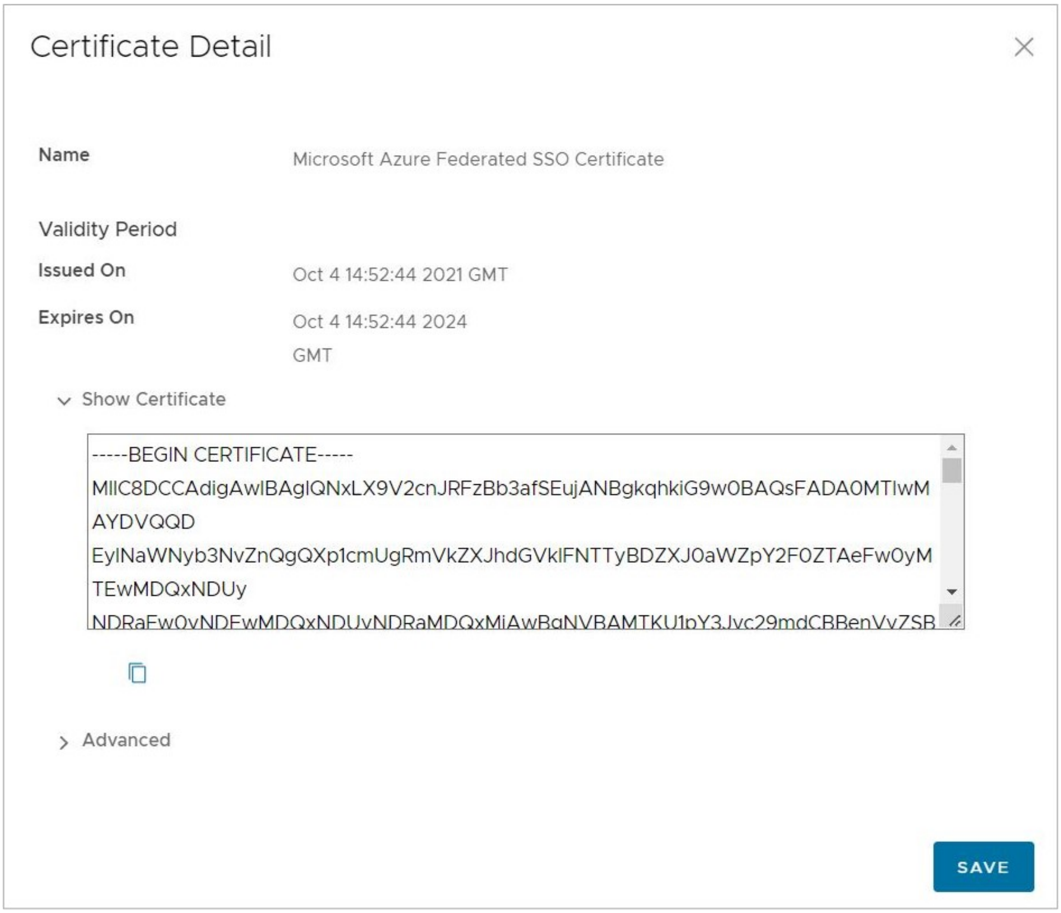
Domain: tlblt.info

Enable SAML Verbose Debugging: ● Yes ○ No

X.509 Certificate

Expires: May 9 21:25:11 2025 GMT

- Under the **X.509 Certificate** section, click on **Add Certificate** and copy the certificate from the notepad application as per step 11 of the Azure AD configuration and paste here, and then click **Save**.



Name: Microsoft Azure Federated SSO Certificate

Validity Period

Issued On: Oct 4 14:52:44 2021 GMT

Expires On: Oct 4 14:52:44 2024 GMT

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdigAwIBAgIQNxLX9V2cnJRFzBb3afSEujANBgkqhkiG9w0BAQsFADA0MTIwM
AYDVQQD
EyINaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yM
TEwMDQxNDUy
NDRaFw0yNDEwMDQxNDUyNDRaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSB
```

- Finally, click **Save Changes** to complete the configuration changes on the **Configure Authentication** screen.

5 Add an SSL Bypass rule for the Workspace ONE Access domain by following the steps below:

   a Navigate to **Cloud Web Security > Configure > Security Policies**.

   b Select an existing policy to add SSL Bypass rule and click the **Edit** button.

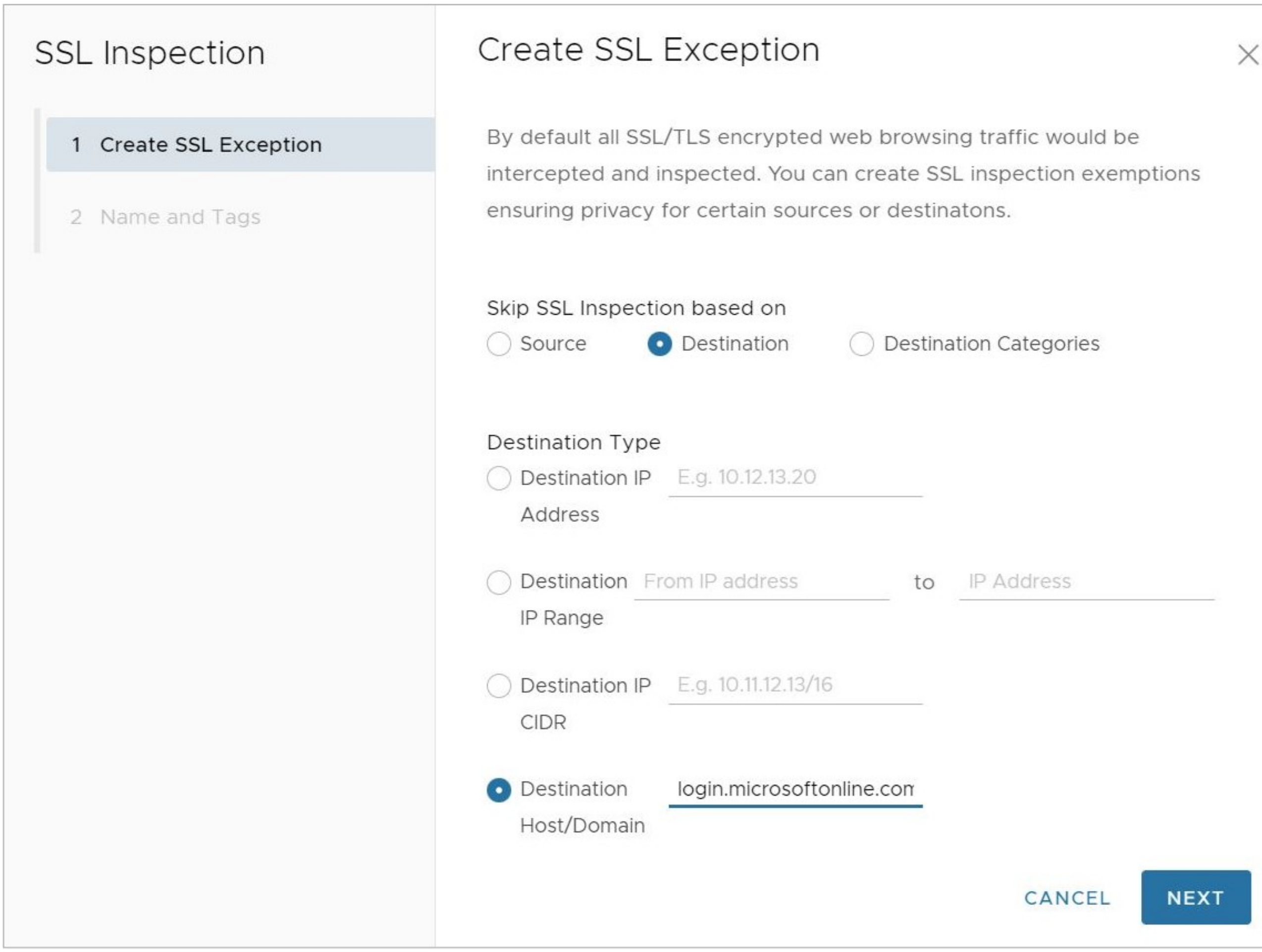
   c Click the **SSL Inspection** tab and click **+ Add Rule**. The **Create SSL Exception** screen appears.

   d In the **Create SSL Exception** screen, configure the following and click **Next**:

      - For **Skip SSL Inspection based on**, select **Destination**.
      - For **Destination Type**, select **Destination Host/Domain**.
      - For **Domain**, enter any one of the following domains:
         - login.microsoftonline.com

- sts.windows.net
- microsoftonline-p.com
- msauth.net
- msftauth.net

.



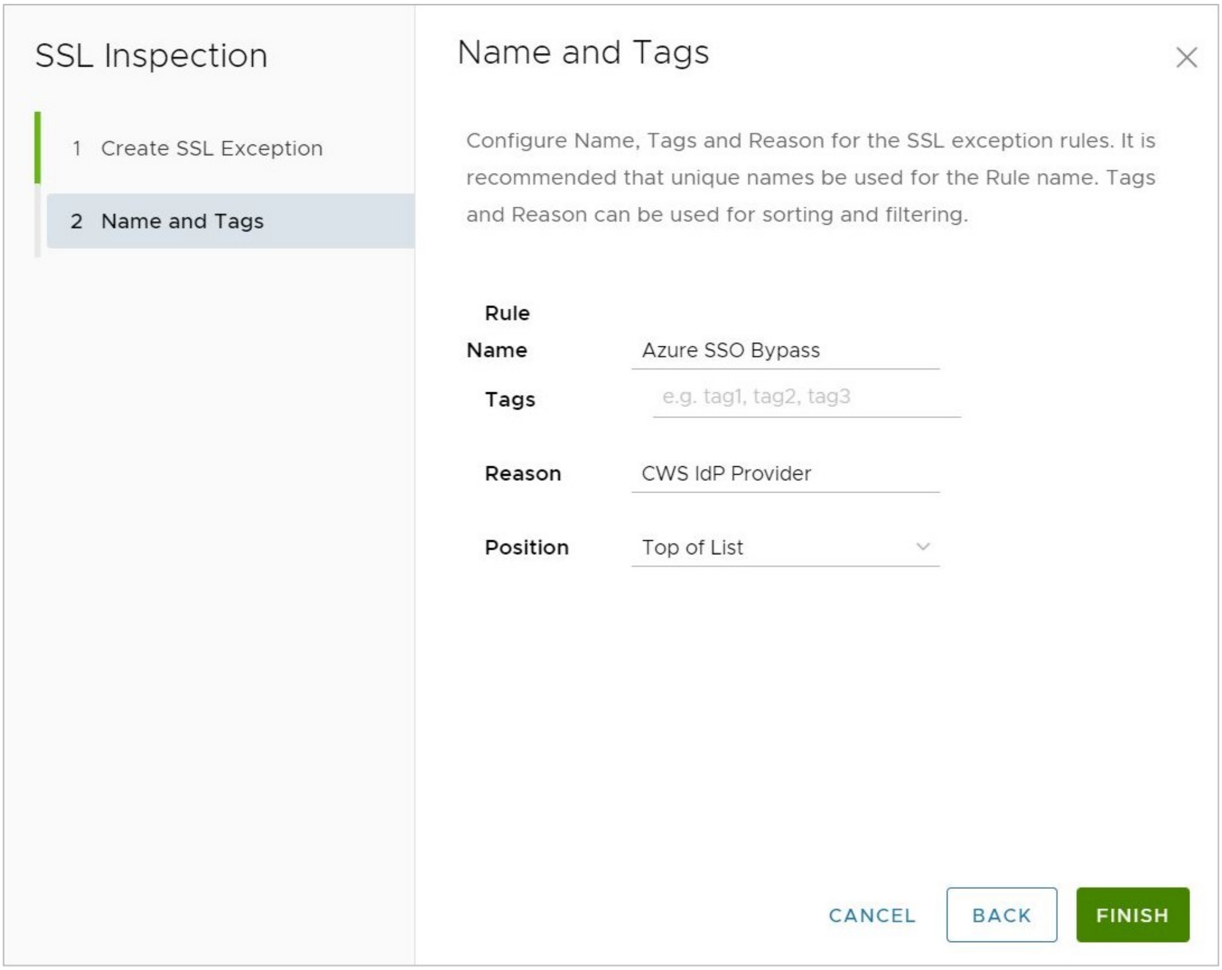
Create SSL Exception

By default all SSL/TLS encrypted web browsing traffic would be intercepted and inspected. You can create SSL inspection exemptions ensuring privacy for certain sources or destinatons.

Skip SSL Inspection based on
○ Source ● Destination ○ Destination Categories

Destination Type
○ Destination IP Address: E.g. 10.12.13.20
○ Destination IP Range: From IP address to IP Address
○ Destination IP CIDR: E.g. 10.11.12.13/16
● Destination Host/Domain: login.microsoftonline.con

e In the **Name and Tags** screen, enter a unique name for the rule and add a reason, if needed.



Name and Tags

Configure Name, Tags and Reason for the SSL exception rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering.

Rule Name: Azure SSO Bypass

Tags: e.g. tag1, tag2, tag3

Reason: CWS IdP Provider

Position: Top of List

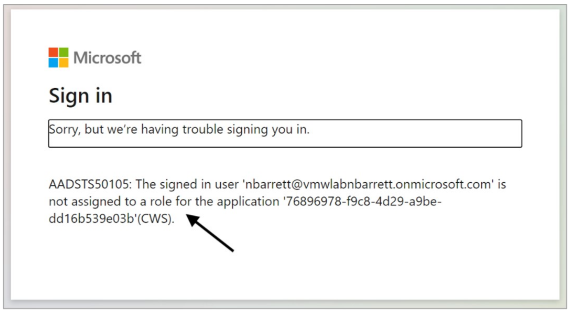
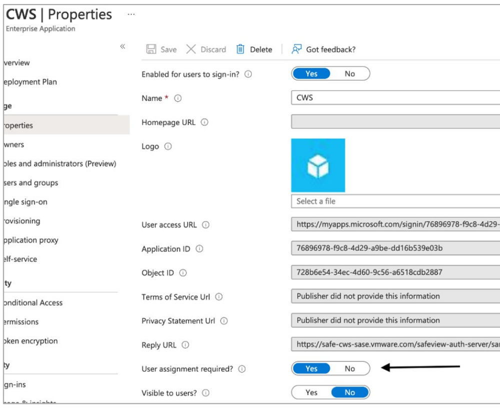
f Click **Finish**, and then **Publish** the applicable Security Policy to apply this new rule.

Important The domain **login.microsoftonline.com** is part of the **Microsoft 365** group of domains as found in the document: Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended. If users have already configured an SSL Bypass rule which includes the full **Microsoft 365** domain group, users can skip this step. If users attempt to configure the above rule while also having the full Microsoft 365 domain group included in an existing SSL Bypass rule, the new rule will throw an error as a unique domain may not be duplicated in multiple SSL bypass rules.

For more information on domains that should have SSL Bypass rules configured, consult Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended.

Troubleshooting

This section covers potential issues with your Azure AD IdP for Cloud Web Security configuration.

Problem	Proposed Solution
Users are getting the following error message when authenticating:  Microsoft Sign in Sorry, but we're having trouble signing you in. AADSTS50105: The signed in user 'nbarrett@vmwlabnbarrett.onmicrosoft.com' is not assigned to a role for the application '76896978-f9c8-4d29-a9be-dd16b539e03b'(CWS).	■ Ensure that all users are assigned to the CWS En ■ Requiring user assignment can be deactivated in tab in Azure AD. ■ They can also be in a group that is assigned to th has appropriate licensing. ■ https://docs.microsoft.com/en-us/azure/active-d access-portal  CWS | Properties Enterprise Application Enabled for users to sign-in? Yes Name * CWS User access URL https://myapps.microsoft.com/signin/76896978-f9c8-4d29- Application ID 76896978-f9c8-4d29-a9be-dd16b539e03b Object ID 728b6e54-34ec-4d60-9c56-a6518cdb2887 Terms of Service Url Publisher did not provide this information Privacy Statement Url Publisher did not provide this information Reply URL https://safe-cws-sase.vmware.com/safeview-auth-server/sa User assignment required? Yes Visible to users? No

Configuring Workspace ONE Access as an Identity Provider (IdP) with VMware Cloud Web Security

This section covers configuring Workspace ONE Access as an Identity Provider (IdP) for VMware Cloud Web Security. We first cover the Workspace ONE configuration, and then the VMware Cloud Orchestrator configuration.

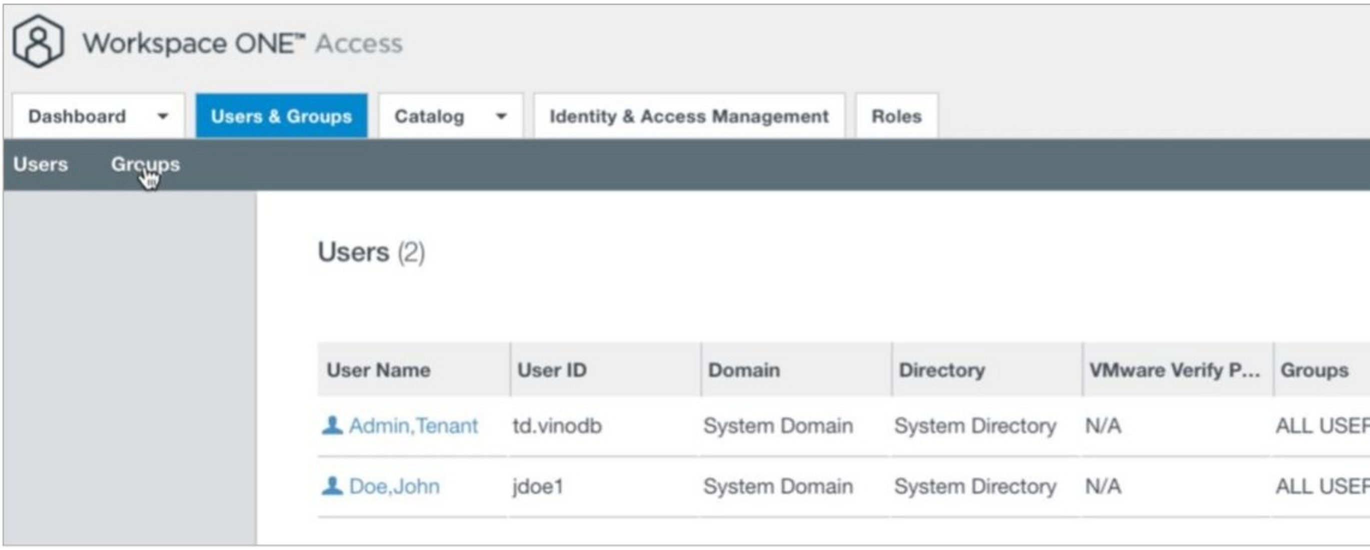
Prerequisites

Users need the following to configure Workspace ONE as an identity provider with VMware Cloud Web Security:

1. A Workspace ONE account.
2. A customer Enterprise on a production VMware Cloud Orchestrator with Cloud Web Security activated. The Orchestrator must use Release 4.5.0 or later.

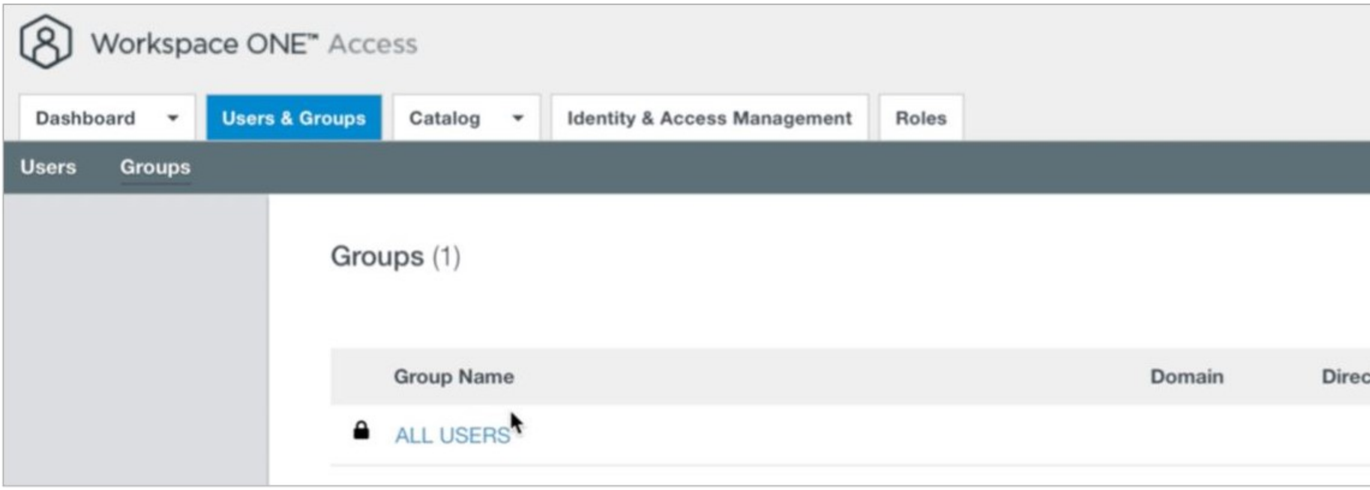
Workspace ONE Access Configuration

1. Create Users and Groups. Associate the users to the group.



Users (2)

User Name	User ID	Domain	Directory	VMware Verify P...	Groups
Admin,Tenant	td.vinodb	System Domain	System Directory	N/A	ALL USEF
Doe,John	jdoe1	System Domain	System Directory	N/A	ALL USEF



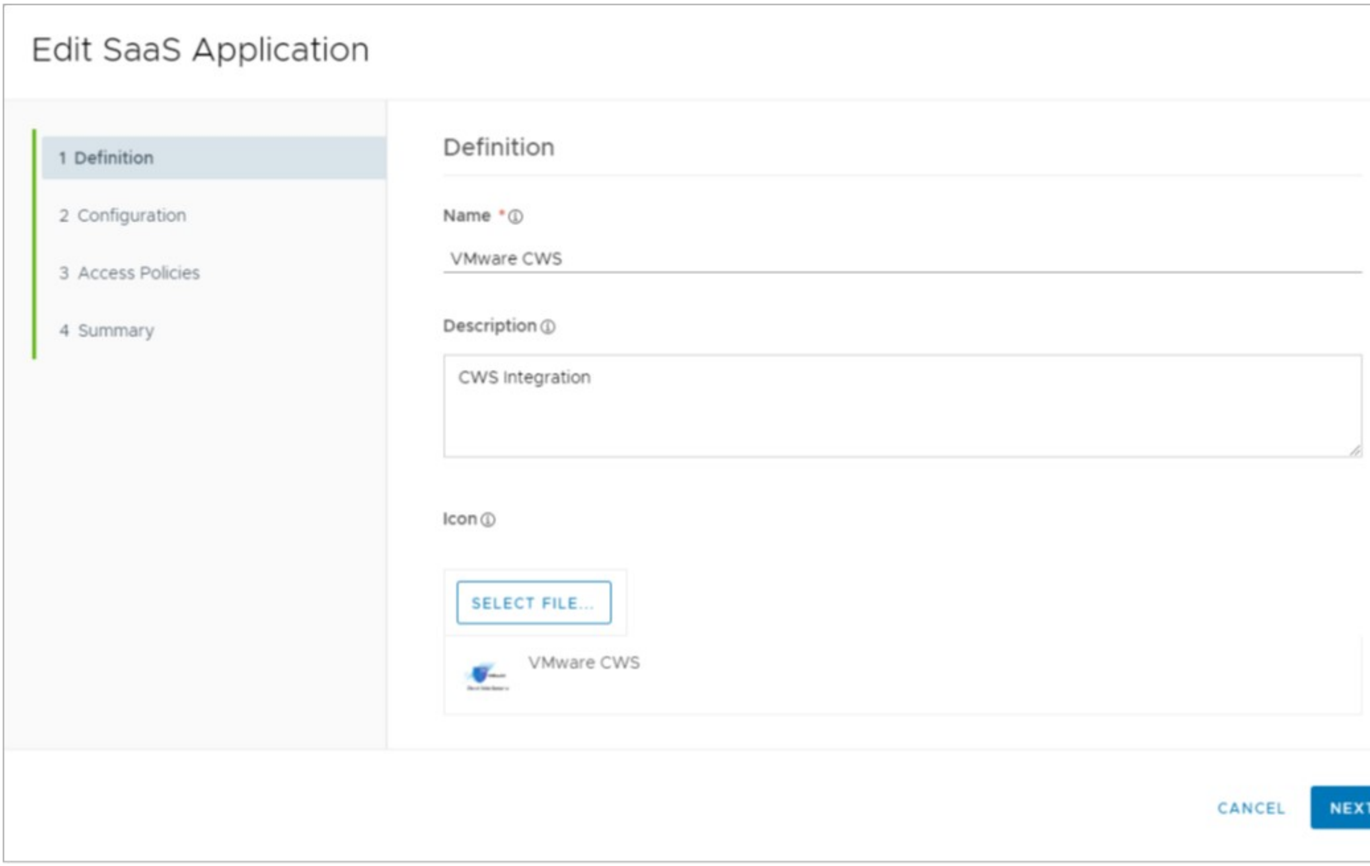
Groups (1)

Group Name	Domain	Direc
ALL USERS		

2 Go to **Catalog > Web Apps**.

3 Click on **New** to add a **New Application**.

4 Name the Application as VMware CWS and click **Next**.



Name * ⓘ
VMware CWS

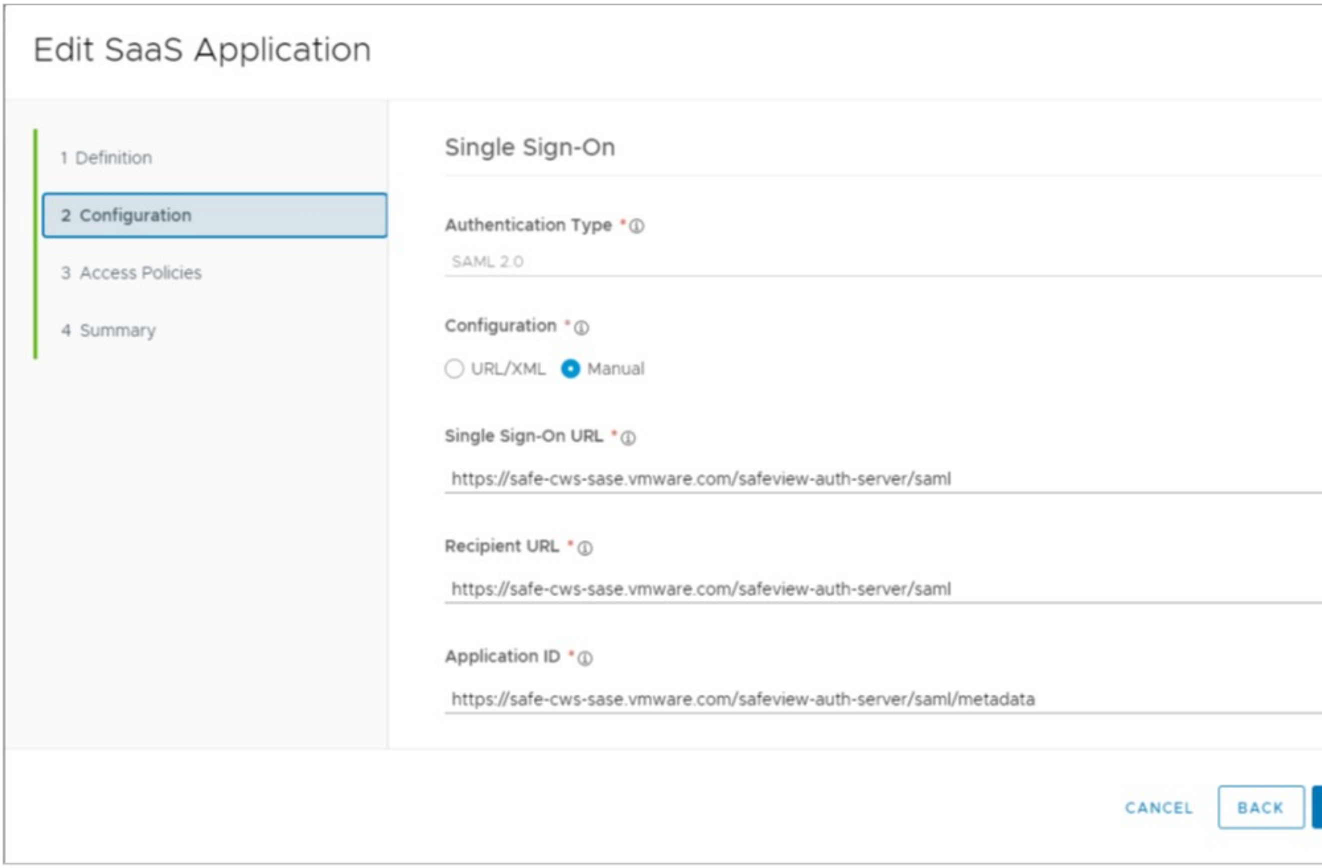
Description ⓘ
CWS Integration

VMware CWS

5 On the **Configuration** section:

   a Enter the following details for Single Sign-On:

      - Authentication Type: SAML 2.0
      - Configuration: Manual
      - Single Sign-On URL: https://safe-cws-sase.vmware.com/safeview-auth-server/saml
      - Recipient URL: https://safe-cws-sase.vmware.com/safeview-auth-server/saml
      - Application ID: https://safe-cws-sase.vmware.com/safeview-auth-server/saml/metadata
      - Username Format: Email Address (name@domain.com)
      - Username Value: ${user.email}



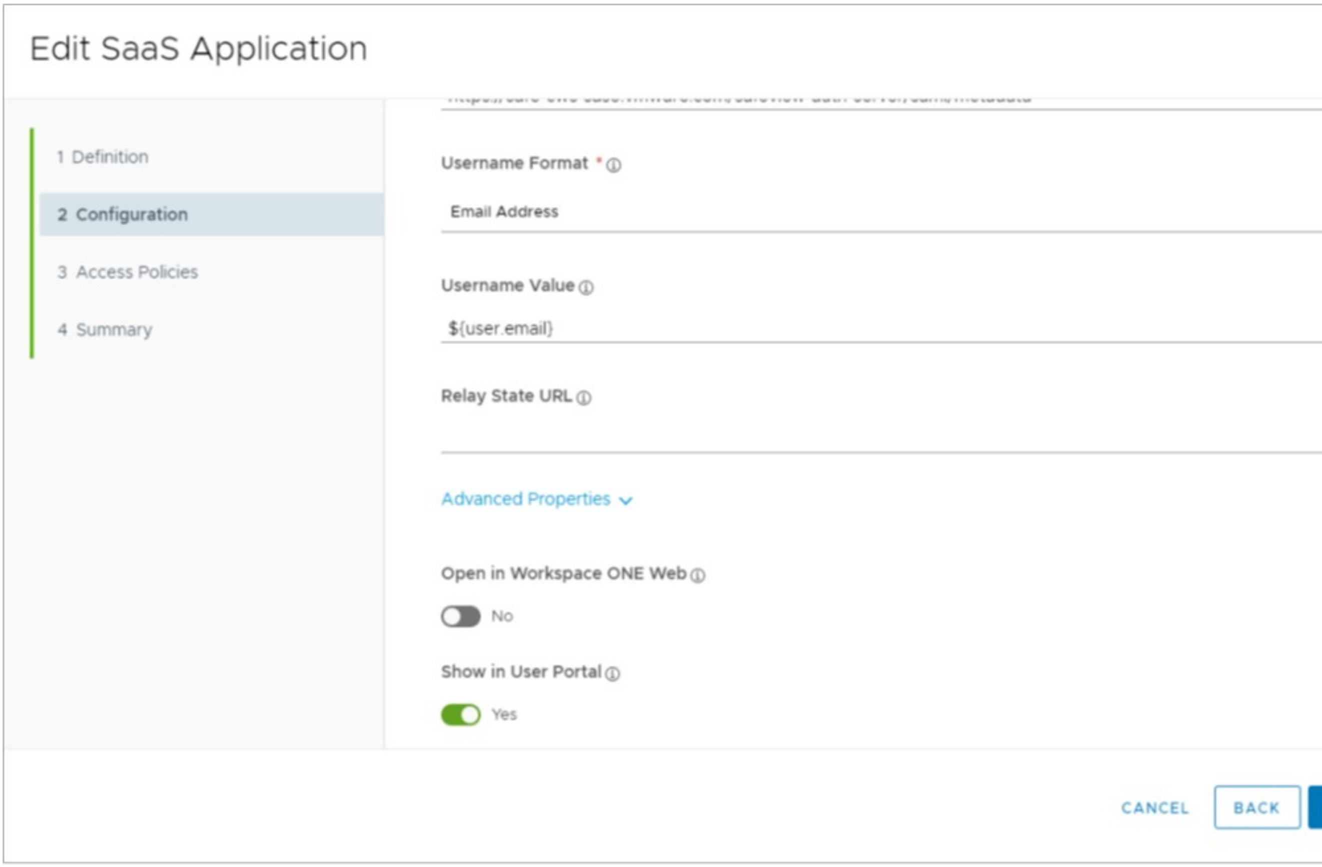
Authentication Type * SAML 2.0

Configuration * ○ URL/XML ● Manual

Single Sign-On URL * https://safe-cws-sase.vmware.com/safeview-auth-server/saml

Recipient URL * https://safe-cws-sase.vmware.com/safeview-auth-server/saml

Application ID * https://safe-cws-sase.vmware.com/safeview-auth-server/saml/metadata



Edit SaaS Application

Username Format * ⓘ: Email Address

Username Value ⓘ: ${user.email}

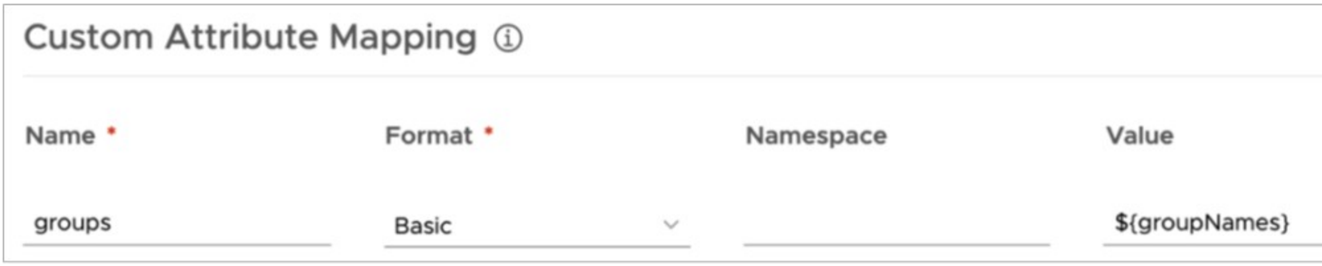
Relay State URL ⓘ:

Open in Workspace ONE Web ⓘ: No

Show in User Portal ⓘ: Yes

b Click on **Advanced Properties** and Add a **Custom Attribute Mapping** as below. This configuration is to send groups attribute in SAML assertion.

Note The Name must be "groups" and the Value is ${groupNames}.

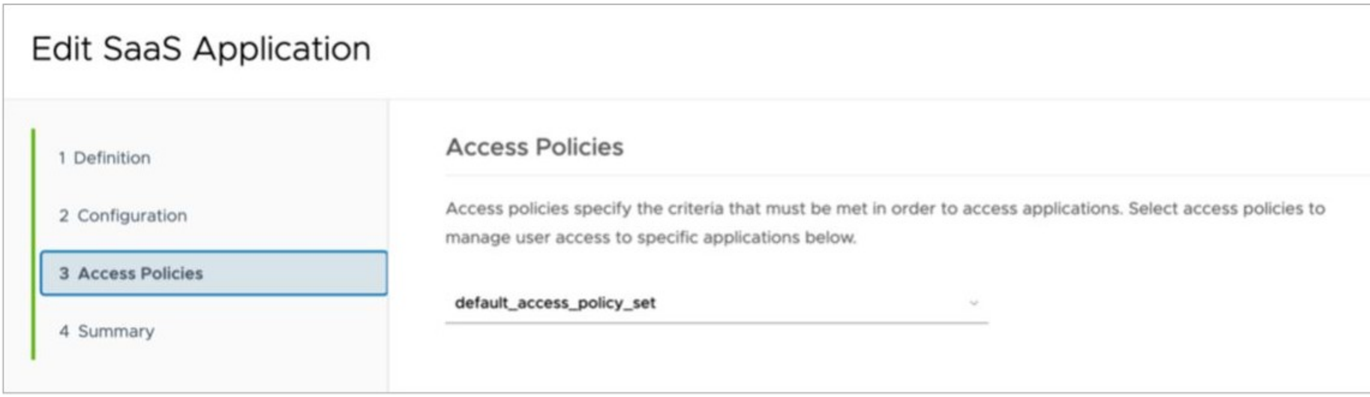


Custom Attribute Mapping ⓘ

Name *	Format *	Namespace	Value
groups	Basic		${groupNames}

c Click **Next**.

6 On the **Access Policies** page, “default_access_policy_set” is automatically selected.



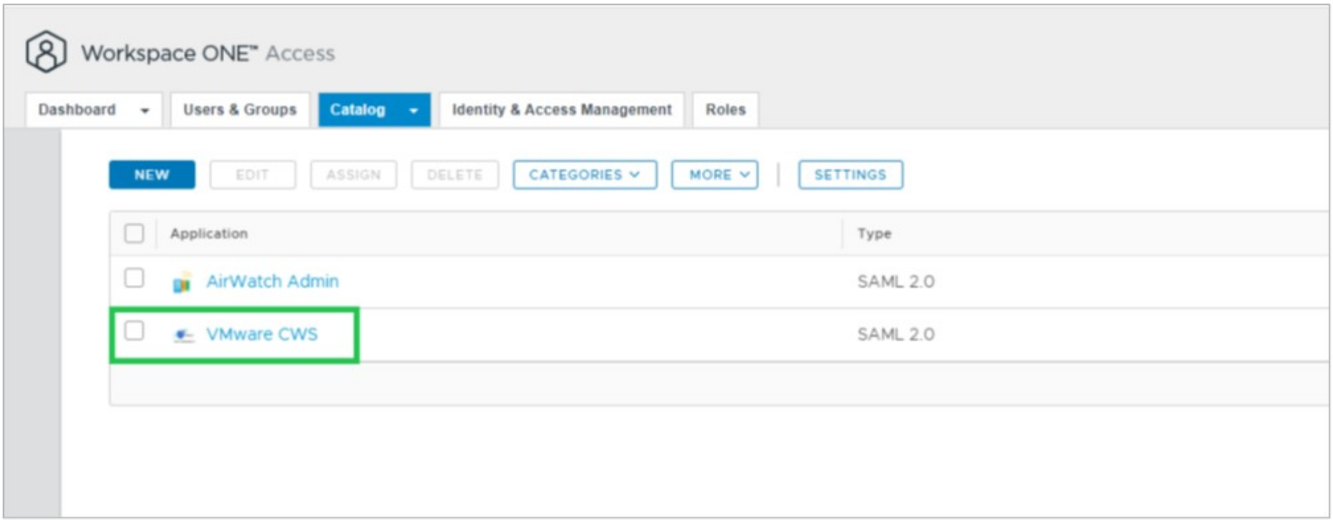
Edit SaaS Application

Access Policies

Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.

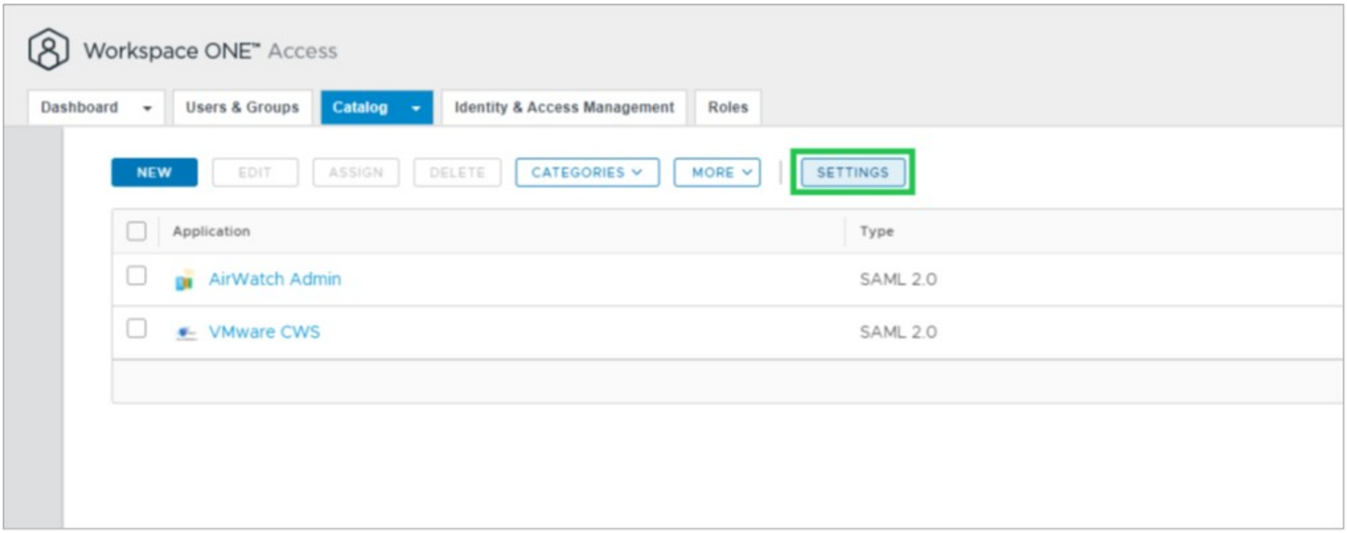
default_access_policy_set

7 Click **Next** and Click **Save and Assign**.



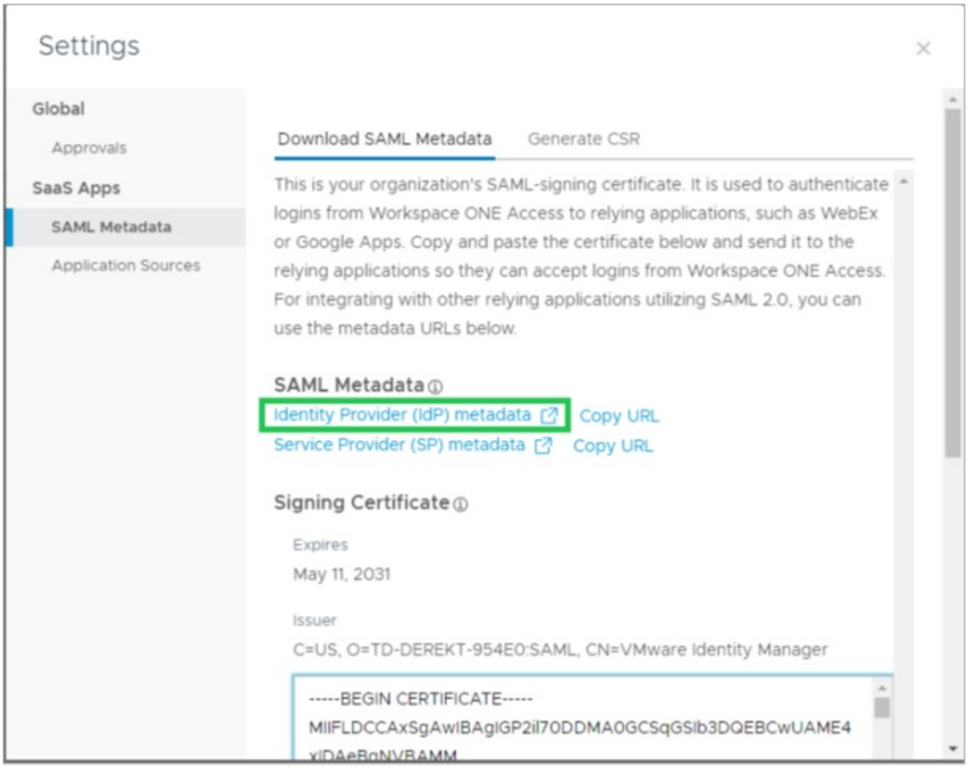
☐ Application	Type
☐ AirWatch Admin	SAML 2.0
☐ VMware CWS	SAML 2.0

8 Under **Catalog** > **Web Apps** >, click on **Settings**.



☐ Application	Type
☐ AirWatch Admin	SAML 2.0
☐ VMware CWS	SAML 2.0

9 In the **Settings** window, go to the **SAML Metadata** section.



This is your organization's SAML-signing certificate. It is used to authenticate logins from Workspace ONE Access to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Workspace ONE Access. For integrating with other relying applications utilizing SAML 2.0, you can use the metadata URLs below.

SAML Metadata ⓘ

Identity Provider (IdP) metadata ↗ Copy URL

Service Provider (SP) metadata ↗ Copy URL

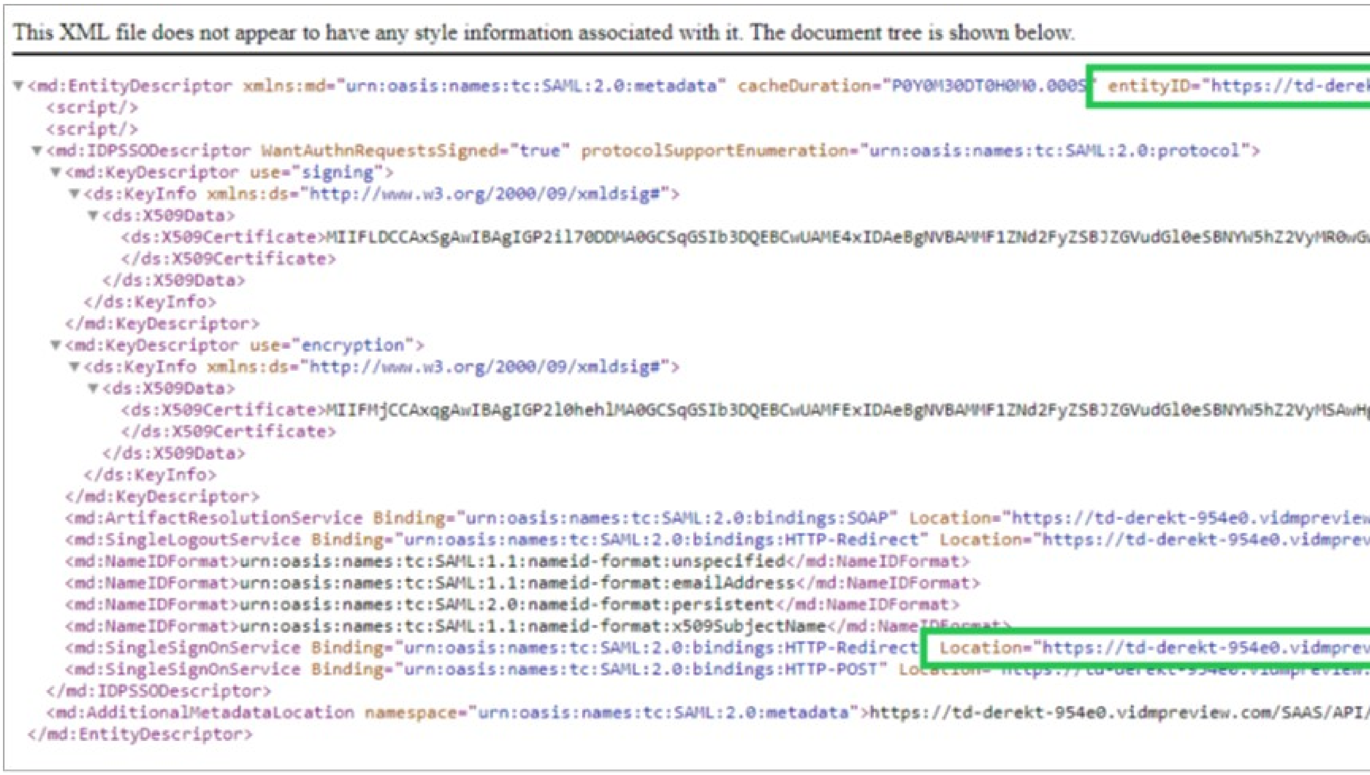
Signing Certificate ⓘ

Expires
May 11, 2031

Issuer
C=US, O=TD-DEREKT-954E0:SAML, CN=VMware Identity Manager

```
-----BEGIN CERTIFICATE-----
MIIFLDCCAxSgAwIBAgIGP2il70DDMA0GCSqGSIb3DQEBCwUAME4
xIDAeBgNVBAMM
```

10 Click on **Identity Provider (IdP) metadata**. This action opens a new window in your browser with XML data. Copy the "entityID" and "Location" URL into a notepad.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

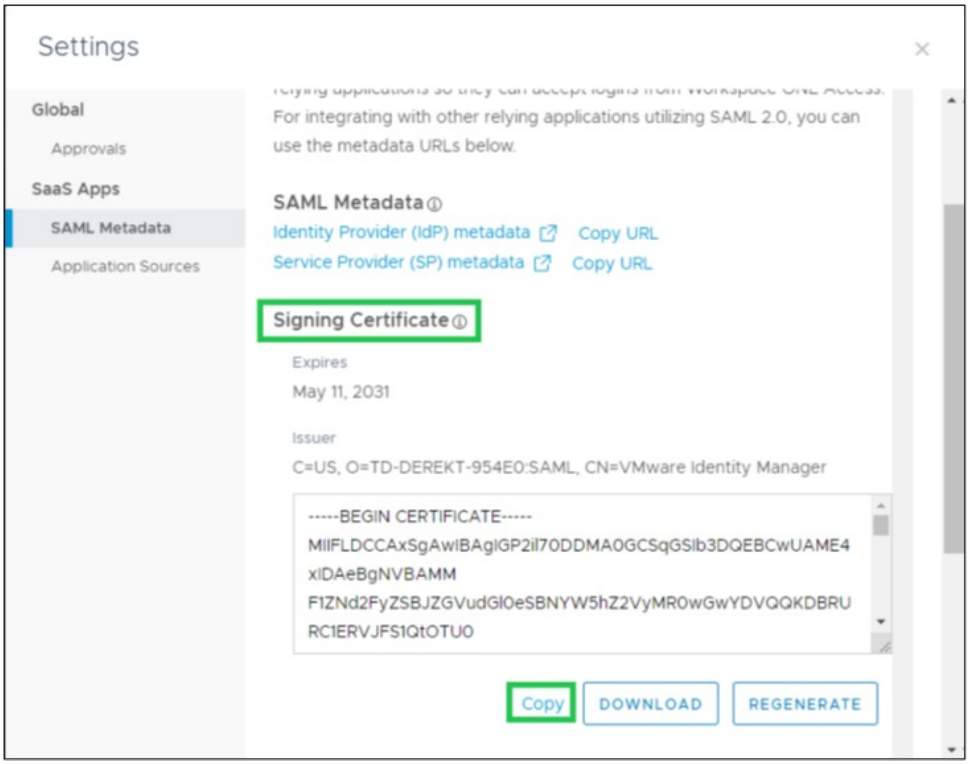
```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" cacheDuration="P0Y0M30DT0H0M0.000S" entityID="https://td-dere
   <script/>
   <script/>
 ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
   ▼<md:KeyDescriptor use="signing">
     ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       ▼<ds:X509Data>
          <ds:X509Certificate>MIIFLDCCAxSgAwIBAgIGP2il70DDMA0GCSqGSIb3DQEBCwUAME4xIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMR0w
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
   ▼<md:KeyDescriptor use="encryption">
     ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
       ▼<ds:X509Data>
          <ds:X509Certificate>MIIFMjCCAxqgAwIBAgIGP2l0hehlMA0GCSqGSIb3DQEBCwUAMFExIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMSAw
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://td-derekt-954e0.vidmpreview
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://td-derekt-954e0.vidmprev
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://td-derekt-954e0.vidmprev
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://td-derekt-954e0.vidmpreview.
  </md:IDPSSODescriptor>
  <md:AdditionalMetadataLocation namespace="urn:oasis:names:tc:SAML:2.0:metadata">https://td-derekt-954e0.vidmpreview.com/SAAS/API/
</md:EntityDescriptor>
```

- entityID: https://<ws1access_server>/SAAS/API/1.0/GET/metadata/idp.xml

- Location: https://<ws1access_server>/SAAS/auth/federation/sso

  where <ws1access-server> is the Workspace ONE Access server in your environment.

11 Go back to the **Setting** window and then copy the contents of **Signing Certificate** to the notepad.



For integrating with other relying applications utilizing SAML 2.0, you can use the metadata URLs below.

SAML Metadata

Identity Provider (IdP) metadata Copy URL

Service Provider (SP) metadata Copy URL

Signing Certificate

Expires

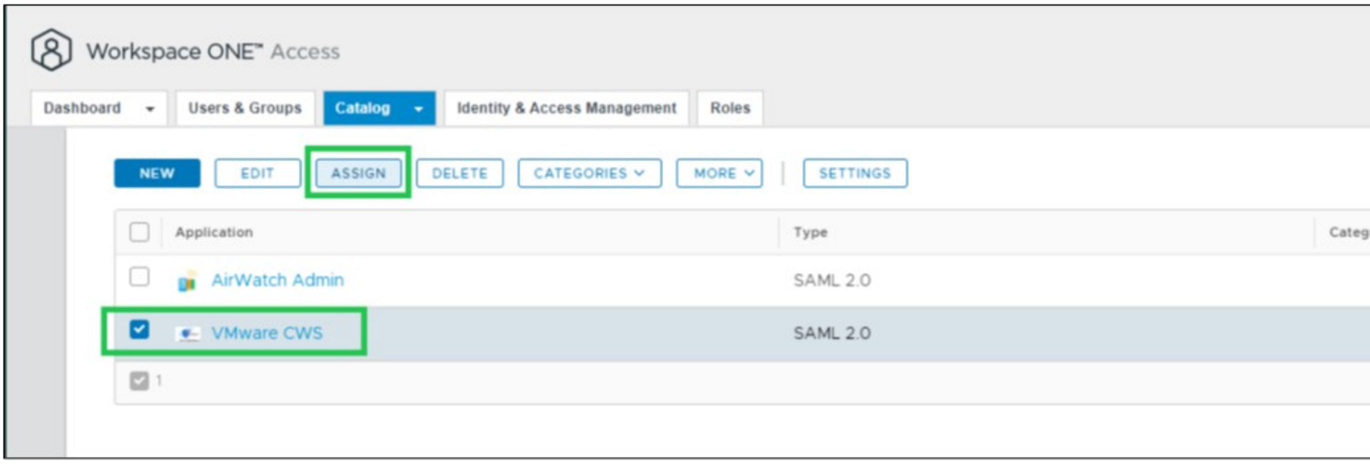
May 11, 2031

Issuer

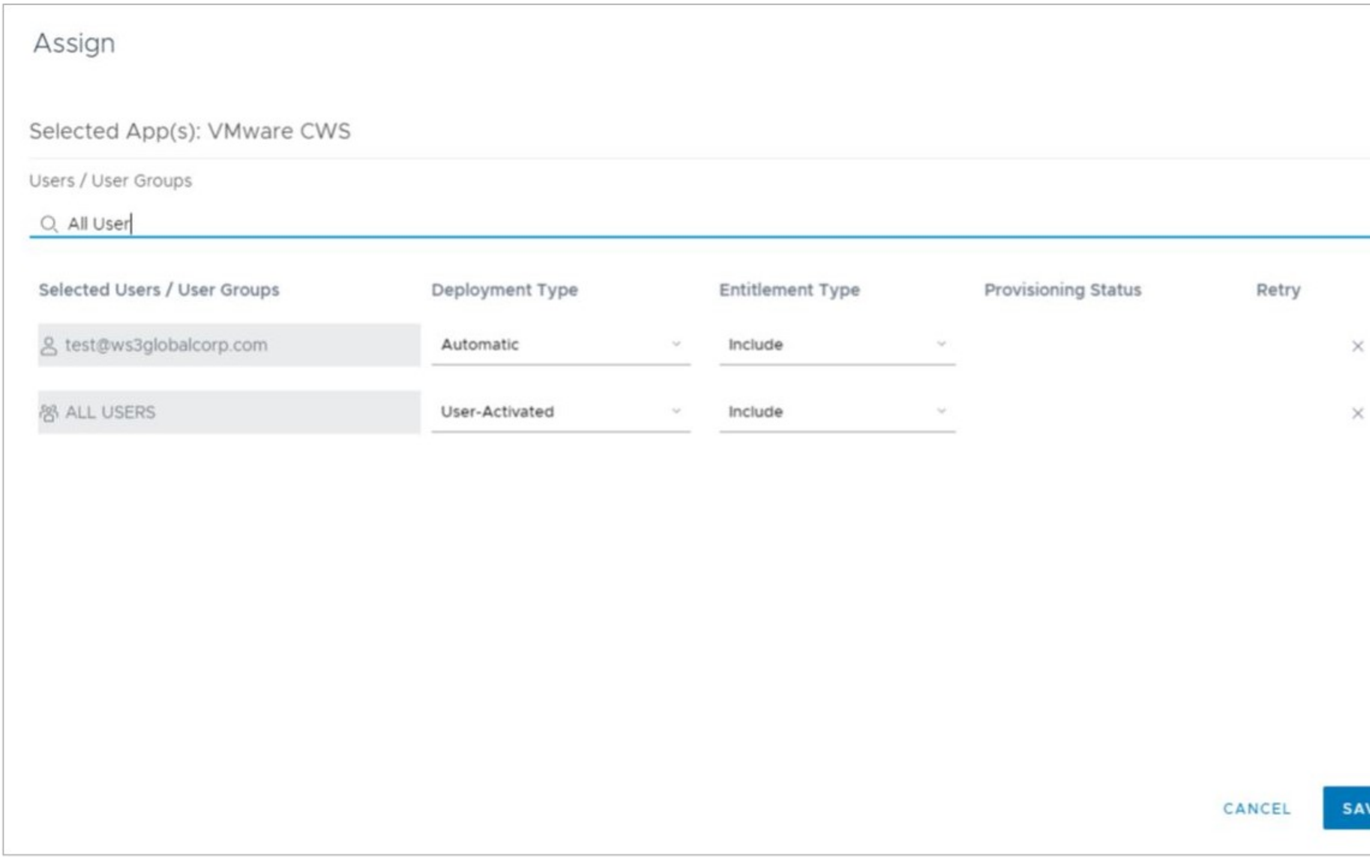
C=US, O=TD-DEREKT-954E0:SAML, CN=VMware Identity Manager

```
-----BEGIN CERTIFICATE-----
MIIFLDCCAxSgAwIBAgIGP2il70DDMA0GCSqGSIb3DQEBCwUAME4
xIDAeBgNVBAMM
F1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMR0wGwYDVQQKDBRU
RC1ERVJFS1QtOTU0
```

12 Assign User Groups to the VMware CWS web application.



☐	Application	Type
☐	AirWatch Admin	SAML 2.0
☑	VMware CWS	SAML 2.0
☑ 1		



Assign

Selected App(s): VMware CWS

Users / User Groups

All User

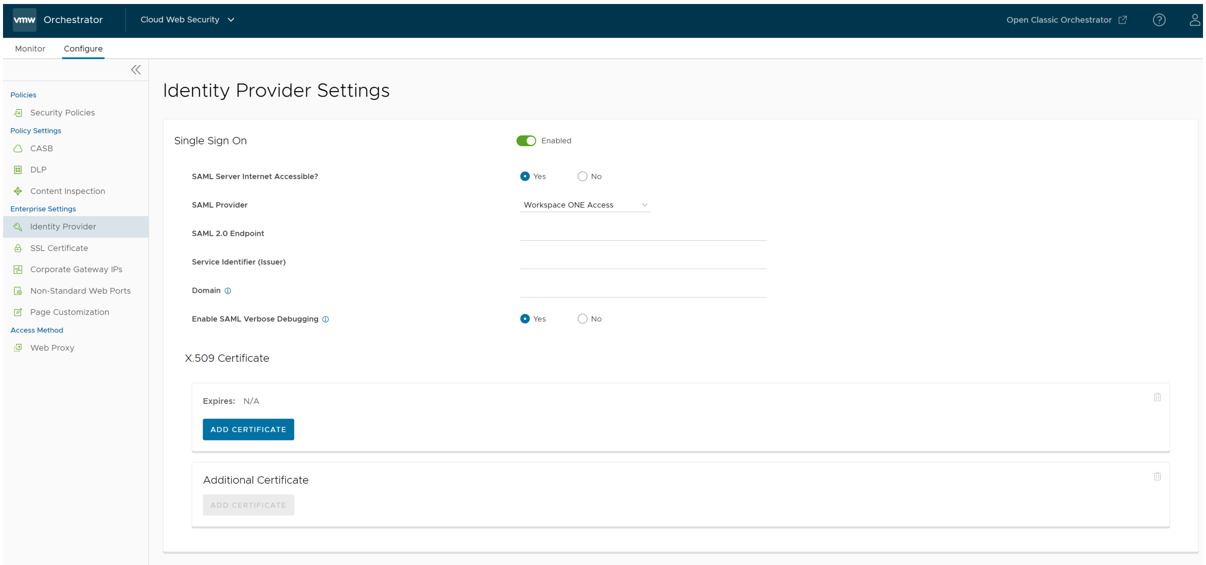
Selected Users / User Groups	Deployment Type	Entitlement Type	Provisioning Status	Retry
test@ws3globalcorp.com	Automatic	Include		
ALL USERS	User-Activated	Include		

VMware Cloud Orchestrator Configuration

1 Log onto the New Orchestrator UI.

2 Go to **Cloud Web Security** > **Configure** > **Enterprise Settings** > **Identity Provider**. The **Identity Provider Settings** page appears.

3 Toggle **Single Sign On** to **Enabled**.



Identity Provider Settings

Single Sign On: Enabled

SAML Server Internet Accessible? ● Yes ○ No

SAML Provider: Workspace ONE Access

SAML 2.0 Endpoint

Service Identifier (Issuer)

Domain

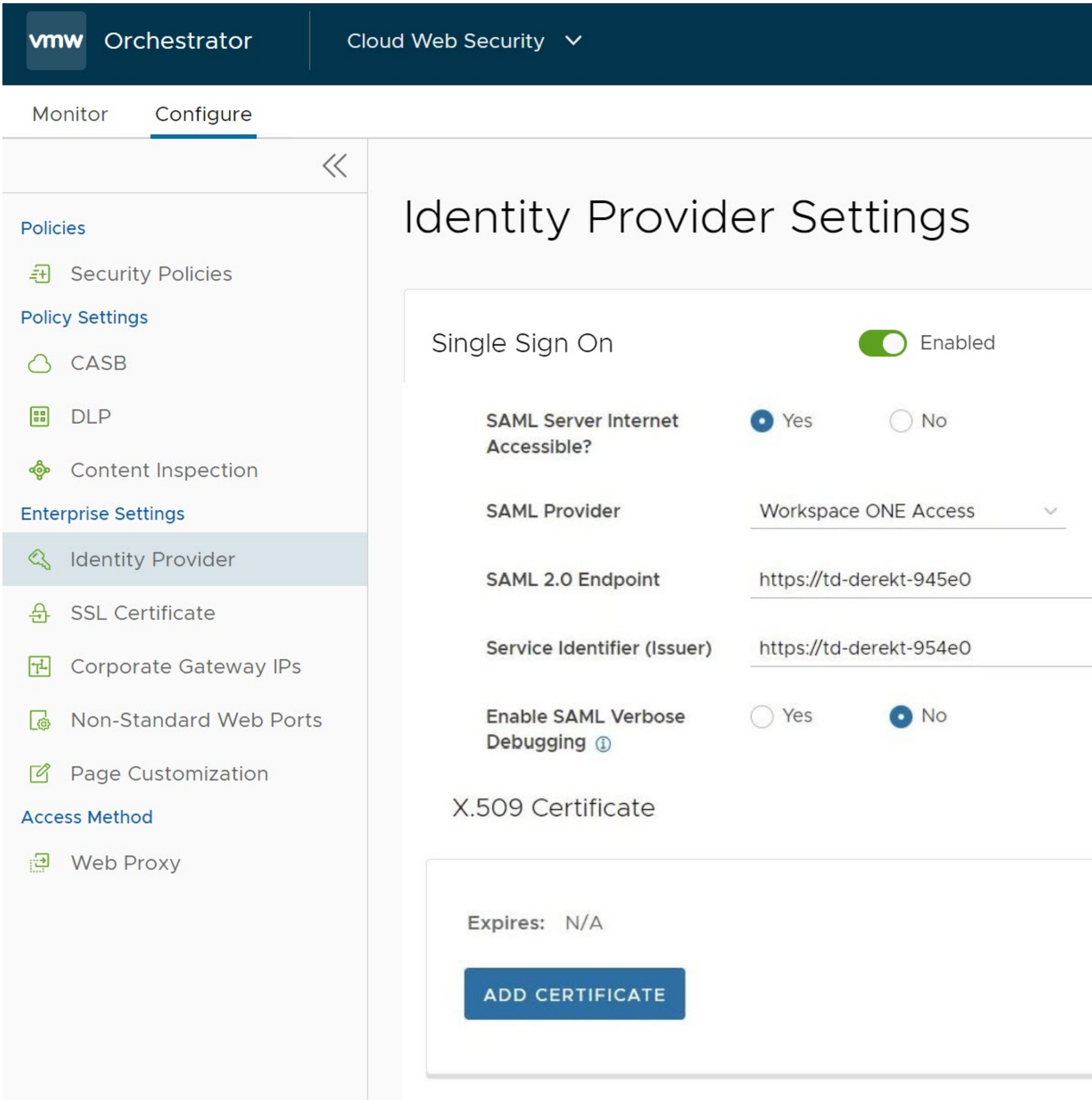
Enable SAML Verbose Debugging ● Yes ○ No

X.509 Certificate

Expires: N/A

4 Configure the following:

  - For **SAML Server Internet Accessible** select **Yes**
  - For **SAML Provider** select **Workspace ONE Access**
  - For **SAML 2.0 Endpoint**, copy the **Location** URL from the notepad. For example, **Location**: https://<ws1access_server>/SAAS/auth/federation/sso
  - For **Service Identifier (Issuer)**, copy the **entityID** URL from the notepad. For example, **entityID**: https://<ws1access_server>/SAAS/API/1.0/GET/metadata/idp.xml
  - X.509 Certificate, click on **Add Certificate** and copy the certificate from the notepad and paste here.
  - Click **Save Changes**



Identity Provider Settings

Single Sign On: Enabled

SAML Server Internet Accessible? ● Yes ○ No

SAML Provider: Workspace ONE Access

SAML 2.0 Endpoint: https://td-derekt-945e0

Service Identifier (Issuer): https://td-derekt-954e0

Enable SAML Verbose Debugging: ○ Yes ● No

X.509 Certificate

Expires: N/A

5 Add an SSL Bypass rule for the Workspace ONE Access domain.

  a Navigate to **Cloud Web Security > Configure > Security Policies**.

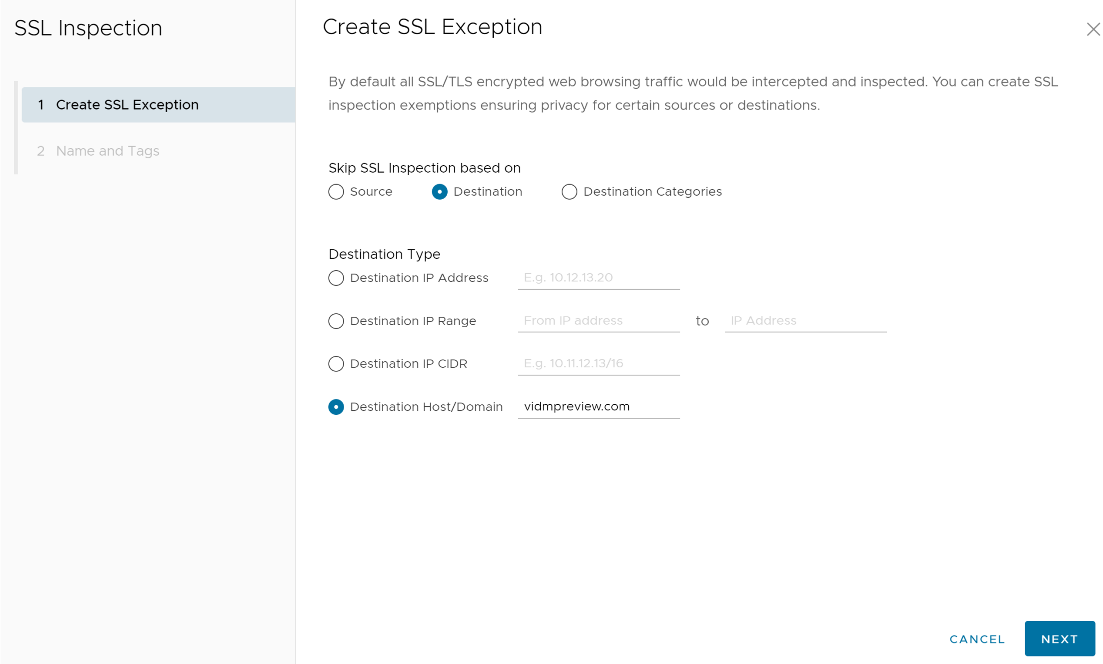
  b Select an existing policy to add SSL Bypass rule and click the **Edit** button.

  c Click the **SSL Inspection** tab and click **+ Add Rule**. The **Create SSL Exception** screen appears.

  d In the **Create SSL Exception** screen, configure the following and click **Next**:

    - For **Skip SSL Inspection based on**, select **Destination**.

- For **Destination Type**, select **Destination Host/Domain**.
- For **Domain**, enter **vidmpreview.com**.



SSL Inspection

1 Create SSL Exception

2 Name and Tags

Create SSL Exception

By default all SSL/TLS encrypted web browsing traffic would be intercepted and inspected. You can create SSL inspection exemptions ensuring privacy for certain sources or destinations.

Skip SSL Inspection based on

○ Source ● Destination ○ Destination Categories

Destination Type

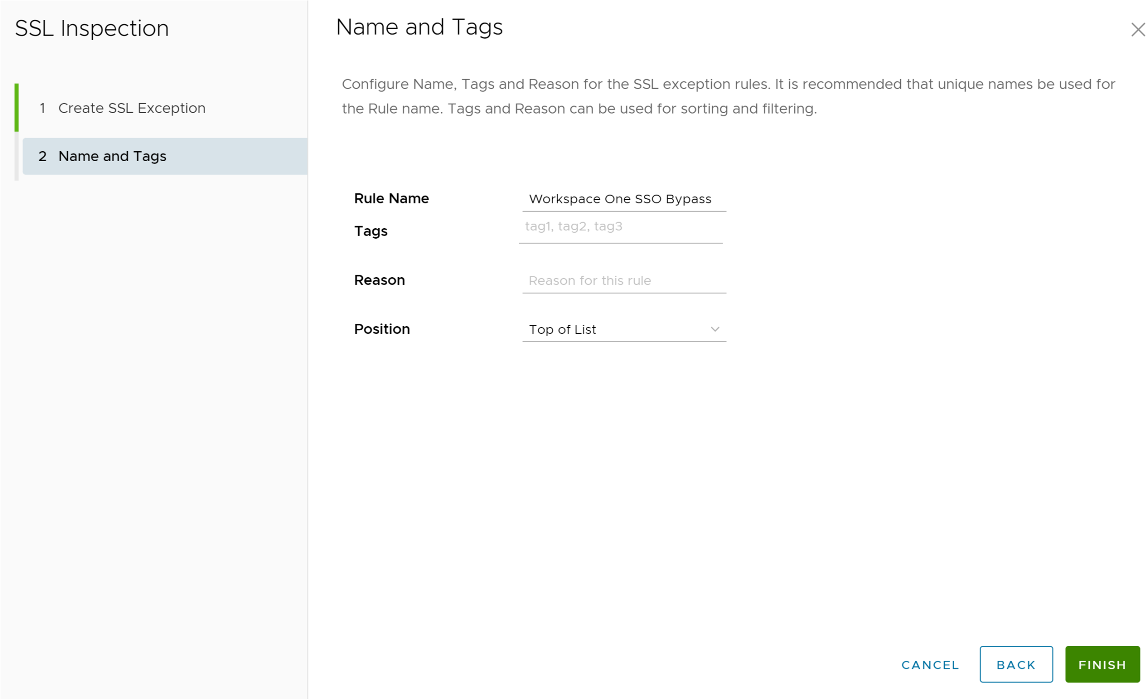
○ Destination IP Address E.g. 10.12.13.20

○ Destination IP Range From IP address to IP Address

○ Destination IP CIDR E.g. 10.11.12.13/16

● Destination Host/Domain vidmpreview.com

e In the **Name and Tags** screen, enter a unique name for the rule and add a reason, if needed.



SSL Inspection

1 Create SSL Exception

2 Name and Tags

Name and Tags

Configure Name, Tags and Reason for the SSL exception rules. It is recommended that unique names be used for the Rule name. Tags and Reason can be used for sorting and filtering.

Rule Name Workspace One SSO Bypass

Tags tag1, tag2, tag3

Reason Reason for this rule

Position Top of List

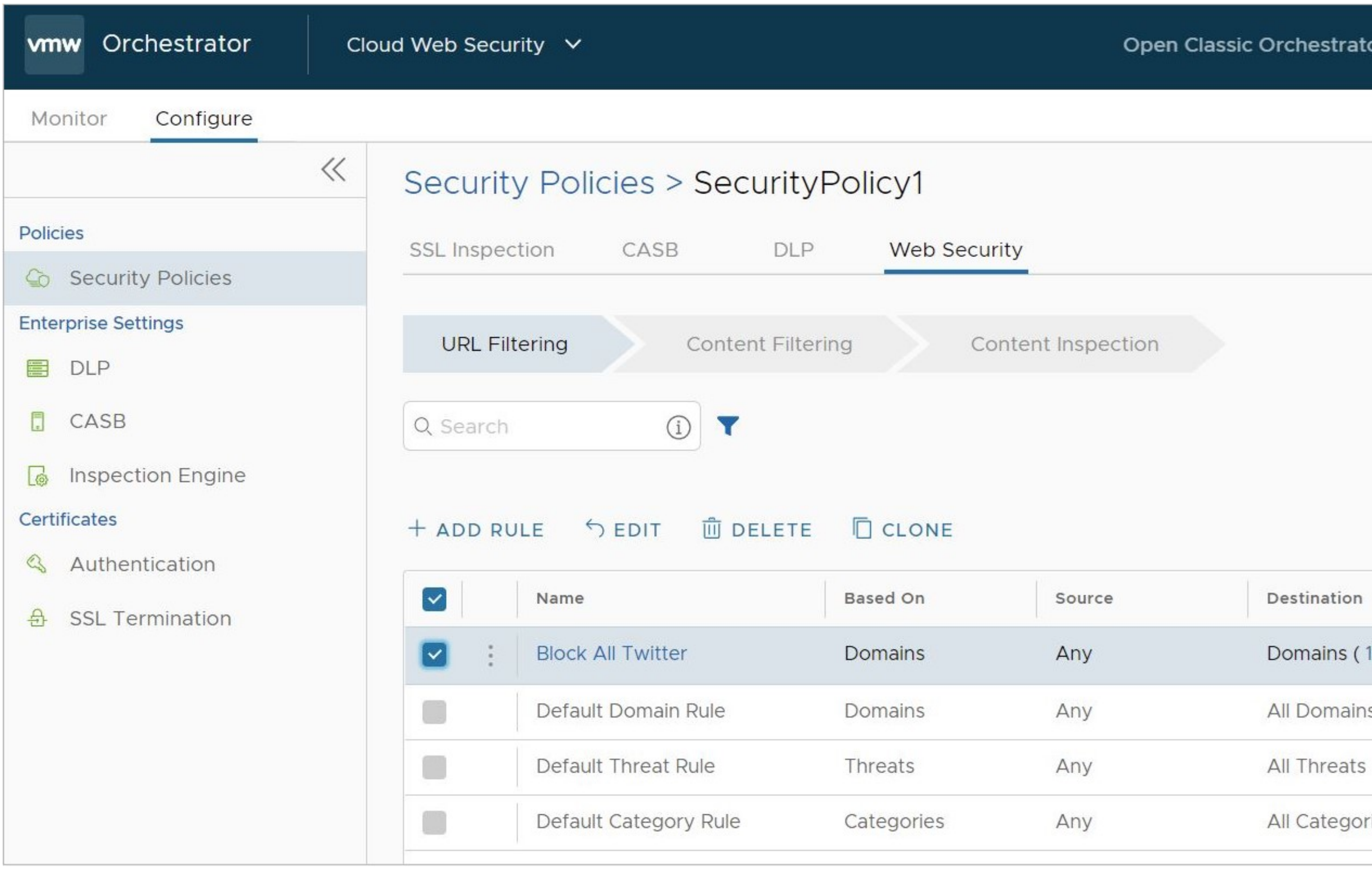
f Click **Finish**, and then **Publish** the applicable Security Policy to apply this new rule.

Important The domain **vidmpreview.com** is part of the **Workspace ONE** pair of domains as found in the document: Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended. If you have already configured an SSL Bypass rule which includes both **Workspace ONE** domains, you can skip this step. If you attempt to configure the above rule while also already having the **Workspace ONE** domain set included in an existing SSL Bypass rule, the new rule will throw an error as only one SSL Bypass domain instance is permitted or needed per Enterprise customer.

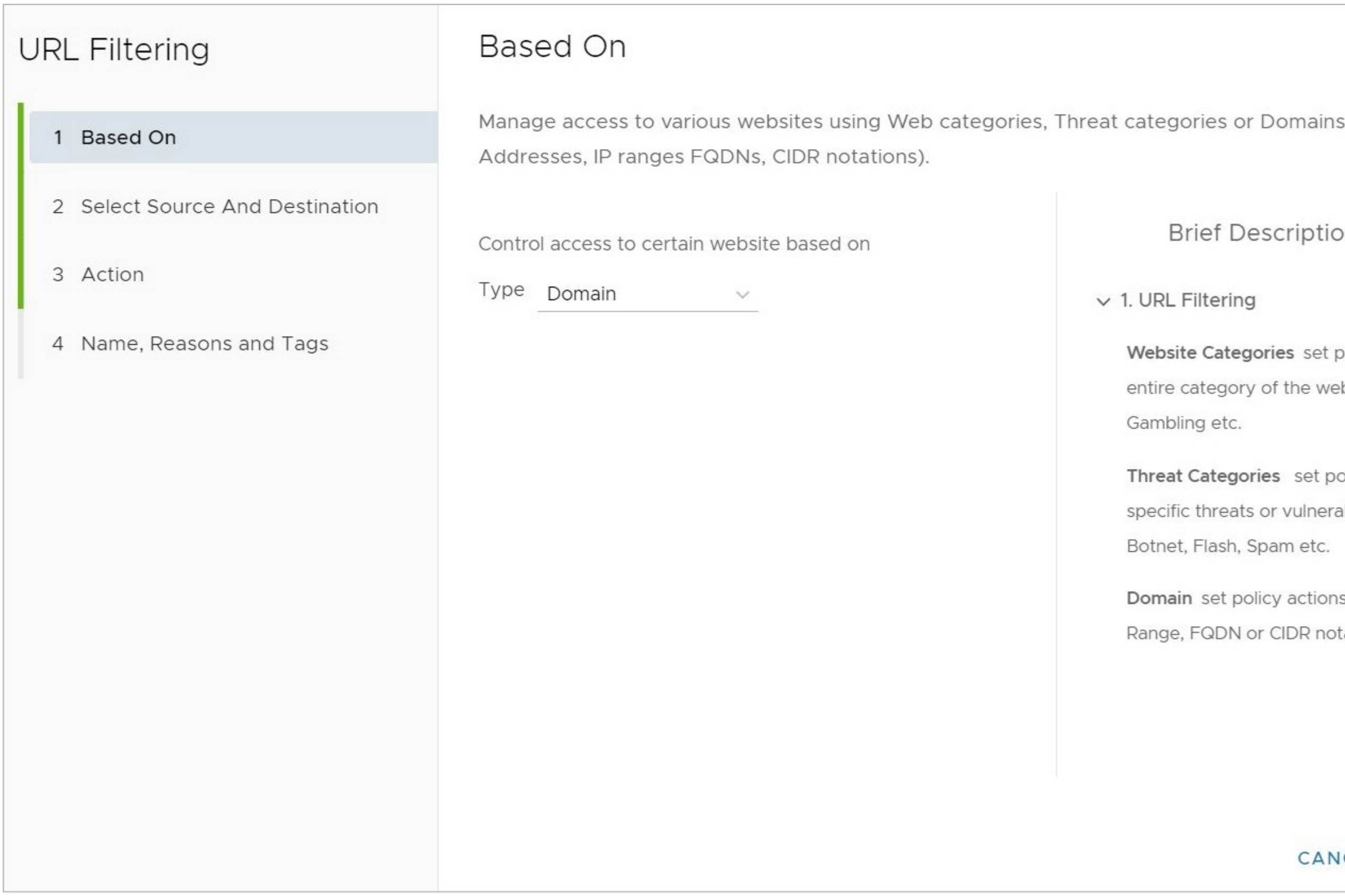
For more information on domains that should have SSL Bypass rules configured, consult Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended.

Verifying Your Configuration

Verifying your configuration may be done using one or more group-based web policy rules on Cloud Web Security. For example, using URL Filtering and blocking Twitter.com.



☑	Name	Based On	Source	Destination
☑	Block All Twitter	Domains	Any	Domains (1
☐	Default Domain Rule	Domains	Any	All Domains
☐	Default Threat Rule	Threats	Any	All Threats
☐	Default Category Rule	Categories	Any	All Categor



Based On

Manage access to various websites using Web categories, Threat categories or Domains Addresses, IP ranges FQDNs, CIDR notations).

Control access to certain website based on

Type: Domain

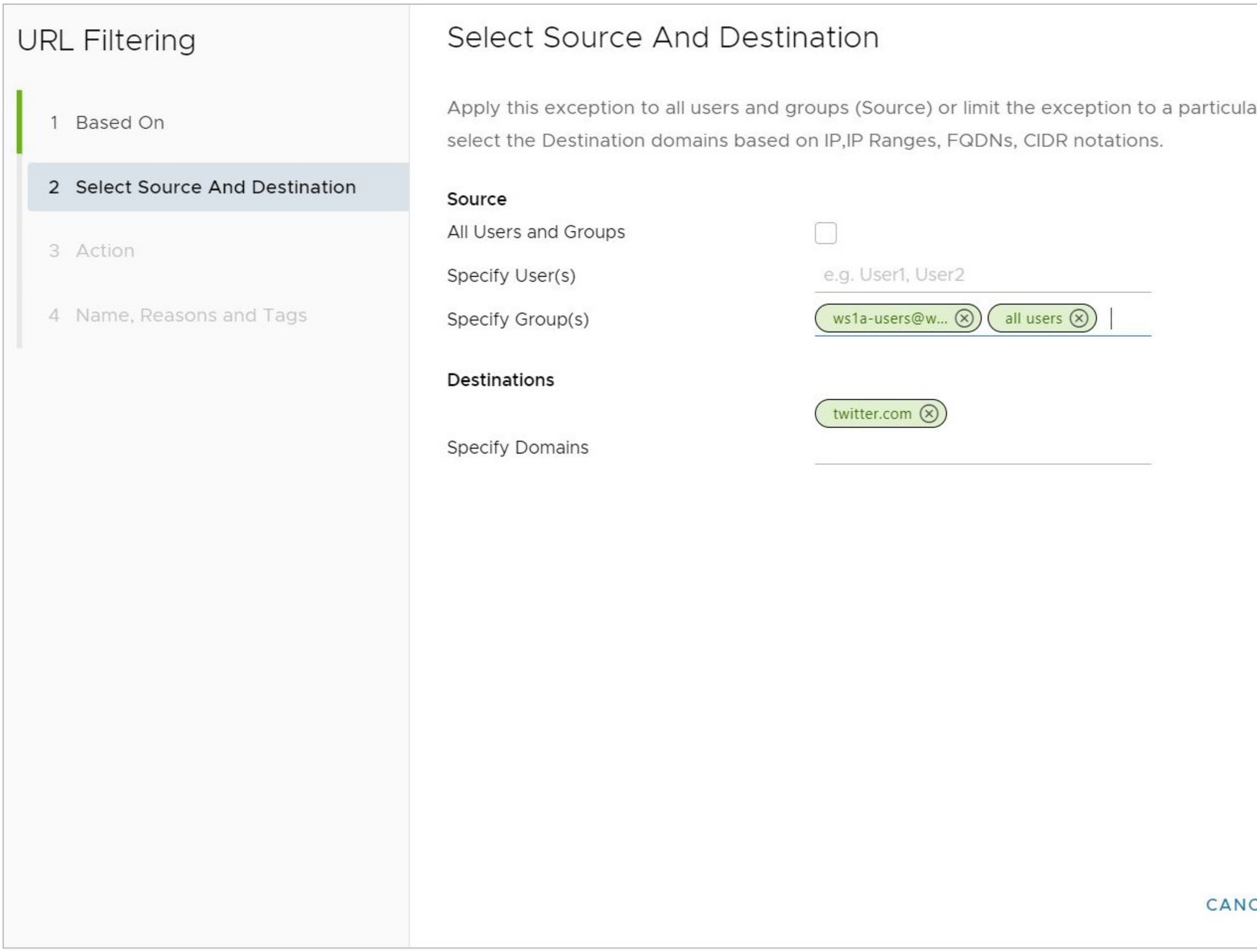
Website Categories set p entire category of the wel Gambling etc.

Threat Categories set po specific threats or vulnera Botnet, Flash, Spam etc.

Domain set policy actions Range, FQDN or CIDR not

Add the Groups to be considered for the URL Filter rule.

Note The groups have to be specified manually. There is no 'search' capability to select which groups. Add the group name as they are setup in Workspace ONE Access.


URL Filtering

1 Based On

2 Select Source And Destination

3 Action

4 Name, Reasons and Tags

Select Source And Destination

Apply this exception to all users and groups (Source) or limit the exception to a particula

select the Destination domains based on IP,IP Ranges, FQDNs, CIDR notations.

Source

All Users and Groups ☐

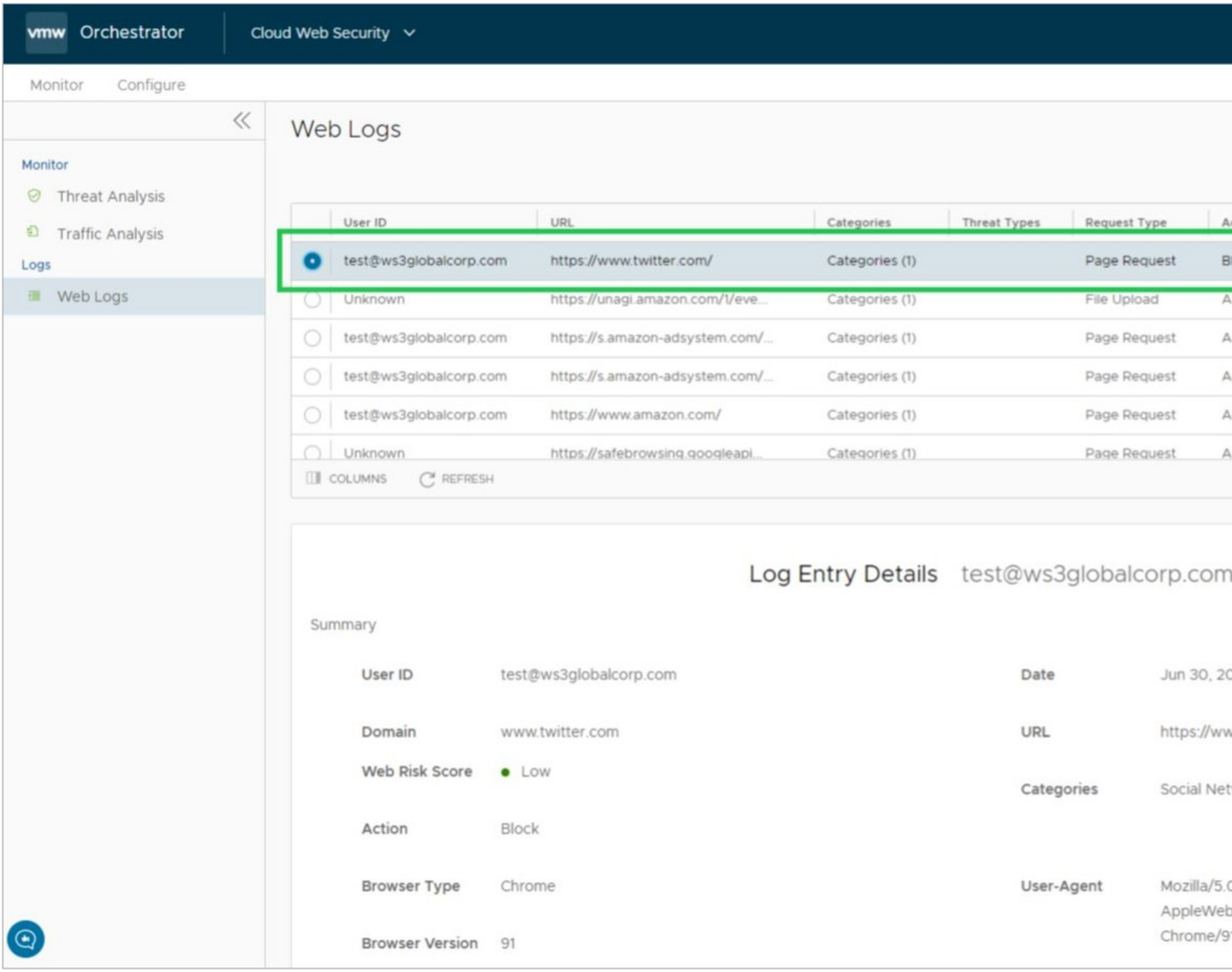
Specify User(s) e.g. User1, User2

Specify Group(s) ws1a-users@w... ⓧ all users ⓧ

Destinations

Specify Domains twitter.com ⓧ

Check the Web Logs under **Cloud Web Security** > **Monitor** > **Web Logs**



Web Logs

	User ID	URL	Categories	Threat Types	Request Type	A
●	test@ws3globalcorp.com	https://www.twitter.com/	Categories (1)		Page Request	Bl
○	Unknown	https://unagi.amazon.com/1/eve...	Categories (1)		File Upload	A
○	test@ws3globalcorp.com	https://s.amazon-adsystem.com/...	Categories (1)		Page Request	A
○	test@ws3globalcorp.com	https://s.amazon-adsystem.com/...	Categories (1)		Page Request	A
○	test@ws3globalcorp.com	https://www.amazon.com/	Categories (1)		Page Request	A
○	Unknown	https://safebrowsing.googleapi...	Categories (1)		Page Request	A

Log Entry Details test@ws3globalcorp.com

Summary

User ID test@ws3globalcorp.com

Domain www.twitter.com

Web Risk Score ● Low

Action Block

Browser Type Chrome

Browser Version 91

Date Jun 30, 20

URL https://ww

Categories Social Net

User-Agent Mozilla/5.0 AppleWeb Chrome/9

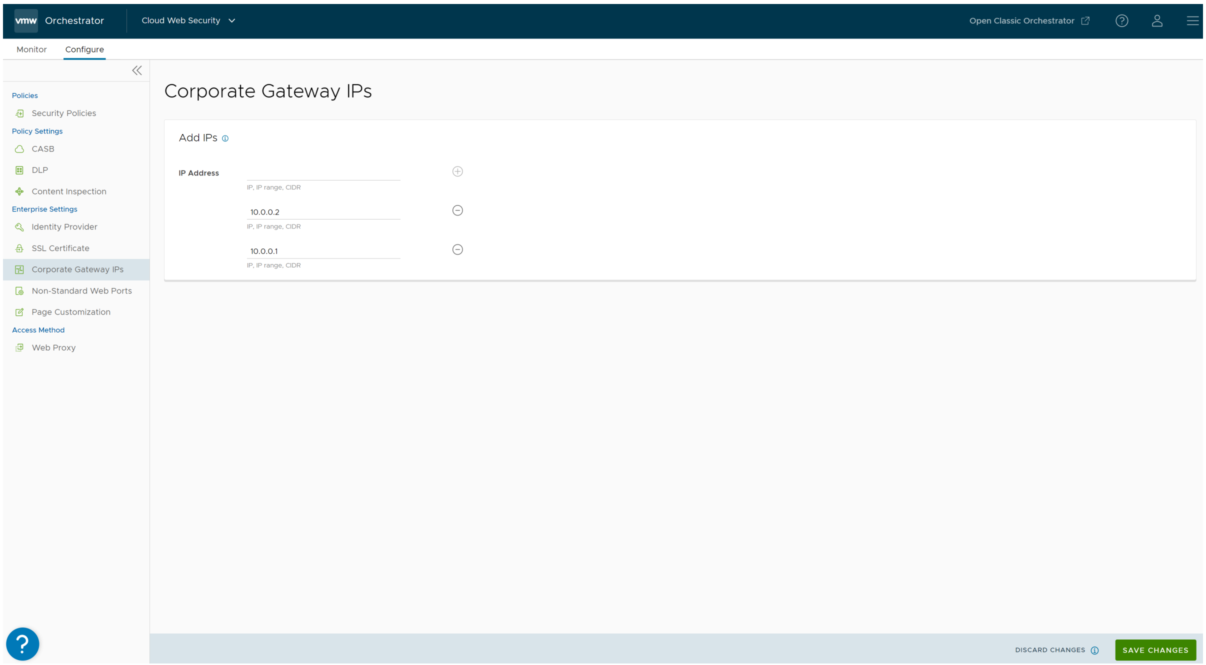
Configure Corporate Gateway IPs

5

Users can define Corporate IP addresses for SAML authentication and non-browser connections.

To add Corporate Gateway IP addresses:

1 Navigate to **Cloud Web Security** > **Configure** > **Enterprise Settings** > **Corporate Gateway IPs**.



10.0.0.2

10.0.0.1

2 In the **Corporate Gateway IPs** page, enter an IP address, or IP address ranges, or CIDR notation.

3 Click the "**+**" button to add more Corporate Gateway IPs.

4 Click the associated "**-**" button to remove existing IPs.

5 Click **Save Changes**.

Configure Non-Standard Web Ports

6

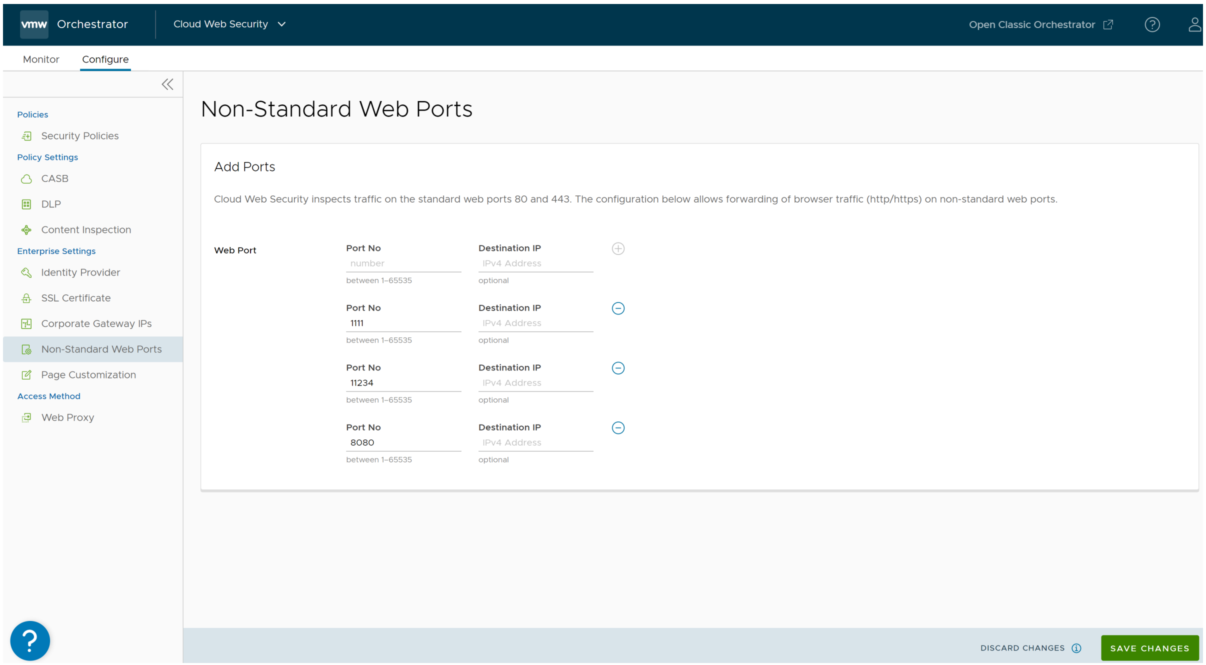
By default, VMware Cloud Web Security inspects web traffic on pre-configured Standard Web Ports 80 (HTTP) and 443 (HTTPS). Release 1.9.0 adds a new support that allows inspection of browser traffic (HTTP/HTTPS) on Non-Standard Web Ports.

To configure a Non-Standard Web Port, perform the following steps:

Procedure

1 Navigate to **Cloud Web Security** > **Configure** > **Enterprise Settings** > **Non-Standard Web Ports**.

The **Non-Standard Web Ports** page appears.



Non-Standard Web Ports

Add Ports

Cloud Web Security inspects traffic on the standard web ports 80 and 443. The configuration below allows forwarding of browser traffic (http/https) on non-standard web ports.

Web Port	Port No	Destination IP
	number between 1–65535	IPv4 Address optional
	1111 between 1–65535	IPv4 Address optional
	11234 between 1–65535	IPv4 Address optional
	8080 between 1–65535	IPv4 Address optional

2 In the **Web Port** field, enter the port number of the Non-Standard Web Port to inspect web traffic and apply configured security policies. Users can enter any port number between 1 through 65535. Optionally, users can enter the destination IP address.

3 Click the "**+**" button to add more Non-Standard Web Ports.

4. Users can edit existing ports by changing the port number. To remove existing ports, click the associated "**-**" button.
5. Click **Save Changes**.

Page Customization

7

VMware Cloud Web Security displays a VMware branded block page by default to all users when the security policies block users from accessing a website or cloud application. The block page is constructed from a series of HTML, CSS, and JavaScript files. Users can customize the block page to adapt it to the needs of their organization and end users.

Page Customization feature allows users to customize their own branded block page to serve users traffic (Web or Data Loss Prevention traffic) when it gets blocked. For example, an Enterprise can display its logo on block page when a request is blocked.

VMware Cloud Web Security allows users to customize:

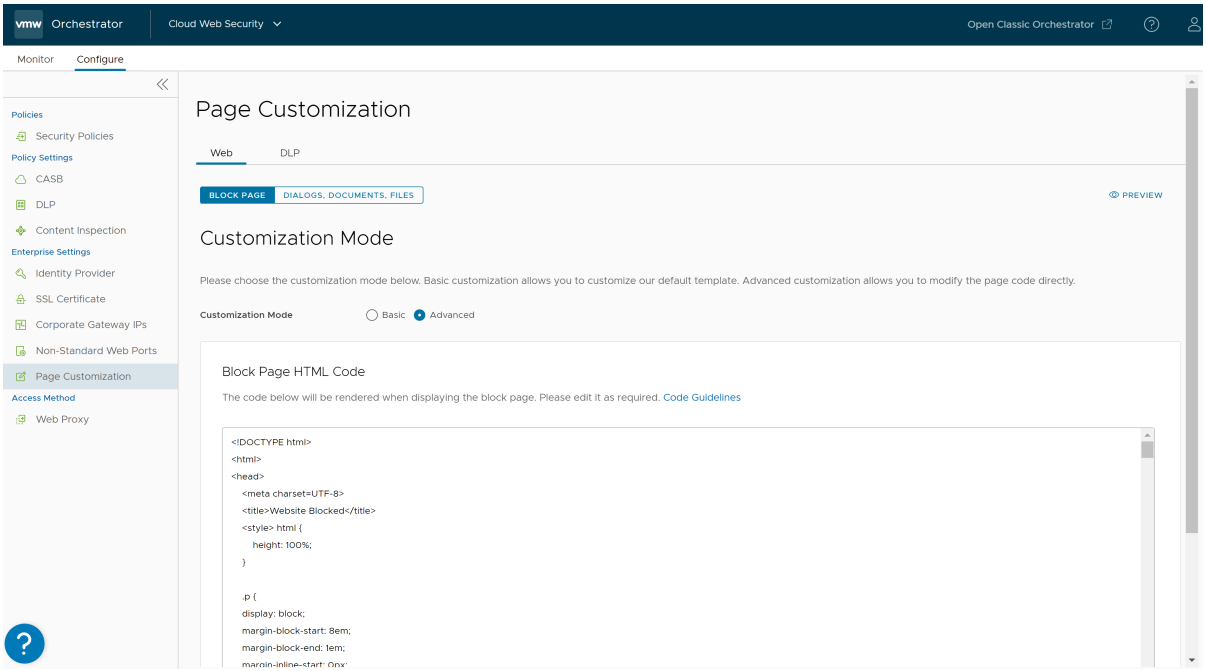
- A Block page that VMware cloud uses to respond to an HTTP request or file upload that violates a configured security policy.
- A Block page that VMware cloud returns when users try to upload a file that violates a configured DLP rule.

Configure Custom Block Page for Web Traffic

To customize a block page for Web traffic, perform the following steps:

1. Navigate to **Cloud Web Security** > **Configure** > **Enterprise Settings** > **Page Customization**.

   The **Page Customization** page appears.



Page Customization

Customization Mode

Please choose the customization mode below. Basic customization allows you to customize our default template. Advanced customization allows you to modify the page code directly.

Customization Mode ○ Basic ● Advanced

Block Page HTML Code

The code below will be rendered when displaying the block page. Please edit it as required. Code Guidelines

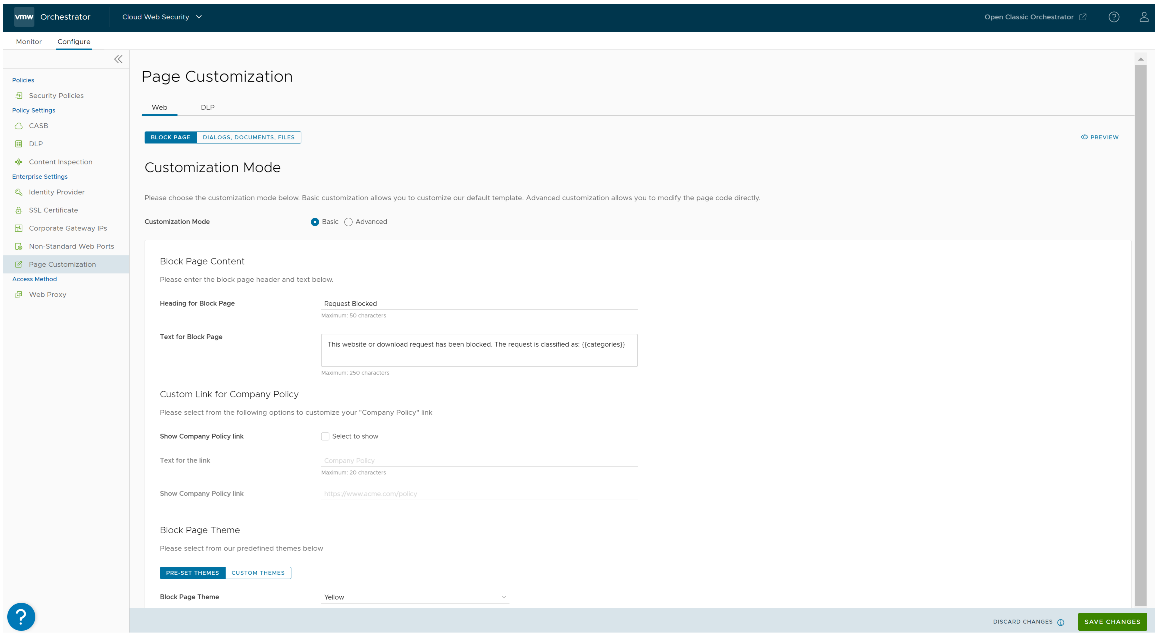
```
<!DOCTYPE html>
<html>
<head>
  <meta charset=UTF-8>
  <title>Website Blocked</title>
  <style> html {
    height: 100%;
  }

  .p {
  display: block;
  margin-block-start: 8em;
  margin-block-end: 1em;
  margin-inline-start: 0px;
```

2 In the **Web** tab, click **Block Page**.

3 Select **Basic** or **Advanced** as the customization mode.

- **Basic** – Allows to customize the default block page template using the various parameters described in the following table.



Page Customization

Customization Mode

Please choose the customization mode below. Basic customization allows you to customize our default template. Advanced customization allows you to modify the page code directly.

Customization Mode ● Basic ○ Advanced

Block Page Content

Please enter the block page header and text below.

Heading for Block Page: Request Blocked

Maximum: 50 characters

Text for Block Page: This website or download request has been blocked. The request is classified as: {{categories}}

Maximum: 250 characters

Custom Link for Company Policy

Please select from the following options to customize your "Company Policy" link

Show Company Policy link ☐ Select to show

Text for the link: Company Policy

Maximum: 20 characters

Show Company Policy link: https://www.acme.com/policy

Block Page Theme

Please select from our predefined themes below

Block Page Theme: Yellow

Field	Description
Heading for Block Page	Enter a header for the block page. The maximum length is 50 characters.

Text for Block Page	Enter the description text to be displayed in the block page. The maximum length is 250 characters.
Show Company Policy Link Check box	Choose the **Select to show** check box to show the company policy link in the customized block page.
Text for the Link	Enter the text to display for the link. The maximum length is 20 characters.
Show Company Policy Link	Enter the URL of the company policy.
Pre-set Themes	Select the Block page theme color from the predefined list: Red, Orange, Yellow, Green, Blue, Indigo, Violet, Grey, White, and Black.
Custom Themes	Allows users to customize the logo, icon, and styles used in the block page.
Logo/Icon	■ **Logo/Icon File** – Upload your logo file into the logo Directory by using one of the following options: ■ **Upload File** – Select and upload the logo file. The recommended dimensions for the logo file are 120px X 40px - Ratio 3:1. **Note** Only files of type “image/” are allowed. ■ **Use URL** - Enter the Logo URL. ■ **Logo/Icon Preview** – The uploaded logo image appears in the preview area.
CSS Styles	■ **Link Color** – Enter the color code to be used for the link that appears in the block page or click the rectangular color box and select the link color. ■ **Background Color** – Enter the color code to be used as the background color for the block page or click the rectangular color box and select the background color. ■ **Text Color** – Enter the color code to be used for the text that appears in the block page or click the rectangular color box and select the text color. ■ **Details Text Color** – Enter the color code to be used for the details text that appears in the block page or click the rectangular color box and select the text color. ■ **Details Highlight Text Color** – Enter the color code to be used for highlighting the details text that appears in the block page or click the rectangular color box and select the highlight text color. ■ **Reason Text Color** – Enter the color code to be used for the reason text that appears in the block page or click the rectangular color box and select the reason text color. ■ **Block Page Type** – Select either Box or Wide as the type for the block page. ■ **Font Family** – Select the font family from the predefined list: Arial, Georgia, Gotham, Helvetica, Lucida, Tahoma, Times, and Verdana.

- **Advanced** – Allows to modify the formatting and style of the Block Page HTML and CSS code. By default, this option is selected. Users can edit the block page code as required and save the changes. For more information, see Custom Block Pages.

4 Click **Preview** to view the customized block page.

5 Click **Save Changes**.

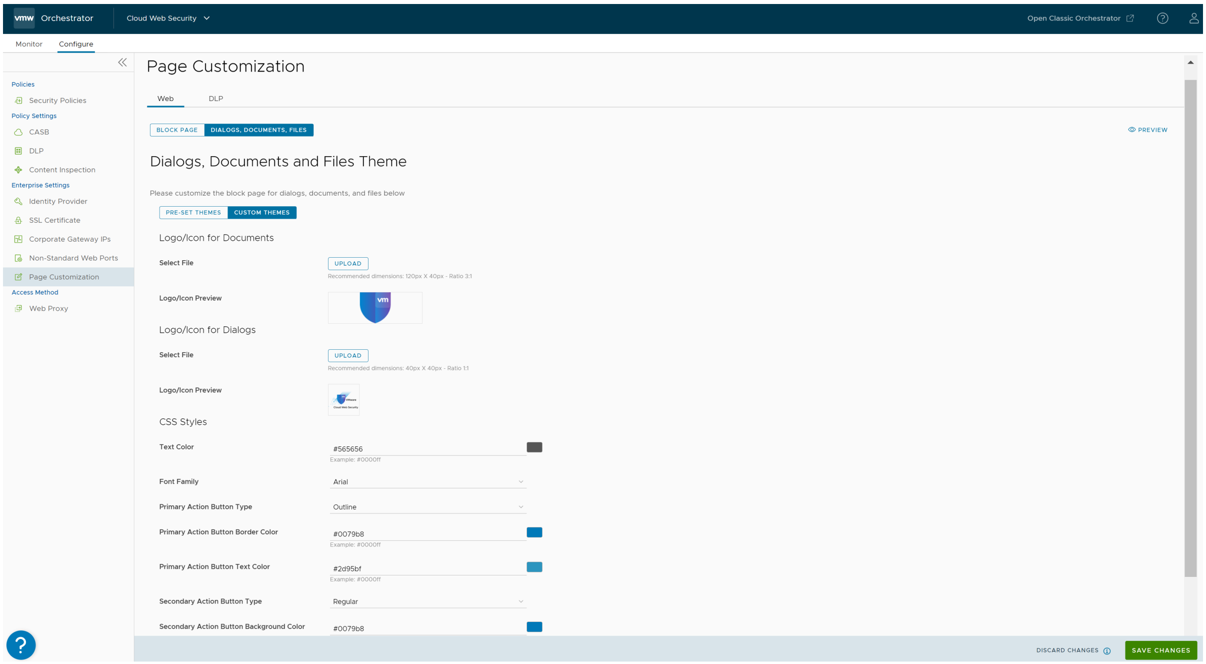
Configure Custom Block Page for Dialog/Document/File Downloads

To customize a block page for Web traffic, perform the following steps:

1 Navigate to **Cloud Web Security** > **Configure** > **Enterprise Settings** > **Page Customization**.

The **Page Customization** page appears.

2 In the **Web** tab, click **Dialogs, Documents, Files**.



Dialogs, Documents and Files Theme

Please customize the block page for dialogs, documents, and files below

Logo/Icon for Documents

Select File: Recommended dimensions: 120px X 40px - Ratio 3:1

Logo/Icon for Dialogs

Select File: Recommended dimensions: 40px X 40px - Ratio 1:1

CSS Styles

Text Color: #565656 (Example: #0000ff)

Font Family: Arial

Primary Action Button Type: Outline

Primary Action Button Border Color: #0079b8 (Example: #0000ff)

Primary Action Button Text Color: #2d95bf (Example: #0000ff)

Secondary Action Button Type: Regular

Secondary Action Button Background Color: #0079b8

3 Select a theme for the block page for dialogs, documents, and files. Use Pre-set themes or create your own custom theme:

- **Pre-set Themes** – Allows to select the Block page theme color from the predefined list of colors: Red, White, Purple, and Light Blue.
- **Custom Themes** – Allows to customize the logo/ icon for documents and Dialogs, and styles used in the block page. By default, **Custom Themes** option is selected.

Field	Description
Logo/Icon for Documents	■ **Select File** - Click **Upload** to select and upload the logo file for documents. The recommended dimensions for the document logo file are 120px X 40px - Ratio 3:1. **Note** Only files of type “image/” are allowed. ■ **Logo/Icon Preview** – The uploaded logo image appears in the preview area.

Logo/Icon for Dialogs	■ **Select File** - Click **Upload** to select and upload the logo file for dialogs. The recommended dimensions for the dialog logo file are 40px X 40px - Ratio 1:1. **Note** Only files of type “image/” are allowed. ■ **Logo/Icon Preview** – The uploaded logo image appears in the preview area.
CSS Styles	■ **Text Color** – Enter the color code to be used for the link that appears in the block page or click the rectangular color box and select the link color. ■ **Font Family** – Select the font family from the predefined list: Arial, Georgia, Gotham, Helvetica, Lucida, Tahoma, Times, and Verdana. ■ **Primary Action Button Type** – Select either Regular or Outline as the action button type. ■ **Primary Action Button Background Color** – Enter the color code to be used for the background of the Primary action button in the block page or click the rectangular color box and select the background color. ■ **Primary Action Button Border Color** – Enter the color code to be used for the border of the Primary action button in the block page or click the rectangular color box and select the border color. ■ **Primary Action Button Text Color** - Enter the color code to be used for the Primary action button text in the block page or click the rectangular color box and select the text color. ■ **Secondary Action Button Type** – Select either Regular or Outline as the action button type. ■ **Secondary Action Button Background Color** – Enter the color code to be used for the background of the Secondary action button in the block page or click the rectangular color box and select the background color. ■ **Secondary Action Button Border Color** – Enter the color code to be used for the border of the Secondary action button in the block page or click the rectangular color box and select the border color. ■ **Secondary Action Button Text Color** - Enter the color code to be used for the Secondary action button text in the block page or click the rectangular color box and select the text color.

4 Click **Preview** to view the customized block page.

5 Click **Save Changes**.

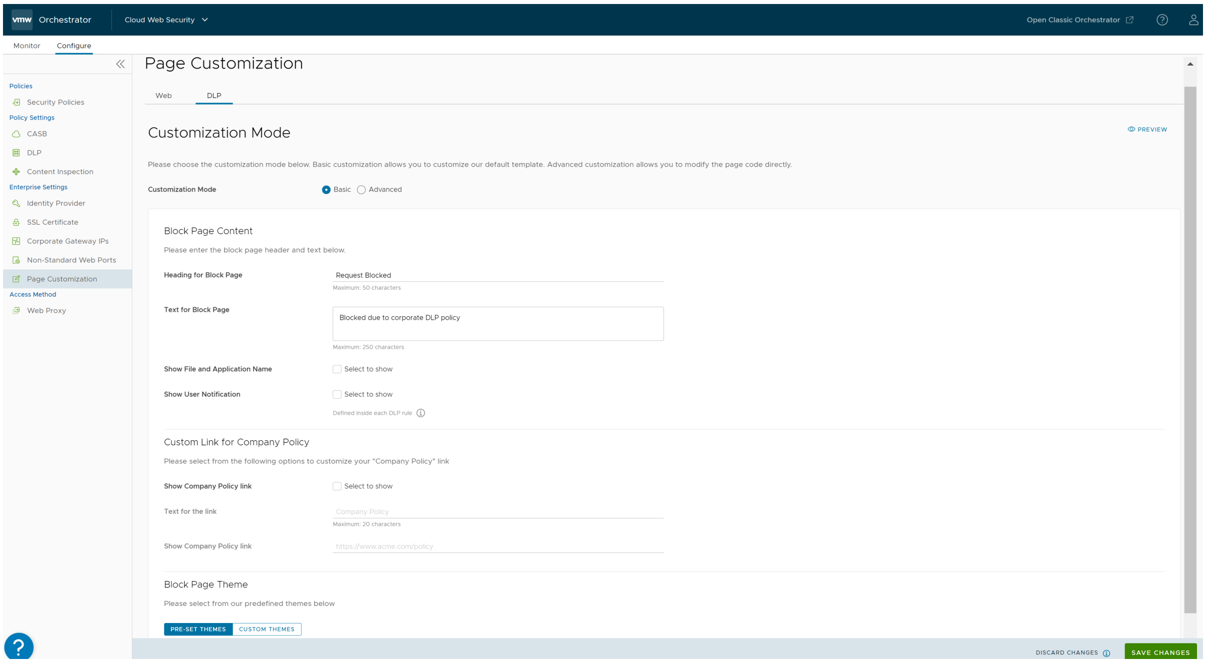
Configure Custom Block Page for DLP Traffic

To customize a block page for DLP traffic, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Enterprise Settings > Page Customization**.

The **Page Customization** page appears.

2 Click the **DLP** tab.



Page Customization

Customization Mode

Please choose the customization mode below. Basic customization allows you to customize our default template. Advanced customization allows you to modify the page code directly.

Customization Mode ● Basic ○ Advanced

Block Page Content

Please enter the block page header and text below.

Heading for Block Page: Request Blocked (Maximum: 50 characters)

Text for Block Page: Blocked due to corporate DLP policy (Maximum: 250 characters)

Show File and Application Name: ☐ Select to show

Show User Notification: ☐ Select to show (Defined inside each DLP rule)

Custom Link for Company Policy

Please select from the following options to customize your "Company Policy" link

Show Company Policy link: ☐ Select to show

Text for the link: Company Policy (Maximum: 20 characters)

Show Company Policy link: https://www.acme.com/policy

Block Page Theme

Please select from our predefined themes below

3 Select any of the following Customization Modes:

- **Basic** – Allows to customize the default block page template using the various parameters described in the following table. By default, this option is selected.

Field	Description
Heading for Block Page	Enter a header for the block page. The maximum length is 50 characters.
Text for Block Page	Enter the description text to be displayed in the block page. The maximum length is 250 characters.
Show File and Application Name	Choose the **Select to show** check box to show the file and application name in the customized block page.
Show User Notification	Choose the **Select to show** check box to show notification to users for a violated DLP rule. The content of these notifications is specified within the DLP rule.
Show Company Policy Link	Choose the **Select to show** check box to show the company policy link in the customized block page.
Text for the Link	Enter the text to display for the link. The maximum length is 20 characters.
Show Company Policy Link	Enter the URL of the company policy.
Pre-set Themes	Select the Block page theme color from the predefined list: Red, Orange, Yellow, Green, Blue, Indigo, Violet, Grey, White, and Black.
Custom Themes	Allows users to customize the logo, icon, and styles used in the block page.

Logo/Icon	■ **Logo/Icon File** – Upload your logo file into the logo Directory by using one of the following options: ■ **Upload File** – Select and upload the logo file. The recommended dimensions for the logo file are 120px X 40px - Ratio 3:1. **Note** Only files of type “image/” are allowed. ■ **Use URL** - Enter the Logo URL. ■ **Image Preview** – The uploaded logo image appears in the preview area.
CSS Styles	■ **Link Color** – Enter the color code to be used for the link that appears in the block page or click the rectangular color box and select the link color. ■ **Background Color** – Enter the color code to be used as the background color for the block page or click the rectangular color box and select the background color. ■ **Text Color** – Enter the color code to be used for the text that appears in the block page or click the rectangular color box and select the text color. ■ **Details Text Color** – Enter the color code to be used for the details text that appears in the block page or click the rectangular color box and select the text color. ■ **Details Highlight Text Color** – Enter the color code to be used for highlighting the details text that appears in the block page or click the rectangular color box and select the highlight text color. ■ **Reason Text Color** – Enter the color code to be used for the reason text that appears in the block page or click the rectangular color box and select the reason text color. ■ **Block Page Type** – Select either Box or Wide as the type for the block page. ■ **Font Family** – Select the font family from the predefined list: Arial, Georgia, Gotham, Helvetica, Lucida, Tahoma, Times, and Verdana.

- **Advanced** – Allows to modify the formatting and style of the Block Page HTML and CSS code. Users can edit the block page code as required and save the changes. For more information, see Custom Block Pages.

4 Click **Preview** to view the customized block page.

5 Click **Save Changes**.

Read the following topics next:

- Custom Block Pages

Custom Block Pages

Defines formatting and style recommendations for HTML and CSS of the Custom Block Page.

CSS

The CSS rules can be attached using external files, in-page `<style>...</style>` tags, or inline `style` attribute.

However, the `<style>...</style>` tag is recommended because it:

- Provides a clear separation of markup from styling

- Produces cleaner HTML markup and is easy to maintain
- Is more efficient with selectors to apply rules to multiple elements on a page improving management as well as making your page size smaller.
- Can be cached by browsers for performance
- Avoids external assets getting blocked by a policy and not displaying correctly

Images

For images, either CSS background or `<img>` tags are supported (via Base64 with JPG, PNG, or SVG).

In general, the Base64 file size is 37% bigger, but there is a risk of external images not being loaded due to a policy. Using Base64 prevents this and is therefore recommended.

To convert to Base64, there are some online services like b64.io that make the conversion and provide the encoded result.

Some examples of Base64 usage for `<img>` tag `src` attribute and CSS *background-image* property:

- `src="data:image/png;base64,iVBORw0KGgoAhEUgAAA ... FTkSuQmCC"`
- `background-image: url(data:image/png;base64,iVBORw0KGgoAAAA ... uQmCC);`

Variables

The following list of variables can be used to display user browsing information:

Variable	Description	Availability
user	User ID	Web and Email block pages
categories	Categories of the blocked page	Web and Email block pages
url	URL of the blocked page	Web and Email block pages
top_threat	Threat of the blocked page	Email block pages only
threat_details	Long description of the threat	Email block pages only
block_message	User notification defined in the DLP rule	DLP block pages only
block_files	Comma-separated list of files that violate the DLP rule	DLP block pages only
block_app	Name of the blocked application	DLP block pages only

Variables can be included directly into the HTML code, using double curly braces.

```
<strong>{{categories}}</strong>
```

Configure SaaS Header Restrictions

8

This section covers using SaaS Header Restrictions in Cloud Web Security to restrict tenant access to specified Software as a Service (SaaS) applications like Office 365 and G Suite and includes an overview, workflow for configuring a SaaS Header Restriction rule, and concludes with additional resources on this topic.

Overview

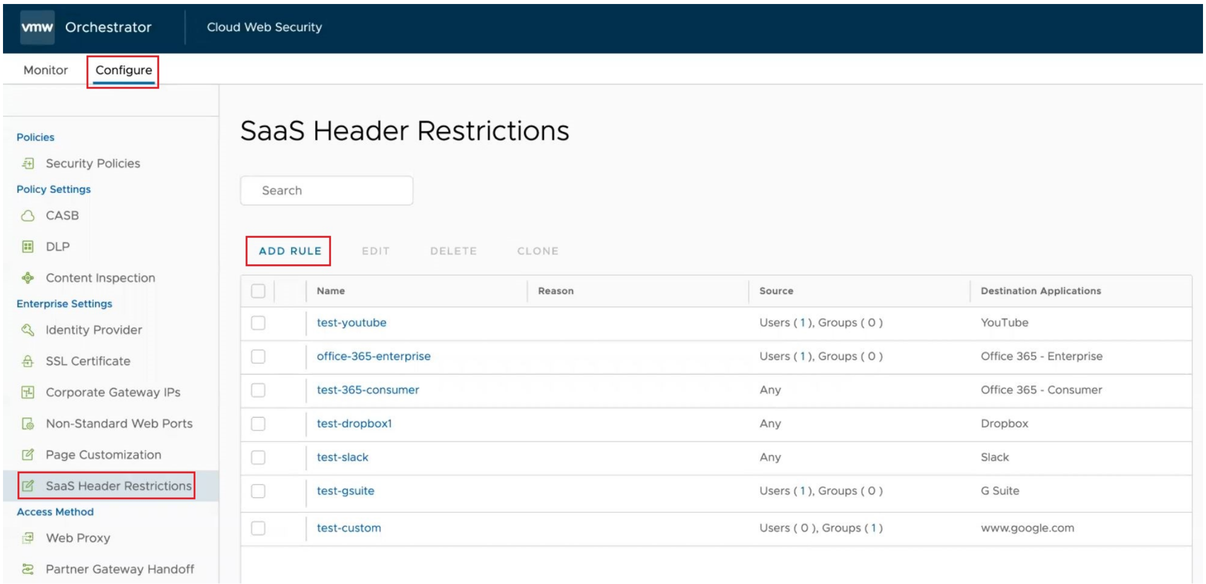
Traditionally, companies restrict domain names or IP addresses when they want to manage access. This approach fails in a world where software as a service (SaaS) applications are hosted in a public cloud and running on shared domain names. For example if a business uses Office 365, they would be working with domain names like `outlook.office.com` and `login.microsoftonline.com`. In the Microsoft example, blocking these addresses would keep users from accessing Outlook on the web entirely, instead of merely restricting them to approved identities and resources.

The solution to this problem is to restrict tenant access, and Cloud Web Security accomplishes this through the use of the **SaaS Header Restriction** feature. This feature allows administrators to enforce tenant restriction policies within SaaS services like Office 365 and G Suite. For example, you may wish to allow access to the Office 365 corporate account for all employees, but forbid them from accessing personal accounts. These restrictions are allowed via insertion of HTTP headers which specify allowed tenants.

Configuring an SaaS Header Restriction

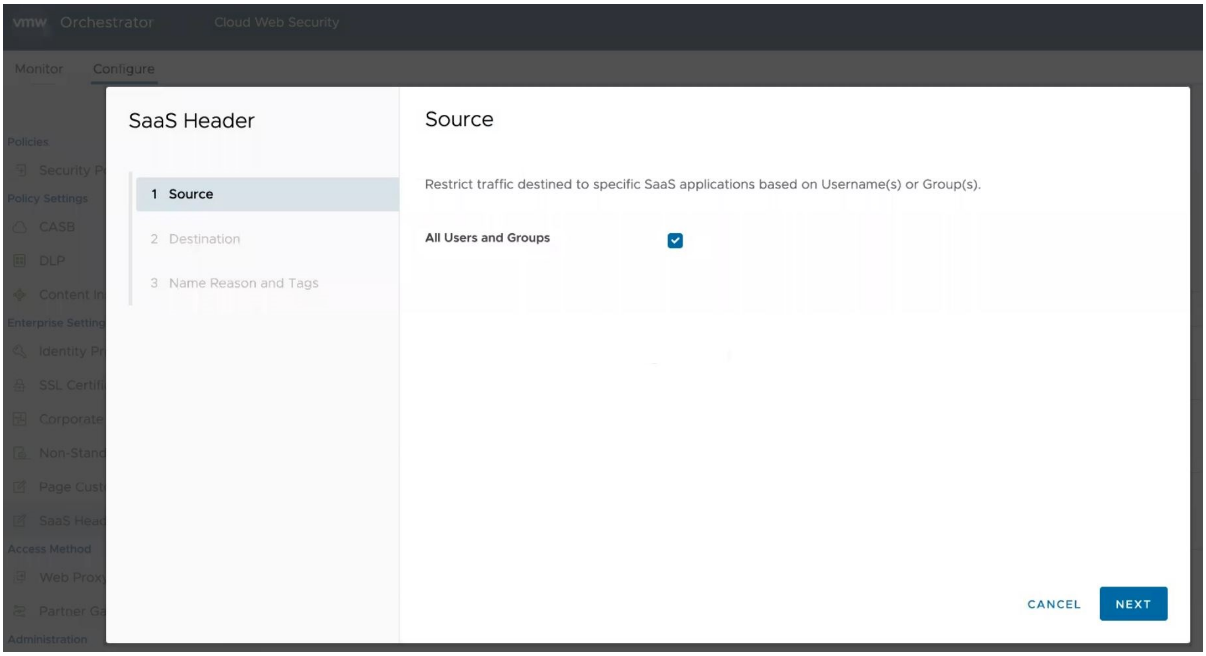
A user can configure an SaaS Header Restriction rule by performing the following steps:

1. Navigate to **Cloud Web Security > Configure > SaaS Header Restrictions**.
2. On the **SaaS Header Restrictions** screen, click **+ ADD RULE** to configure an SaaS Header Restriction rule.



☐	Name	Reason	Source	Destination Applications
☐	test-youtube		Users (1), Groups (0)	YouTube
☐	office-365-enterprise		Users (1), Groups (0)	Office 365 - Enterprise
☐	test-365-consumer		Any	Office 365 - Consumer
☐	test-dropbox1		Any	Dropbox
☐	test-slack		Any	Slack
☐	test-gsuite		Users (1), Groups (0)	G Suite
☐	test-custom		Users (0), Groups (1)	www.google.com

The **SaaS Header > Source** screen appears.



Restrict traffic destined to specific SaaS applications based on Username(s) or Group(s).

All Users and Groups ☑

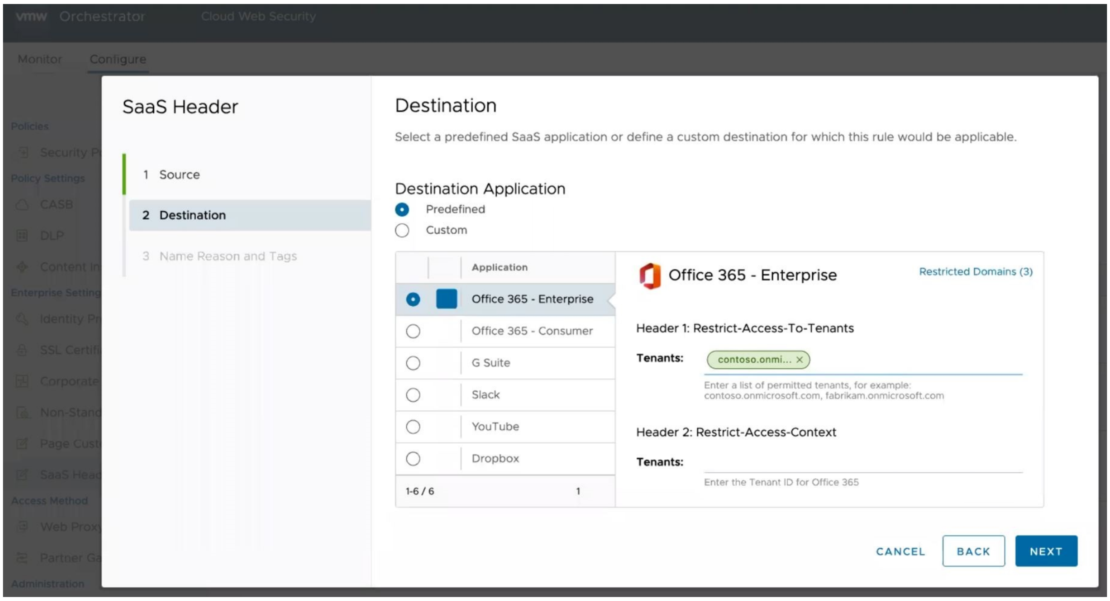
3 In the **Source** screen, choose **All Users and Groups** to have the SaaS Header rule apply to everyone in the enterprise. This option is checked by default. Uncheck this option and choose **Specify User(s)** and **Specify Group(s)** fields to specify one or more users and/or groups to which the rule would apply.

Click **Next**, the **Destination** screen appears.

4 In the **Destination Application** screen, a user has two paths: Predefined or Custom.

   a **Predefined Destination Application**: Select among one of six predefined applications: Office 365 - Enterprise, Office 365 - Consumer, G Suite, Slack, YouTube, and Dropbox. Each preconfigured application includes the restricted domains and headers for that applications. Depending on the application a user may need to manually configure additional information as outlined below:

      1 **Office 365 - Enterprise** presents two additional parameters that must be configured to complete the rule:



Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application

● Predefined

○ Custom

	Application
●	Office 365 - Enterprise
○	Office 365 - Consumer
○	G Suite
○	Slack
○	YouTube
○	Dropbox
1-6 / 6	1

Office 365 - Enterprise

Header 1: Restrict-Access-To-Tenants

Tenants: contoso.onmi... ×

Enter a list of permitted tenants, for example: contoso.onmicrosoft.com, fabrikam.onmicrosoft.com

Header 2: Restrict-Access-Context

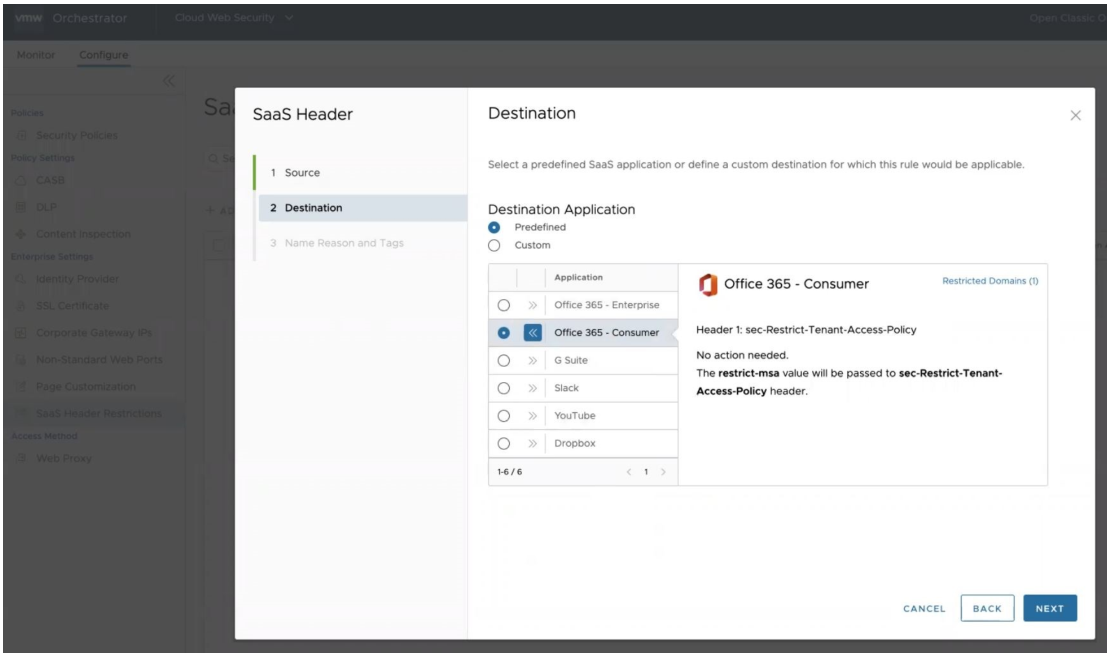
Tenants:

Enter the Tenant ID for Office 365

         a **Header 1: Restrict-Access-To-Tenants** Enter a list of permitted tenants. Anything not listed as permitted will be blocked by Cloud Web Security.

         b **Header 2: Restrict-Access-Context** Enter the Tenant ID for the service used by your enterprise. The user would need to configure the Tenant ID for their subscription to Office 365. Any tenant ID not listed would be blocked by Cloud Web Security.

      2 **Office 365 - Consumer**: contrasts with the Enterprise version by requiring no additional configuration as the restrict-msa value is passed to the sec-Restrict-Tenant-Access-Policy header.



SaaS Header

1 Source
2 Destination
3 Name Reason and Tags

Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application

● Predefined
○ Custom

	Application
○	Office 365 - Enterprise
●	Office 365 - Consumer
○	G Suite
○	Slack
○	YouTube
○	Dropbox

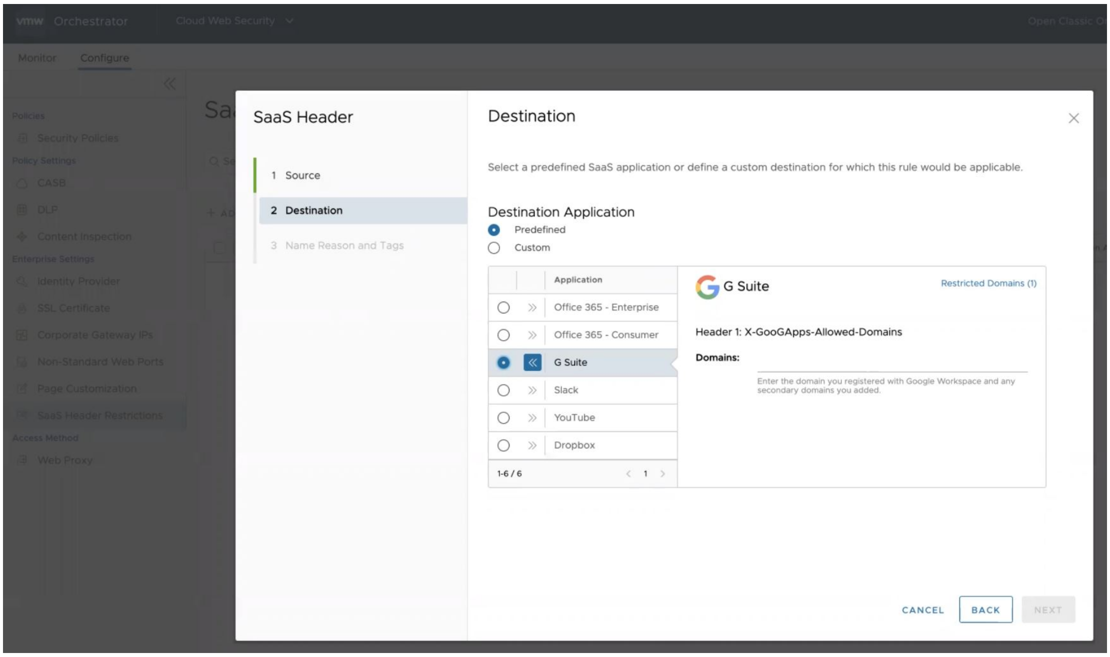
1-6 / 6

Office 365 - Consumer — Restricted Domains (1)

Header 1: sec-Restrict-Tenant-Access-Policy

No action needed.
The **restrict-msa** value will be passed to **sec-Restrict-Tenant-Access-Policy** header.

3 **G Suite**: Enter the domain you registered with Google Workspace along with any secondary domains you added.



SaaS Header

1 Source
2 Destination
3 Name Reason and Tags

Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application

● Predefined
○ Custom

	Application
○	Office 365 - Enterprise
○	Office 365 - Consumer
●	G Suite
○	Slack
○	YouTube
○	Dropbox

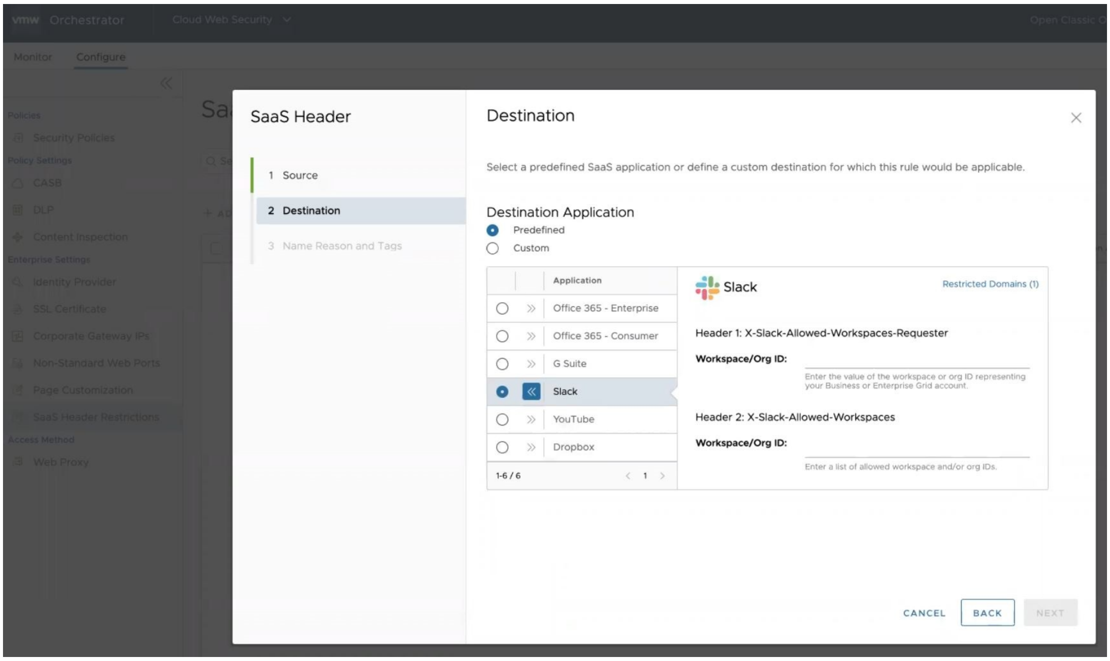
1-6 / 6

G Suite — Restricted Domains (1)

Header 1: X-GooGApps-Allowed-Domains

Domains: Enter the domain you registered with Google Workspace and any secondary domains you added.

4 **Slack** presents two additional fields that you must configure to complete the rule:



Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application
● Predefined
○ Custom

Slack

Header 1: X-Slack-Allowed-Workspaces-Requester

Workspace/Org ID:

Enter the value of the workspace or org ID representing your Business or Enterprise Grid account.

Header 2: X-Slack-Allowed-Workspaces

Workspace/Org ID:

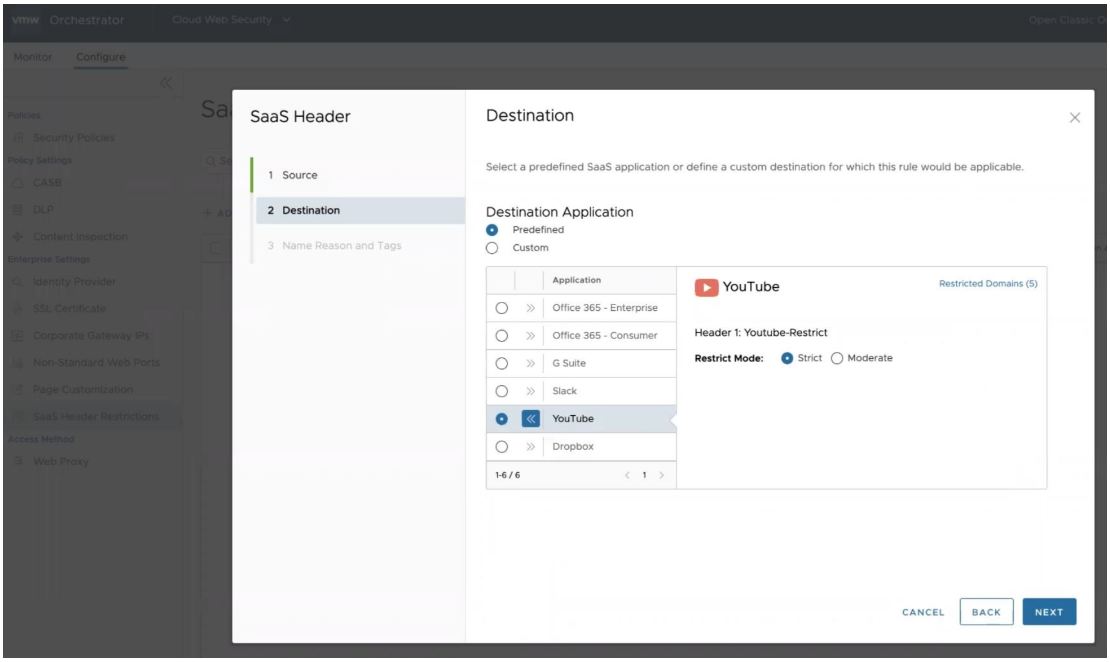
Enter a list of allowed workspace and/or org IDs.

a **Header 1: X-Slack-Allowed-Workspaces-Requester** Enter the value of the workspace or organization ID representing your Business or Enterprise Grid account. Anything not listed as permitted will be blocked by Cloud Web Security.

b **Header 2: X-Slack-Allowed-Workspaces** Enter a list of allowed workspace and/or organizational IDs. Any ID not listed would be blocked by Cloud Web Security.

5 **YouTube**: To complete the rule you need to specify whether you want YouTube's **Restrict Mode** to be **Strict** or **Moderate**. Per YouTube's documentation Manage your organization's YouTube settings, the Restrict Modes are defined as follows:

- **Strict Restricted YouTube access**—This setting is the most restrictive, but it doesn't block all videos. Strict Restricted Mode filters out many videos based on an automated system, while leaving some videos available for viewing.
- **Moderate Restricted YouTube access**—This setting is similar to Strict Restricted Mode, but makes a much larger collection of videos available.



Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application

● Predefined
○ Custom

	Application
○	Office 365 - Enterprise
○	Office 365 - Consumer
○	G Suite
○	Slack
●	YouTube
○	Dropbox

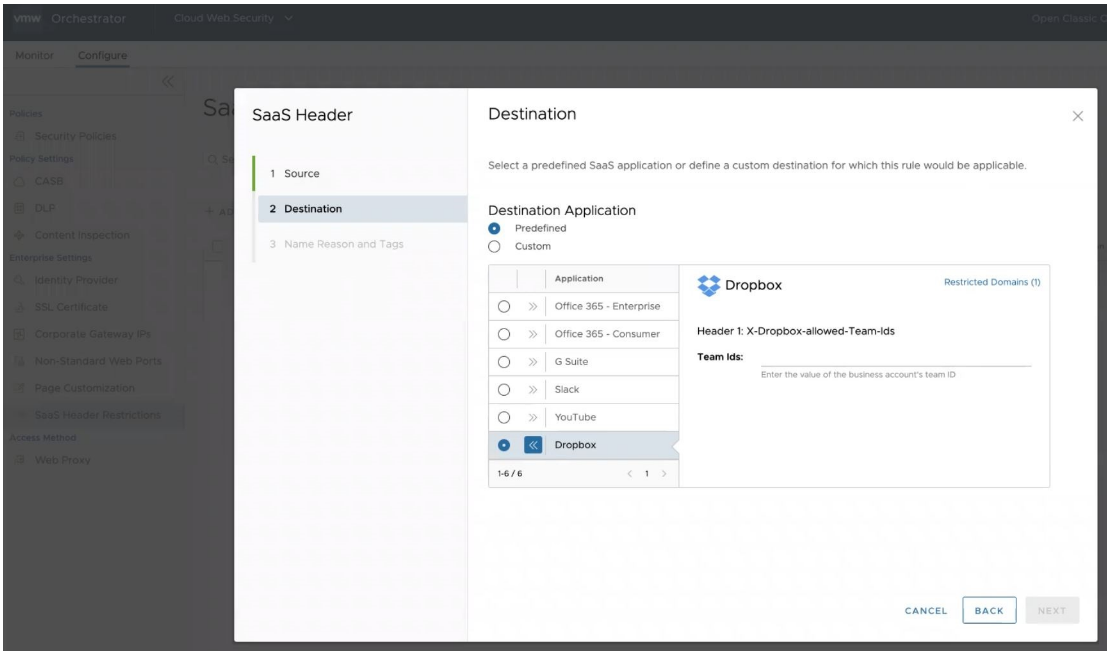
1-6 / 6

YouTube

Header 1: Youtube-Restrict

Restrict Mode: ● Strict ○ Moderate

6 **Dropbox**: Enter the value of the business account's team ID as this will be the only ID allowed by Cloud Web Security.



Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application

● Predefined
○ Custom

	Application
○	Office 365 - Enterprise
○	Office 365 - Consumer
○	G Suite
○	Slack
○	YouTube
●	Dropbox

1-6 / 6

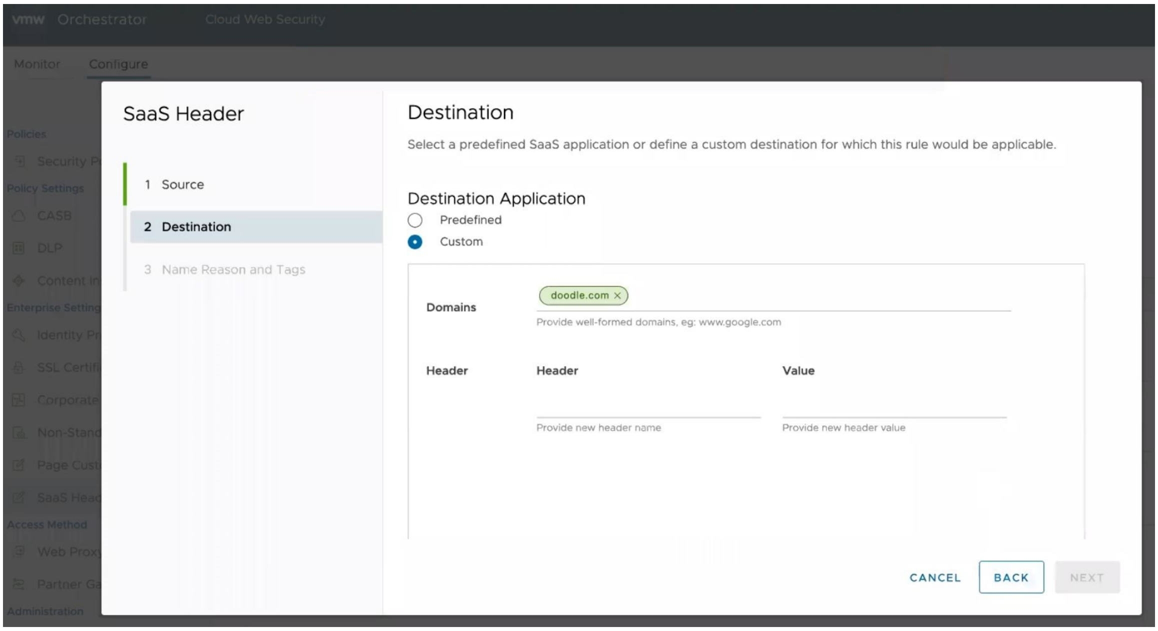
Dropbox

Header 1: X-Dropbox-allowed-Team-Ids

Team Ids: Enter the value of the business account's team ID

Note For any Predefined Application, if there is additional configuration required and you are not certain what those values are, reach out to the customer representative for that application.

b **Custom Destination Application** requires you to enter the SaaS application domains along with all header values associated with the application. As this is a custom application you will need to consult with that application's website and/or customer representative to first confirm that tenant restriction through the use of headers is supported and then locate the domains and header values to ensure this rule is properly configured.



Destination

Select a predefined SaaS application or define a custom destination for which this rule would be applicable.

Destination Application
○ Predefined
● Custom

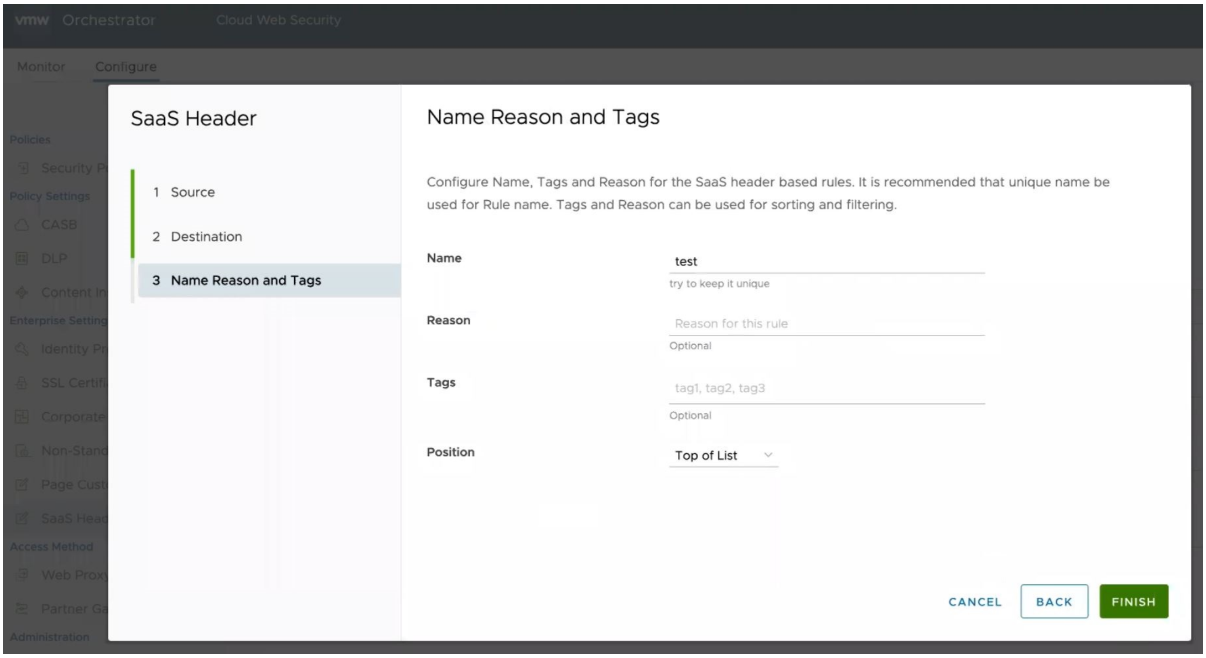
Domains: doodle.com ×
Provide well-formed domains, eg: www.google.com

Header
Header
Provide new header name
Value
Provide new header value

Note Not all SaaS applications support tenant restriction through the use of headers, and it is important when configuring a custom application that you confirm this feature is supported for the application you want to restrict. Only the predefined applications listed earlier are confirmed as compatible with SaaS Header Restriction.

Click **Next**, the **Name, Reasons, and Tags** screen appears.

5 In the **Name, Reason, and Tags** screen, configure a unique Rule Name (required), Reason (if needed), Tags (if used), and a Position for the rule on the list of URL Filtering rules (the options are either 'Top of List' or 'Bottom of List').



SaaS Header

1 Source

2 Destination

3 Name Reason and Tags

Name Reason and Tags

Configure Name, Tags and Reason for the SaaS header based rules. It is recommended that unique name be used for Rule name. Tags and Reason can be used for sorting and filtering.

Name: test
try to keep it unique

Reason: Reason for this rule
Optional

Tags: tag1, tag2, tag3
Optional

Position: Top of List

6 Click **Finish** and the newly created rule appears in the **SaaS Header Restriction** list and is applied.

Additional Resources for Predefined Applications

Below are links to documentation for the predefined application destinations to better inform you about how tenant restriction through headers works for each application.

- **Microsoft Office 365**
  - Use tenant restrictions to manage access to SaaS apps
  - Block access to consumer accounts
- **G Suite**
  - Block access to consumer accounts
- **Slack**
  - Approve Slack workspaces for your network
- **YouTube**
  - Control YouTube content available to users
  - Manage your organization's YouTube settings (Restrict Modes)
- **Dropbox**
  - Network Control for the Dropbox Application

Web Proxy Configuration

9

This section covers the configuration of the VMware Cloud Web Security Web Proxy feature.

Read the following topics next:

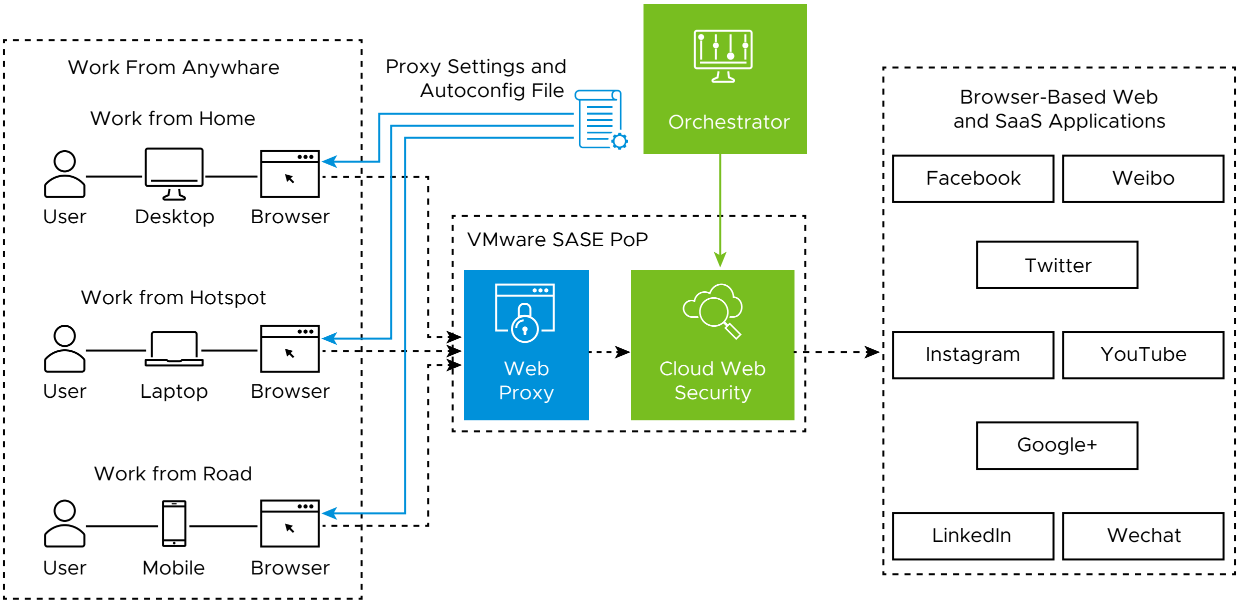
- Web Proxy Overview
- Prerequisites
- Activate Web Proxy
- Proxy Auto-Config Files
- Configure Host
- Troubleshoot Web Proxy

Web Proxy Overview

The VMware Cloud Web Security (CWS) Web Proxy feature is designed to activate the standalone use of the Cloud Web Security service 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-configured (PAC) file can have its Web traffic redirected to the VMware Cloud Web Security service for security inspection.

The Web Proxy Service is hosted by a VMware SASE Point of Presence (PoP) and activated using the VMware Cloud Orchestrator. When users activate the Web Proxy functionality in CWS:

- 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

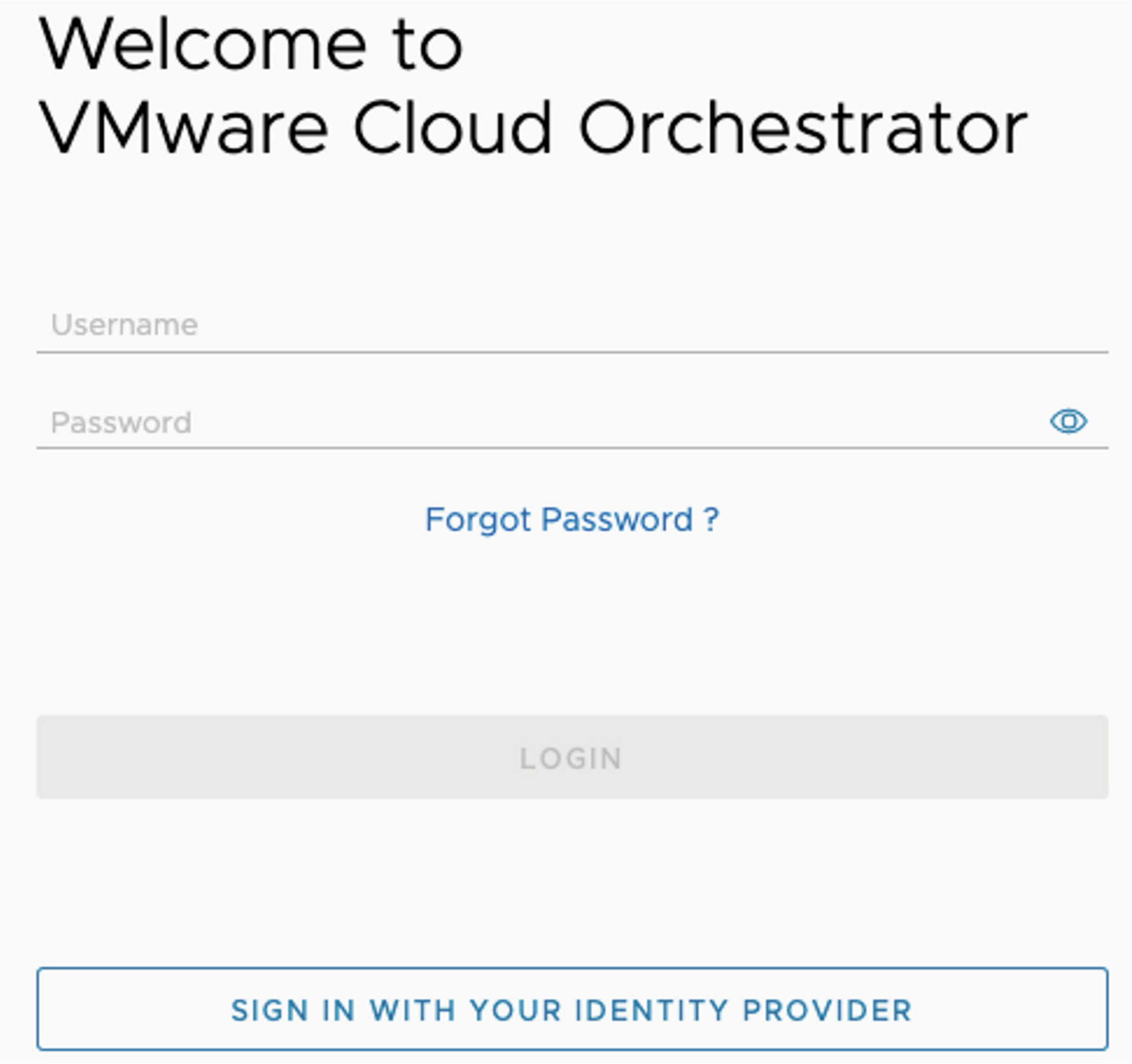
The following are the perquisites for the Cloud Web Security Web Proxy configuration.

SSL Certificate

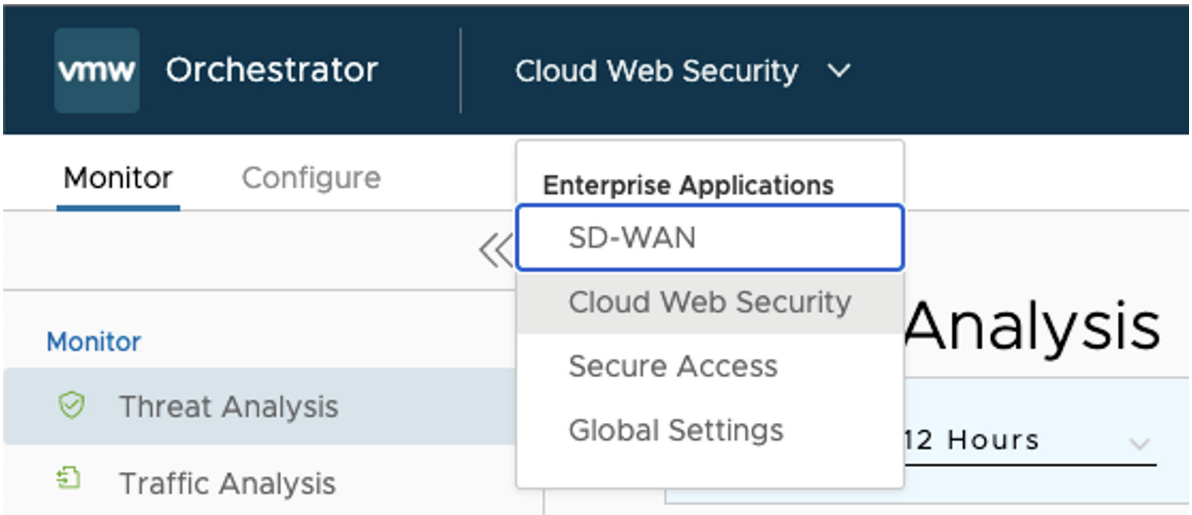
When users first connect to the Web Proxy, users would open their browser and navigate to a website for example, an HTTPS site. The Web Proxy performs an SSL intercept of this traffic and returns a redirect to the authentication service. So, it is recommended to have the VMware Root Certificate installed on the endpoint instead of instructing users to accept the security warning.

To retrieve the root certificate and install it on a host, perform the following steps:

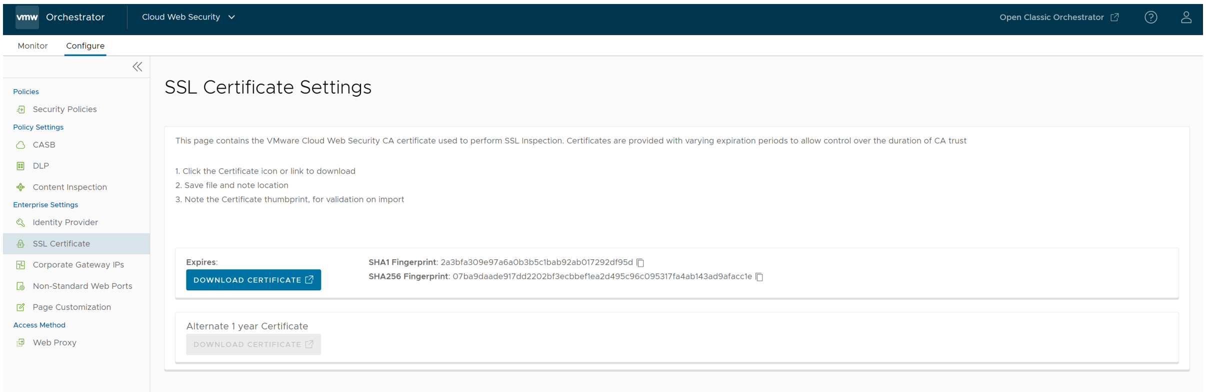
1 Open a web browser and navigate to VMware Cloud Orchestrator.


Welcome to
VMware Cloud Orchestrator
Username
Password
Forgot Password ?
LOGIN
SIGN IN WITH YOUR IDENTITY PROVIDER

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



3 Click on the **Configure** tab and under **Enterprise Settings**, select **SSL Certificate**. The **SSL Certificate Settings** screen appears.



SSL Certificate Settings

This page contains the VMware Cloud Web Security CA certificate used to perform SSL Inspection. Certificates are provided with varying expiration periods to allow control over the duration of CA trust

1. Click the Certificate icon or link to download
2. Save file and note location
3. Note the Certificate thumbprint, for validation on import

Expires:

SHA1 Fingerprint: 2a3bfa309e97a6a0b3b5c1bab92ab017292df95d

SHA256 Fingerprint: 07ba9daade917dd2202bf3ecbbef1ea2d495c96c095317fa4ab143ad9afacc1e

Alternate 1 year Certificate

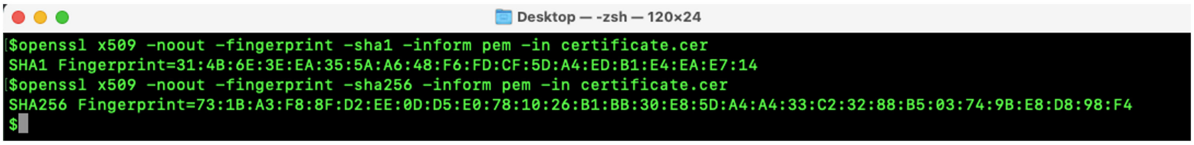
4 Click on **Download Certificate** and save the file to the host machine.

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.

The following are the OpenSSL Commands to Compute Certificate Fingerprint:

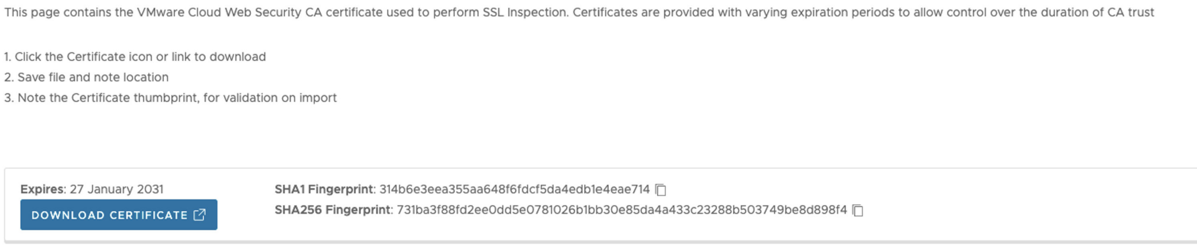
```
$openssl x509 -noout -fingerprint -sha1 -inform pem -in certificate.cer
$openssl x509 -noout -fingerprint -sha256 -inform pem -in certificate.cer
```

Figure 9-1. OpenSSL Commands in Terminal



```
[$openssl x509 -noout -fingerprint -sha1 -inform pem -in certificate.cer
SHA1 Fingerprint=31:4B:6E:3E:EA:35:5A:A6:48:F6:FD:CF:5D:A4:ED:B1:E4:EA:E7:14
[$openssl x509 -noout -fingerprint -sha256 -inform pem -in certificate.cer
SHA256 Fingerprint=73:1B:A3:F8:8F:D2:EE:0D:D5:E0:78:10:26:B1:BB:30:E8:5D:A4:A4:33:C2:32:88:B5:03:74:9B:E8:D8:98:F4
$
```

Figure 9-2. SSL Certificate SHA1, SHA256 Fingerprints



This page contains the VMware Cloud Web Security CA certificate used to perform SSL Inspection. Certificates are provided with varying expiration periods to allow control over the duration of CA trust

1. Click the Certificate icon or link to download
2. Save file and note location
3. Note the Certificate thumbprint, for validation on import

Expires: 27 January 2031

SHA1 Fingerprint: 314b6e3eea355aa648f6fdcf5da4edb1e4eae714

SHA256 Fingerprint: 731ba3f88fd2ee0dd5e0781026b1bb30e85da4a433c23288b503749be8d898f4

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:

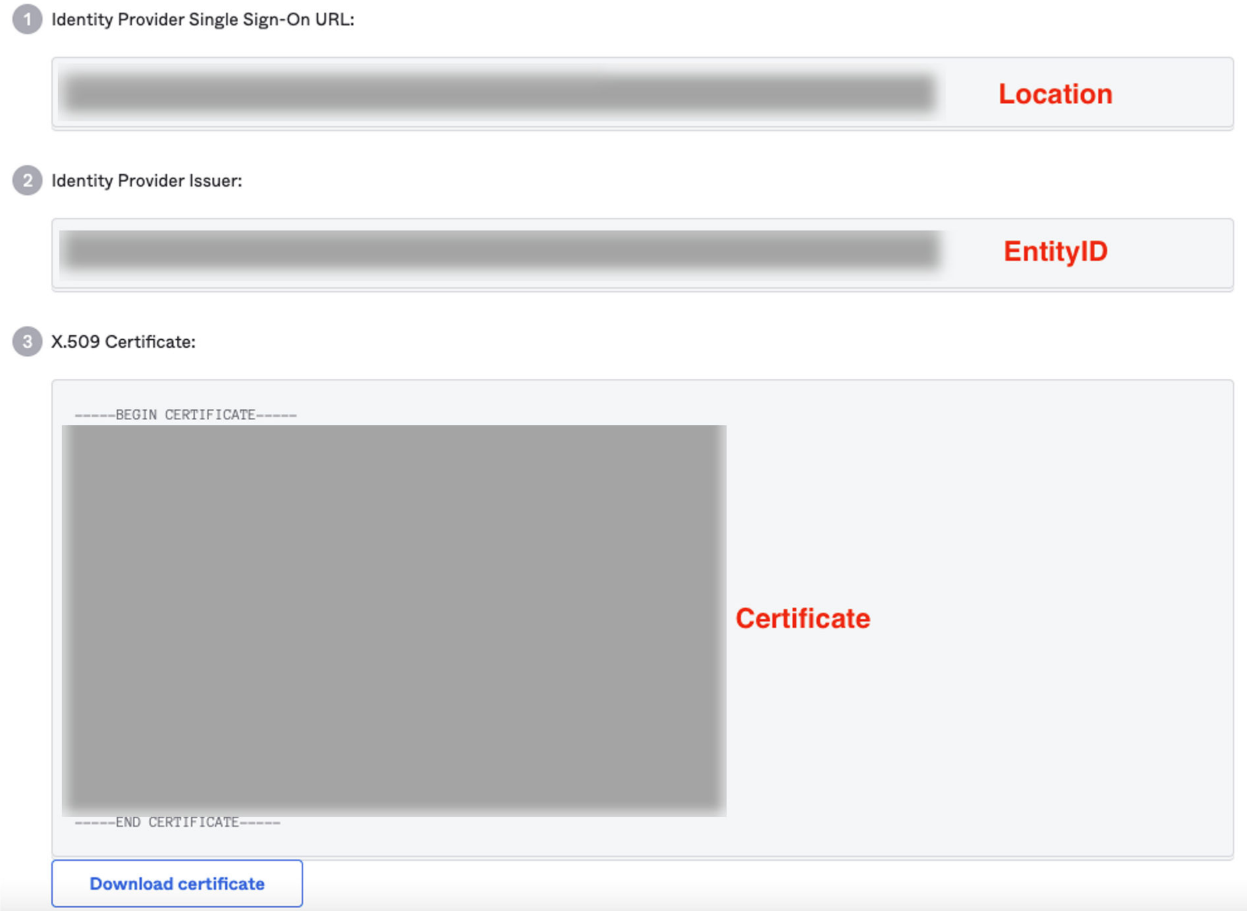
- Google Chrome
- Mozilla Firefox

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.

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

Figure 9-3. Okta Configuration for VMware Integration



1 Identity Provider Single Sign-On URL:

2 Identity Provider Issuer:

3 X.509 Certificate:

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

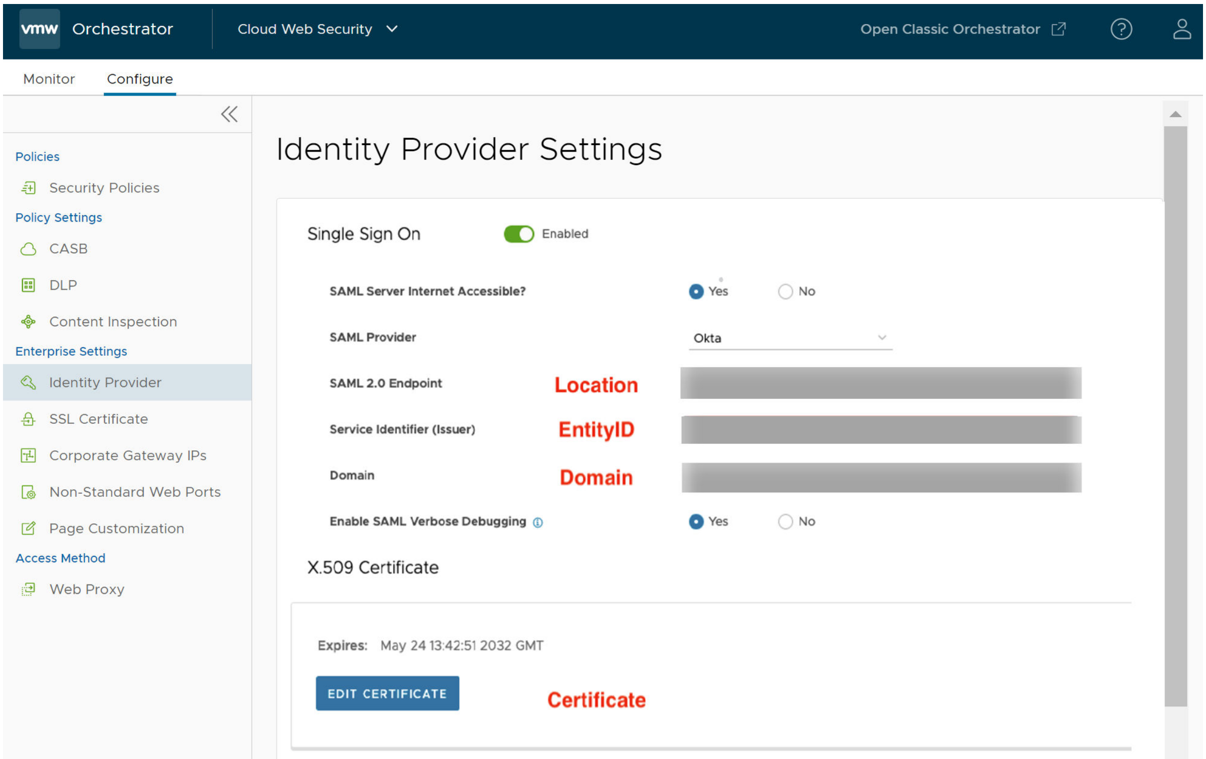
-----END CERTIFICATE-----

- 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.

Activating Single Sign On (SSO)

To integrate an IdP and configure IdP information in CWS, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Enterprise Settings > Identity Provider**. The following screen appears.



Identity Provider Settings

Single Sign On: Enabled

SAML Server Internet Accessible? ● Yes ○ No

SAML Provider: Okta

SAML 2.0 Endpoint: [redacted]

Service Identifier (Issuer): [redacted]

Domain: [redacted]

Enable SAML Verbose Debugging: ● Yes ○ No

X.509 Certificate

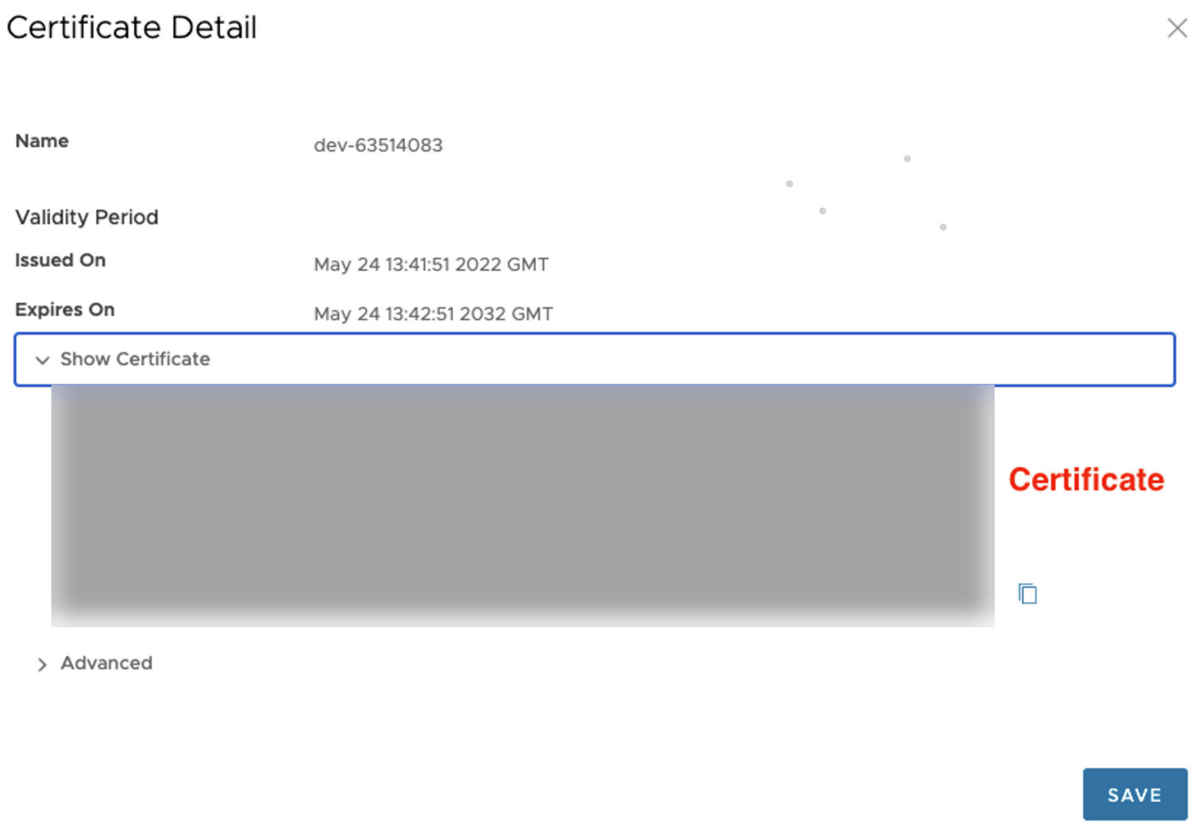
Expires: May 24 13:42:51 2032 GMT

2 Turn on the **Single Sign On** toggle button and enter the following details:

Field	Description
SAML Server Internet Accessible	Select Yes to access SAML Server Internet.
SAML Provider	Select Okta from the list.
SAML 2.0 Endpoint	Copy and paste the **Location** information from the IdP.
Service Identifier (Issuer)	Copy and paste the **EntityID** information from the IdP.
Domain	Enter your company's domain (for example, vmware.com). **Note** Users will authenticate to the service using their email address. The user's email domain must match what is configured here.
Enable SAML Verbose Debugging	Select Yes or No depending on whether you want to activate SAML Verbose Debugging. By default, SAML debugging is deactivated unless troubleshooting SAML login issues.

3 After setting the above attributes, ensure to save the changes by clicking the **Save Changes** button.

4 Click the **Edit Certificate** button to configure the IdP certificate information in CWS. The **Certificate Detail** pop-up window appears.



Certificate Detail

Name dev-63514083

Validity Period

Issued On May 24 13:41:51 2022 GMT

Expires On May 24 13:42:51 2032 GMT

5 Under the **Show Certificate** section, paste the Certificate information copied from the IdP and click **Save**.

6 After configuring all the required IdP information, click **Save Changes**.

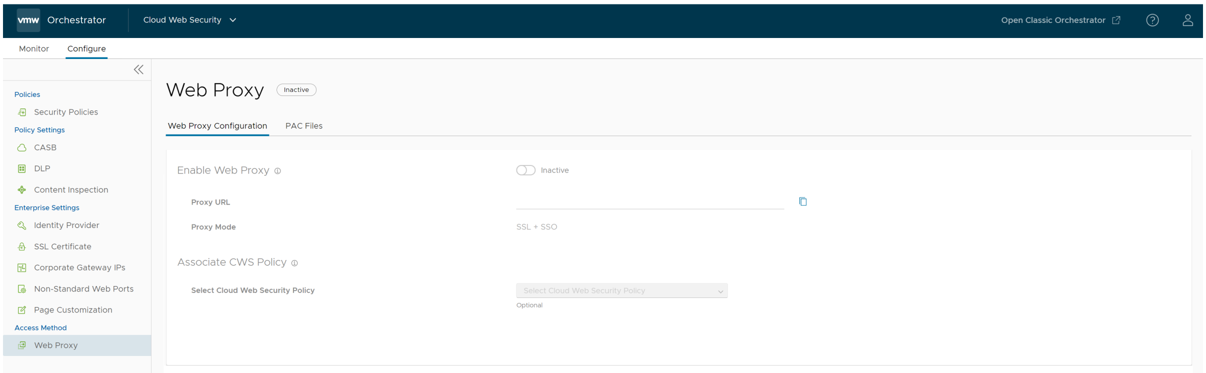
Activate Web Proxy

Users can activate the Web Proxy service, associate a Cloud Web Security policy, and generate a PAC file from the Web Proxy configuration screen.

Note Before activating Web Proxy service, ensure Single Sign On (SSO) is activated.

To activate the Web Proxy service, perform the following the service:

1 Navigate to **Cloud Web Security** > **Configure** > **Access Method** > **Web Proxy**. The **Web Proxy** screen appears.



Enable Web Proxy: Inactive

Proxy URL:

Proxy Mode: SSL + SSO

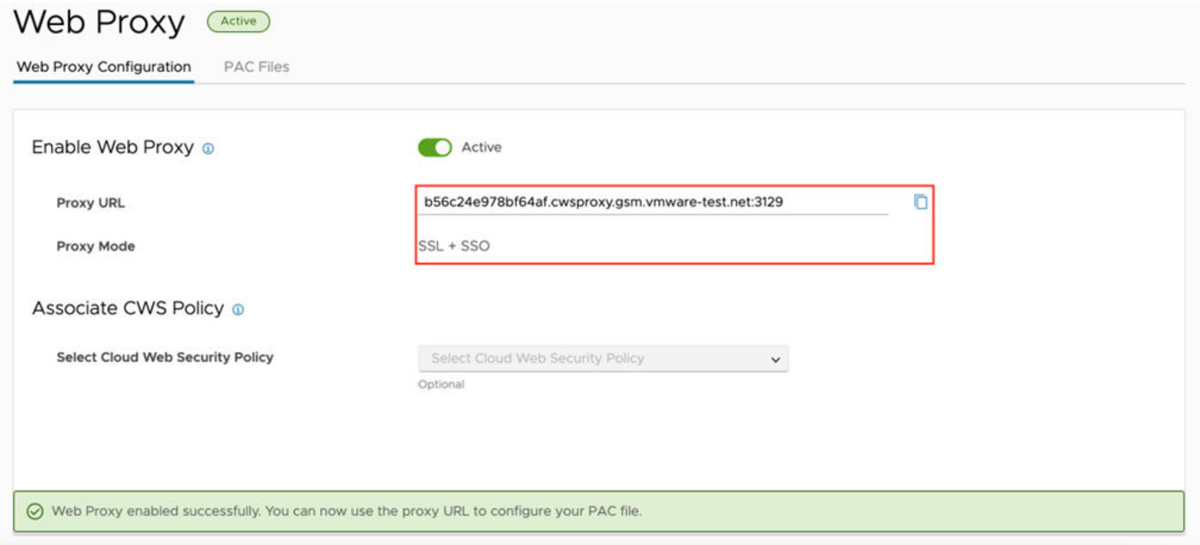
Associate CWS Policy

Select Cloud Web Security Policy: Select Cloud Web Security Policy (Optional)

2 In the **Web Proxy Configuration** tab, turn on the **Enable Web Proxy** toggle button.

3 The Web Proxy service changes from the **Inactive** state to the **Active** state.

4 After the service is activated, the Proxy URL and Proxy Mode information are auto populated and appears in the **Web Proxy** Configuration screen:



Enable Web Proxy: Active

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

Proxy Mode: SSL + SSO

Associate CWS Policy

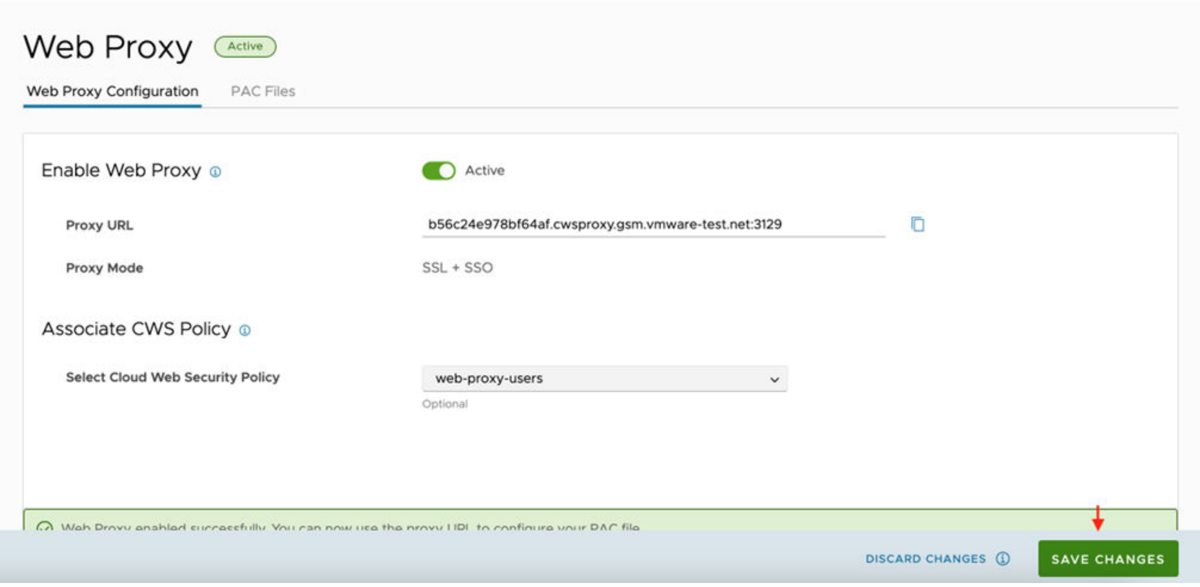
Select Cloud Web Security Policy: Select Cloud Web Security Policy (Optional)

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

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

The Web Proxy is activated, and users can use the Proxy URL to configure Proxy Auto-Config (PAC) file. For more information, see Proxy Auto-Config Files.

5 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. To associate a Cloud Web Security policy for Web Proxy users, select a policy from the **Select Cloud Web Security Policy** drop-down menu.



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)

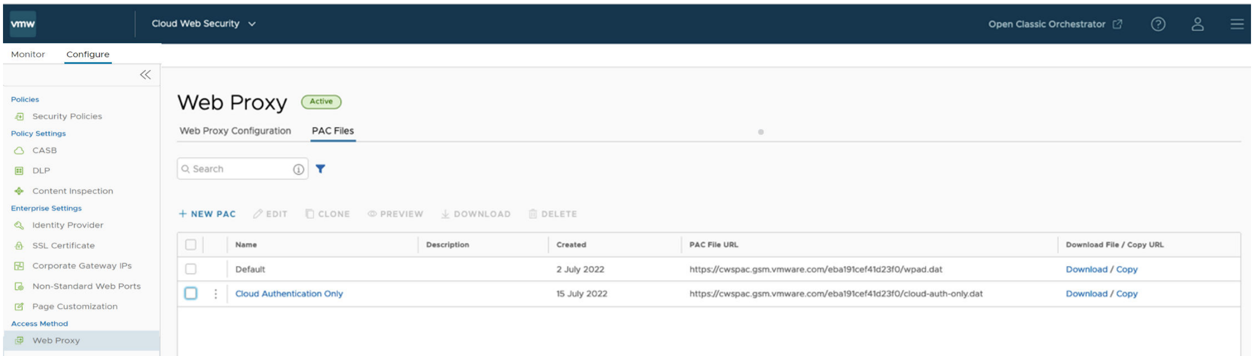
Web Proxy enabled successfully. You can now use the proxy URL to configure your PAC file.

6 Click **Save Changes**.

Proxy Auto-Config Files

When the Web Proxy Configuration is activated, Cloud Web Security automatically creates a default Proxy Auto-Config (PAC) file. Users can also create custom PAC file(s) based on their organization’s needs when connecting to the service.

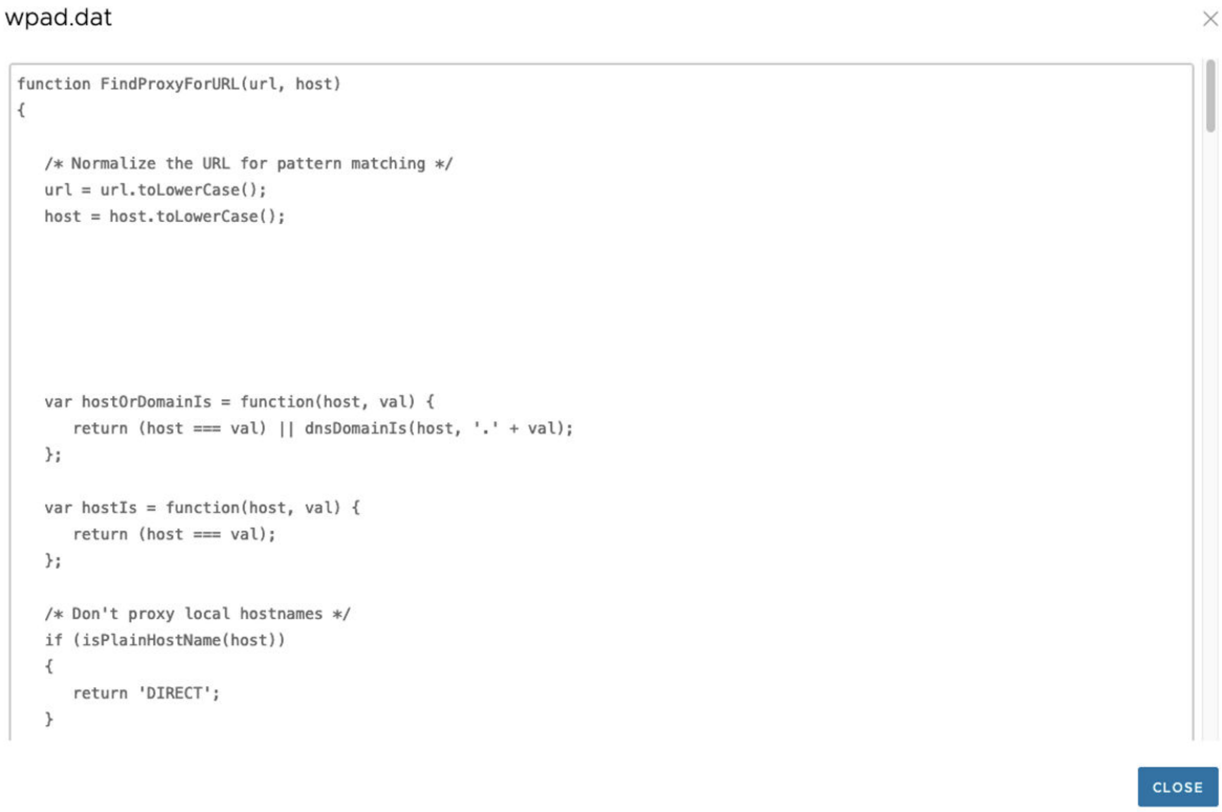
Users can view or configure the PAC files in CWS by navigating to **Cloud Web Security > Configure > Access Method > Web Proxy > PAC Files**.



☐	Name	Description	Created	PAC File URL	Download File / Copy URL
☐	Default		2 July 2022	https://cwspac.gsm.vmware.com/eba191cef41d23f0/wpad.dat	Download / Copy
☐	Cloud Authentication Only		15 July 2022	https://cwspac.gsm.vmware.com/eba191cef41d23f0/cloud-auth-only.dat	Download / Copy

Default PAC File

The **Default** PAC File is read-only. To view the Default PAC file's configuration details, select the **Default** PAC File and then click the **PREVIEW** button.



```
function FindProxyForURL(url, host)
{

   /* Normalize the URL for pattern matching */
   url = url.toLowerCase();
   host = host.toLowerCase();






   var hostOrDomainIs = function(host, val) {
      return (host === val) || dnsDomainIs(host, '.' + val);
   };

   var hostIs = function(host, val) {
      return (host === val);
   };

   /* Don't proxy local hostnames */
   if (isPlainHostName(host))
   {
      return 'DIRECT';
   }
```

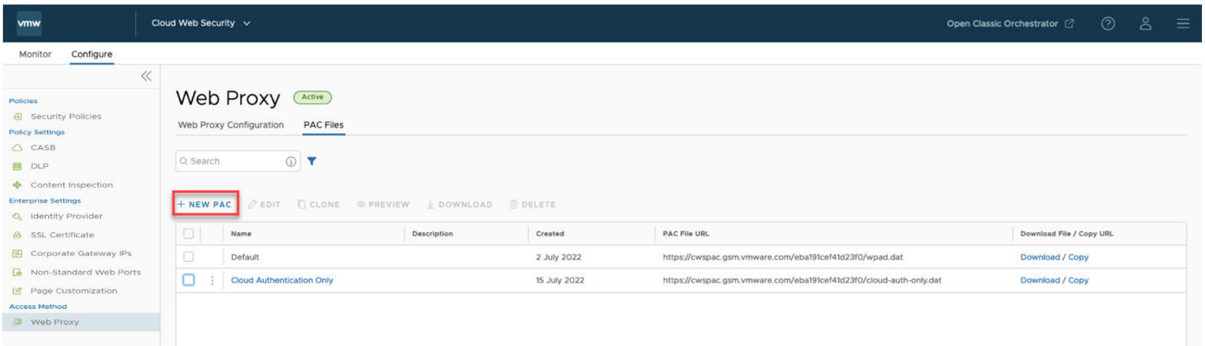
While users do not need to concern themselves with creating the exact syntax, as the built-in wizard will guide them through PAC file configuration, it is useful to understand the directives in the file.

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 File

To create a custom PAC file, perform the following steps:

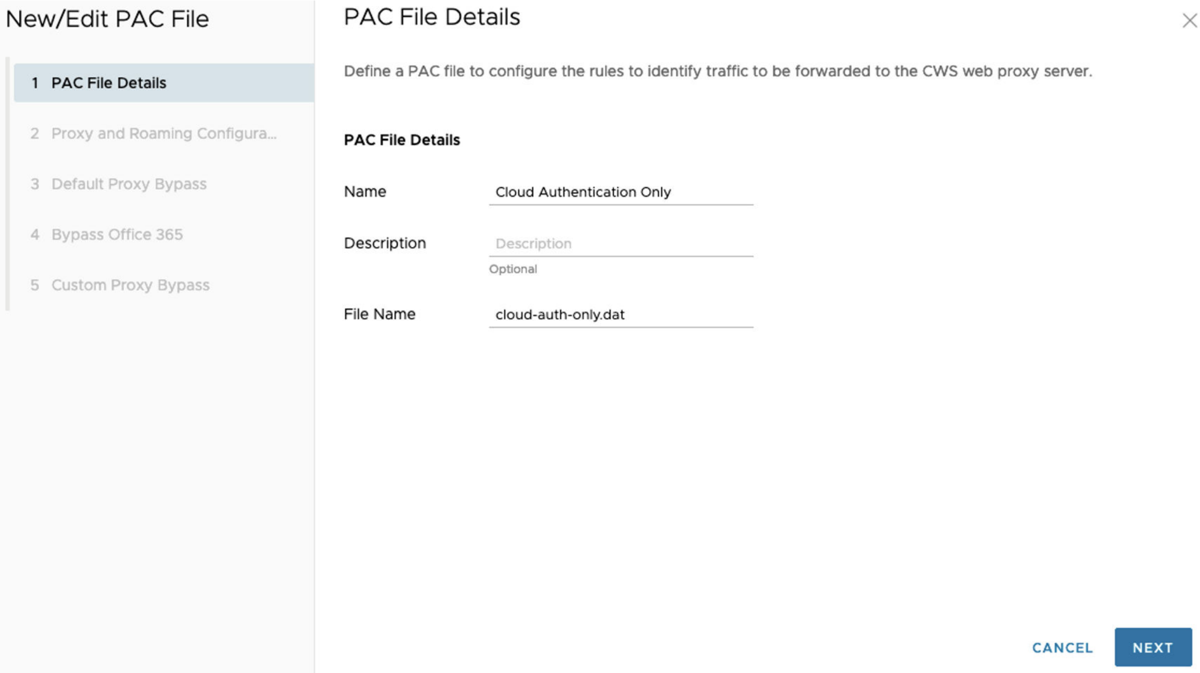
1 Navigate to **Cloud Web Security > Configure > Access Method > Web Proxy > PAC Files**.



Name	Description	Created	PAC File URL	Download File / Copy URL
Default		2 July 2022	https://cwspac.gsm.vmware.com/eba191cef41d23f0/wpad.dat	Download / Copy
Cloud Authentication Only		15 July 2022	https://cwspac.gsm.vmware.com/eba191cef41d23f0/cloud-auth-only.dat	Download / Copy

2 Click **+ NEW PAC** on the **PAC Files** configuration page.

The **New/Edit PAC File** page appears.



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

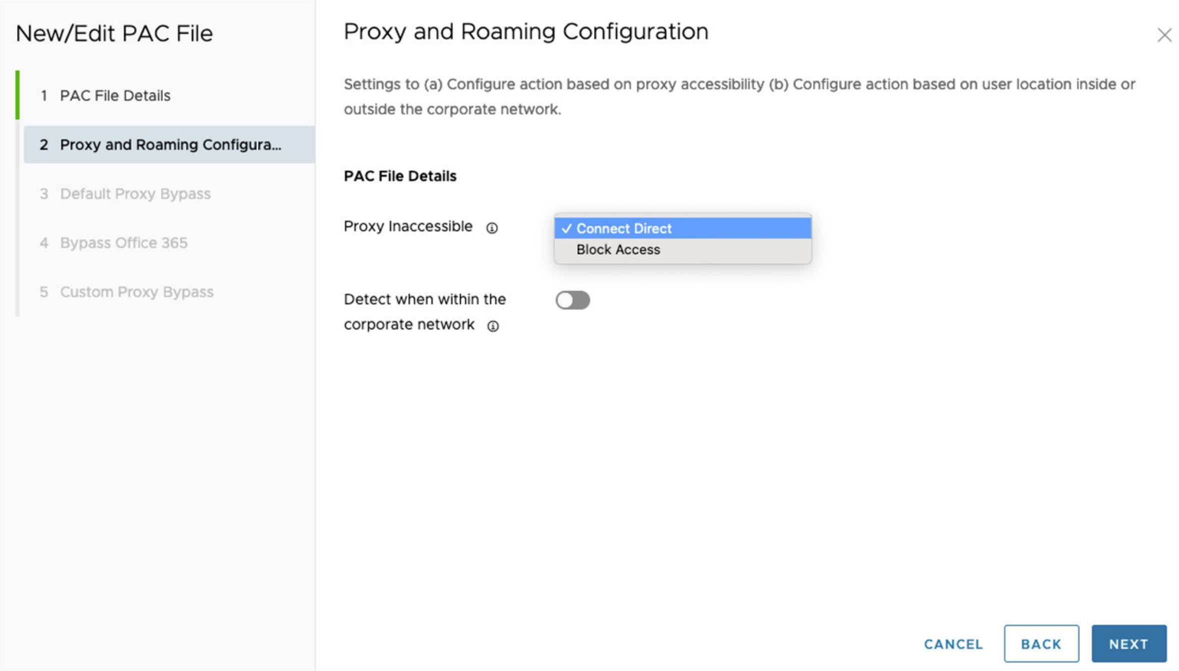
Description: Description (Optional)

File Name: cloud-auth-only.dat

3 In the **PAC File Details** page, enter the required PAC file details and click **Next**.

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

4 The **Proxy and Roaming Configuration** page allows users to determine how their remote clients connect to the proxy service when using this PAC file by configuring actions based on the following parameters:



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

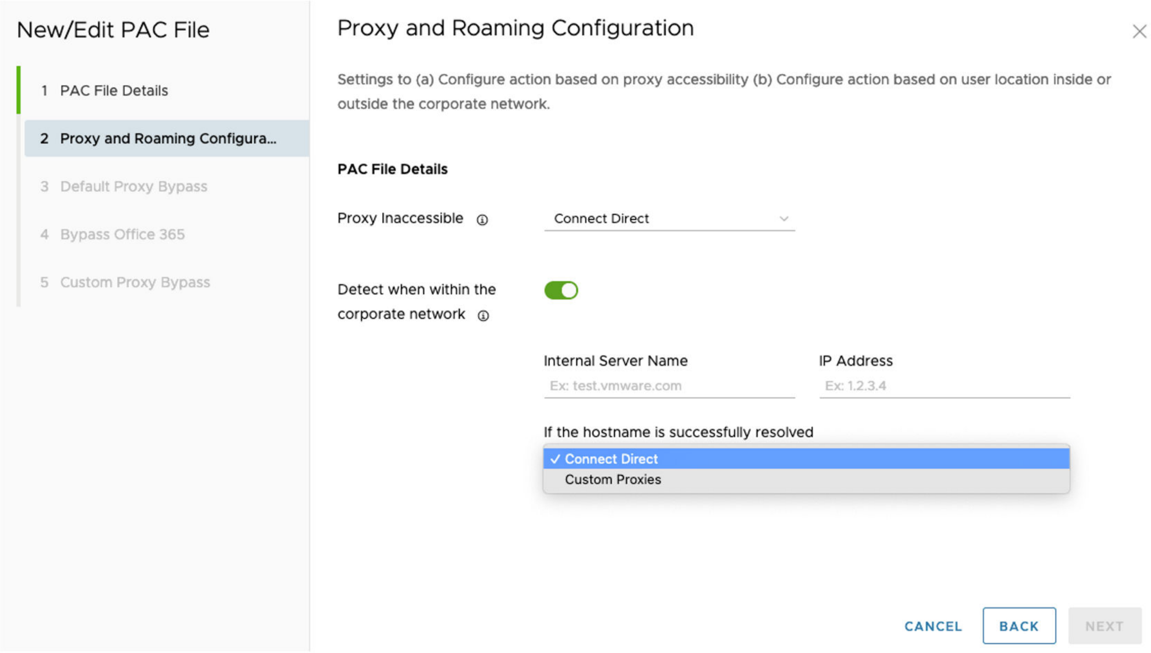
Settings to (a) Configure action based on proxy accessibility (b) Configure action based on user location inside or outside the corporate network.

PAC File Details

Proxy Inaccessible: ✓ Connect Direct / Block Access

Detect when within the corporate network: ○

- **Proxy Inaccessible** - Users can select either **Connect Direct** or **Block Access** options based on if clients should or should not be allowed to the Internet if the proxy is inaccessible.
- **Detect when within the corporate network** - Toggle the button ON to determine if the client is within a 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: Ex: test.vmware.com

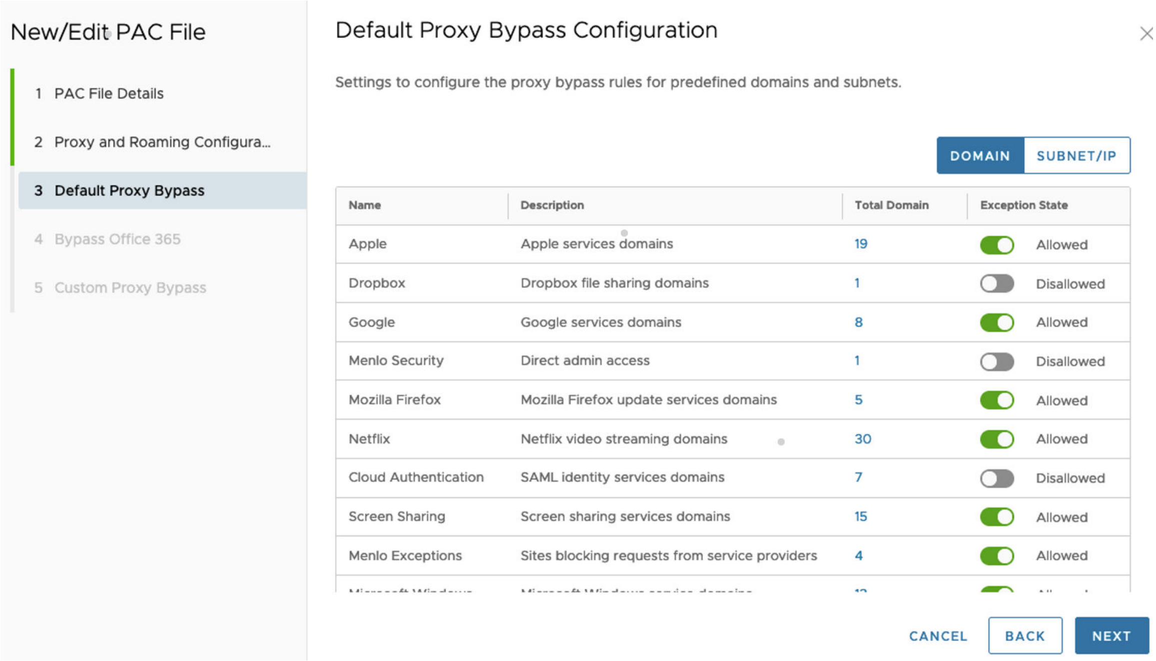
IP Address: Ex: 1.2.3.4

If the hostname is successfully resolved: ✓ Connect Direct / Custom Proxies

- If the client is within the corporate network, users can configure an action if the client should use the corporate network's Internet access or be redirected to an on-premises proxy server by entering the following details:
  - **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.
- Click **Next**. The **Default Proxy Bypass Configuration** page appears.

5 In the **Default Proxy Bypass Configuration** page, users can configure proxy bypass rules for predefined domains and subnet/IPs that should not be sent to the Web Proxy.

- Click the **Domain** button and under the **Exception State** column, toggle the button to turn On or Off the domains that should be allowed or bypassed from proxy.

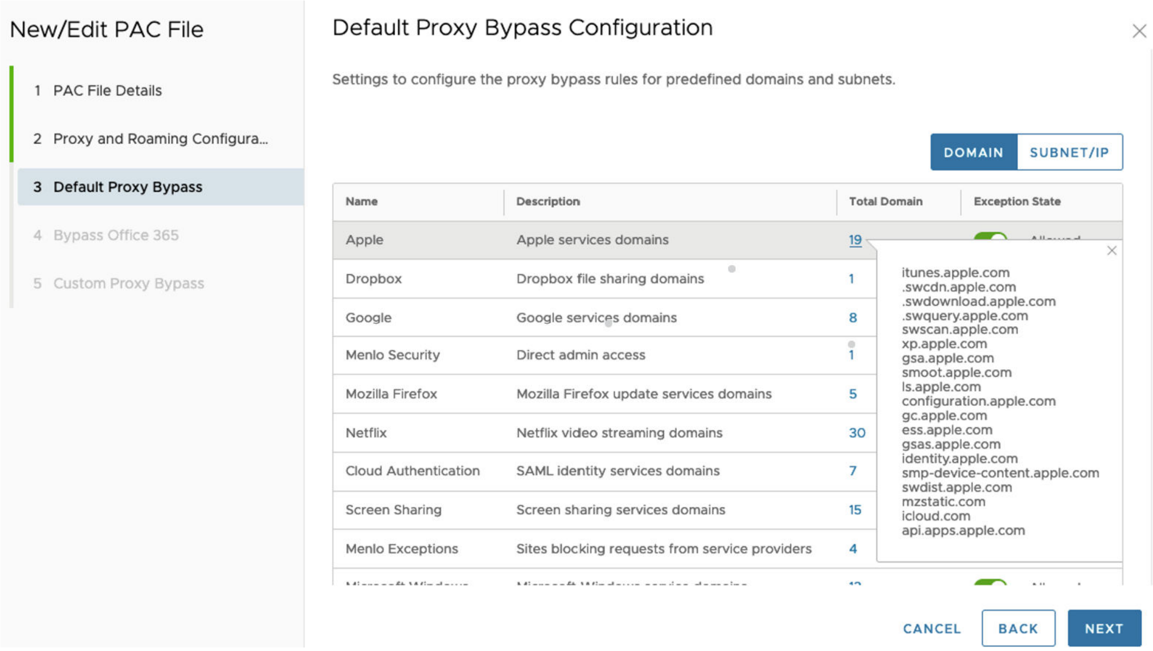


Default Proxy Bypass Configuration

Settings to configure the proxy bypass rules for predefined domains and subnets.

Name	Description	Total Domain	Exception State
Apple	Apple services domains	19	Allowed
Dropbox	Dropbox file sharing domains	1	Disallowed
Google	Google services domains	8	Allowed
Menlo Security	Direct admin access	1	Disallowed
Mozilla Firefox	Mozilla Firefox update services domains	5	Allowed
Netflix	Netflix video streaming domains	30	Allowed
Cloud Authentication	SAML identity services domains	7	Disallowed
Screen Sharing	Screen sharing services domains	15	Allowed
Menlo Exceptions	Sites blocking requests from service providers	4	Allowed

- Under the **Total Domain** column, click the number link to view the domains associated to the application.



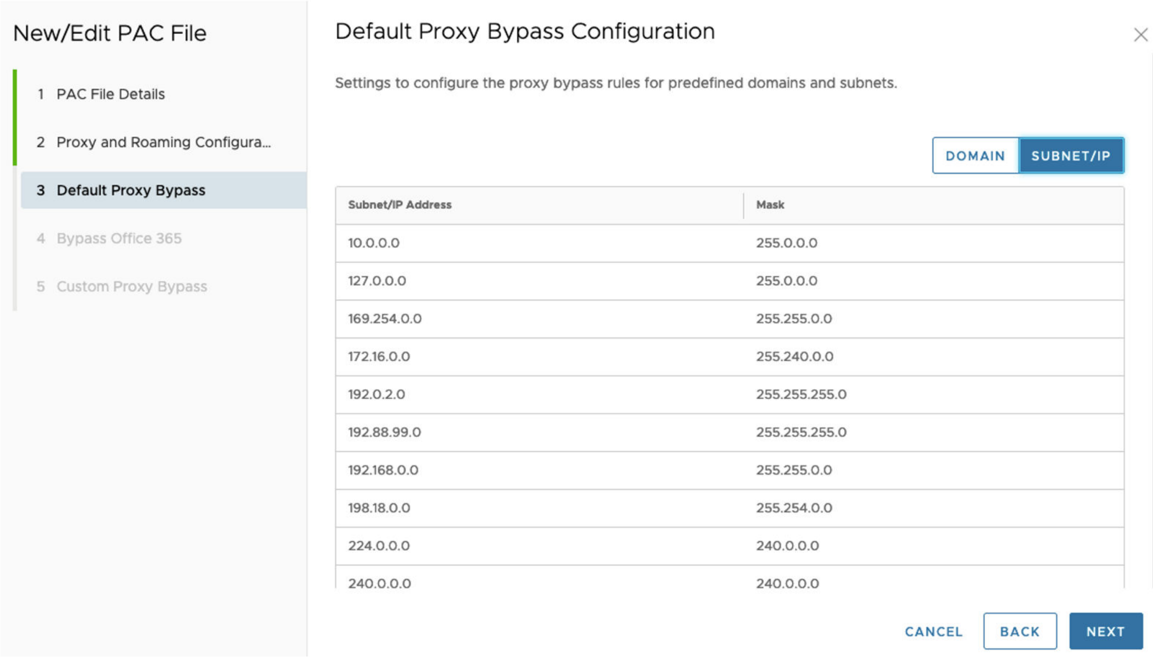
Default Proxy Bypass Configuration

Settings to configure the proxy bypass rules for predefined domains and subnets.

Name	Description	Total Domain	Exception State
Apple	Apple services domains	19	
Dropbox	Dropbox file sharing domains	1	
Google	Google services domains	8	
Menlo Security	Direct admin access	1	
Mozilla Firefox	Mozilla Firefox update services domains	5	
Netflix	Netflix video streaming domains	30	
Cloud Authentication	SAML identity services domains	7	
Screen Sharing	Screen sharing services domains	15	
Menlo Exceptions	Sites blocking requests from service providers	4	

itunes.apple.com
.swcdn.apple.com
.swdownload.apple.com
.swquery.apple.com
swscan.apple.com
xp.apple.com
gsa.apple.com
smoot.apple.com
ls.apple.com
configuration.apple.com
gc.apple.com
ess.apple.com
gsas.apple.com
identity.apple.com
smp-device-content.apple.com
swdist.apple.com
mzstatic.com
icloud.com
api.apps.apple.com

- Click the **Subnet/IP** button to view the subnets excluded from Web Proxy.



Default Proxy Bypass Configuration

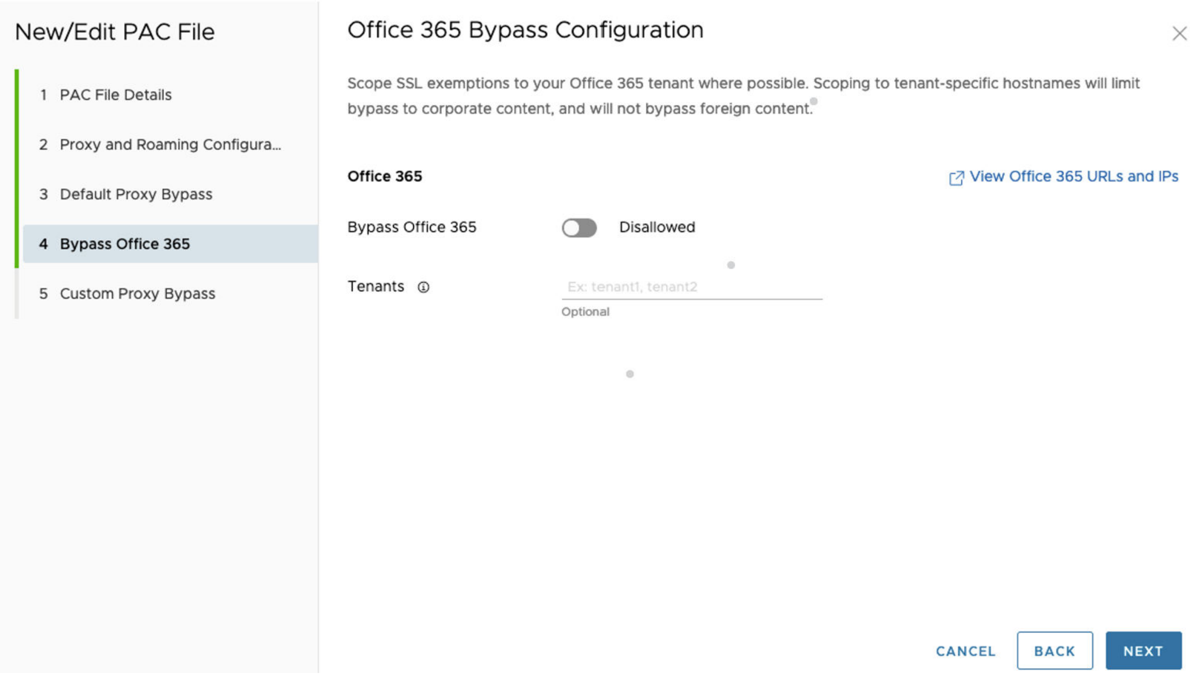
Settings to configure the proxy bypass rules for predefined domains and subnets.

Subnet/IP Address	Mask
10.0.0.0	255.0.0.0
127.0.0.0	255.0.0.0
169.254.0.0	255.255.0.0
172.16.0.0	255.240.0.0
192.0.2.0	255.255.255.0
192.88.99.0	255.255.255.0
192.168.0.0	255.255.0.0
198.18.0.0	255.254.0.0
224.0.0.0	240.0.0.0
240.0.0.0	240.0.0.0

- Click **Next**. The **Office 365 Bypass Configuration** page appears.

6 In the **Office 365 Bypass Configuration** page, configure bypass of Microsoft 365 domains and specific tenants and click **Next**.

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.



Scope SSL exemptions to your Office 365 tenant where possible. Scoping to tenant-specific hostnames will limit bypass to corporate content, and will not bypass foreign content.

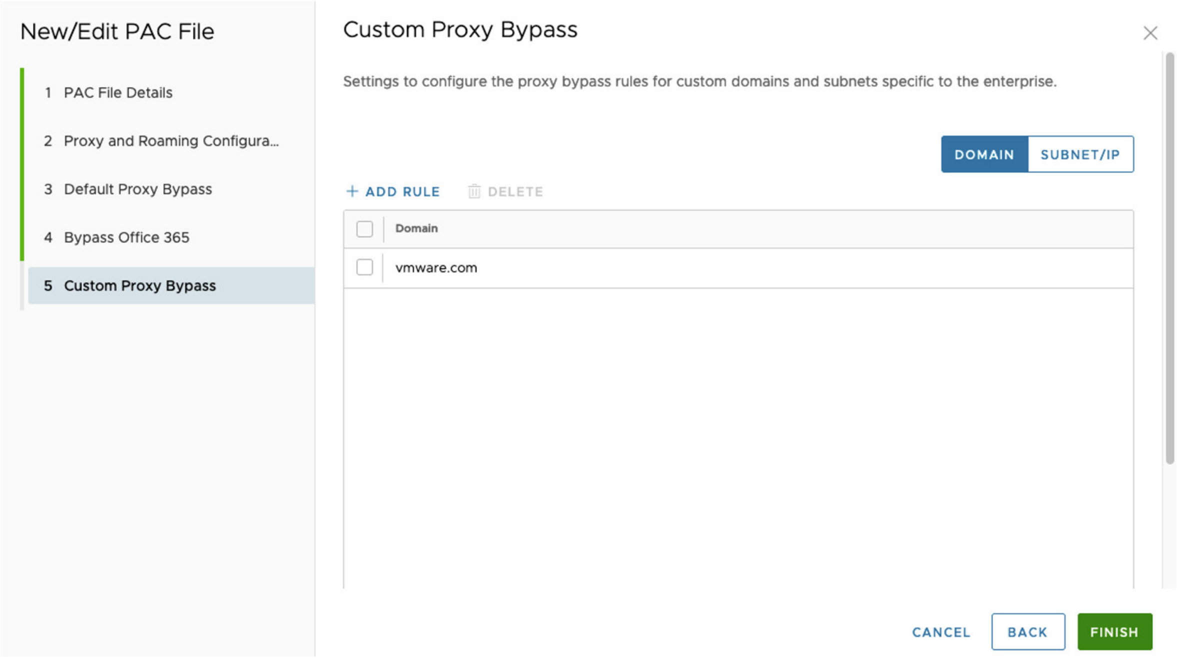
Office 365

Bypass Office 365 ○ Disallowed

Tenants: Ex: tenant1, tenant2 (Optional)

- **Bypass Office 365** - Toggle the button ON to allow easy bypass of Microsoft 365 domains. These domains will be added to the PAC file to be bypassed.
- **Tenants** - Specify your company specific subdomains provided by Microsoft.

7 In the **Custom Proxy Bypass Configuration** page, configure the proxy bypass rules for custom domains and subnets specific to the Enterprise.



Settings to configure the proxy bypass rules for custom domains and subnets specific to the enterprise.

☐	Domain
☐	vmware.com

- To add a proxy bypass rule for custom domain, click **Domain** > **+ Add Rule** and enter a valid domain name.
- To add a proxy bypass rule for subnets, click **Subnet/IP** > **+ Add Rule** and enter either the network address (subnet) or the IP address (host) and the appropriate subnet mask value.
- To delete a rule that is no longer to be bypassed, select the rule and click **Delete**.

8 Click **Finish**. The Custom PAC file is created and appears in the **PAC File** configuration table.

Configure Host

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

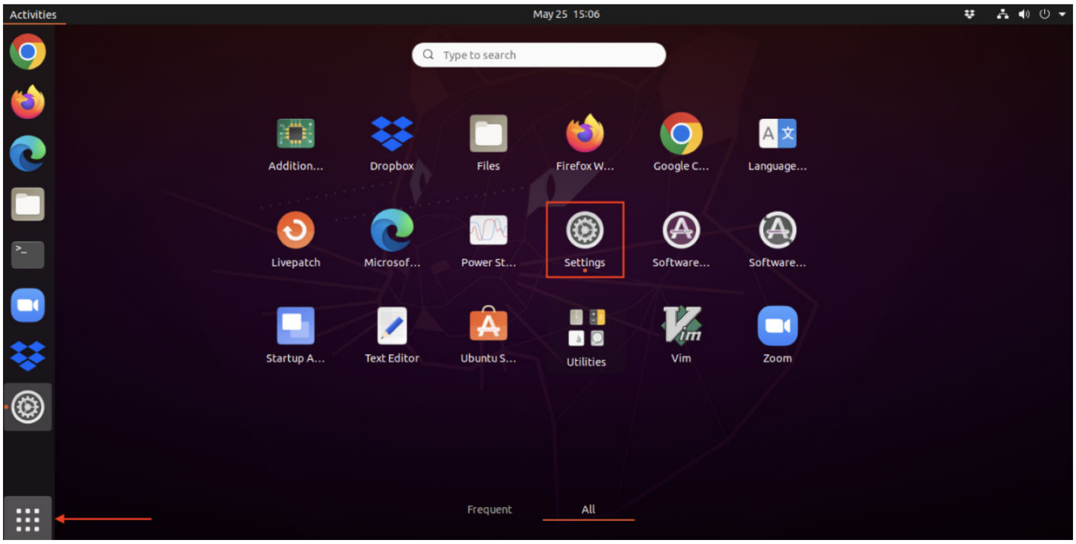
A host can be configured manually or automatically. The manual configuration requires the administrator to specify the proxy URL and port that Web browser traffic should be redirected towards. Additionally, manual entry of domains and endpoints pass might be required to ensure correct operations. The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

Ubuntu

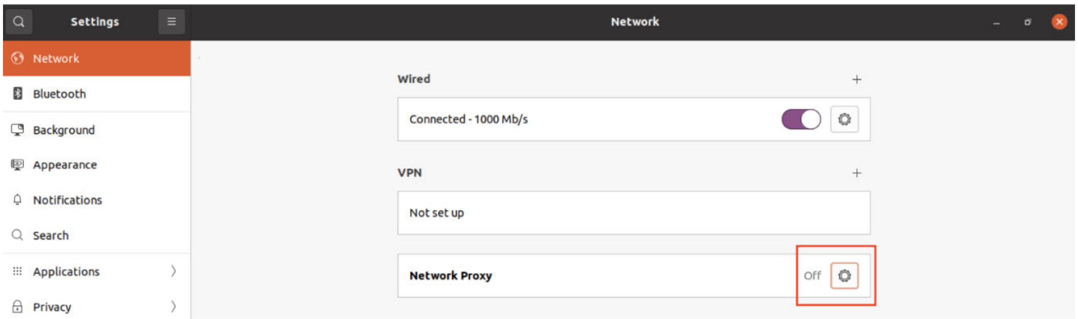
The following is a simple example highlighting the manual configuration on an Ubuntu Desktop host. The general concepts shown here apply to Windows, macOS, Android, and iOS devices.

Follow the below steps for manually configuring an Ubuntu Desktop host:

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



2 In the **Settings** window, on the left pane, click **Network**.



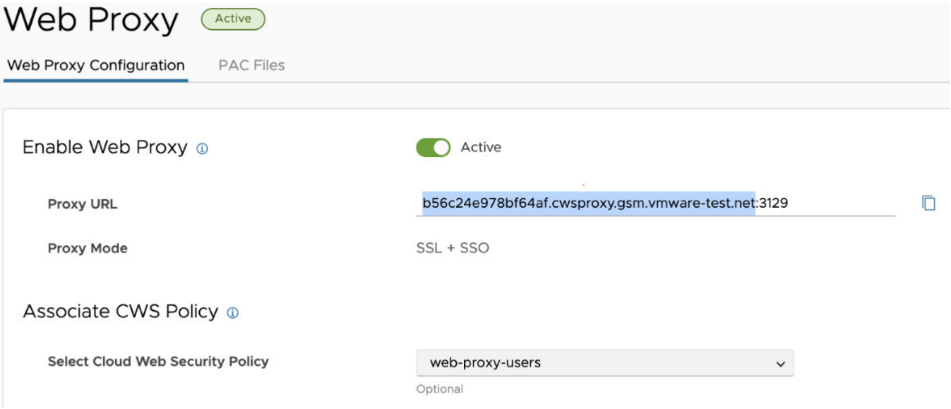
Connected - 1000 Mb/s

Not set up

Network Proxy Off

3 Go to **Network Proxy** and then click the Cog Wheel to turn the proxy settings ON (manually or automatically) or OFF.

4 For manual configuration, users must retrieve the URL + Port information from Cloud Web Security. Navigate to **Cloud Web Security** > **Configure** > **Access Methods** > **Web Proxy** > **Web Proxy Configuration**, and then copy the Proxy URL.



Web Proxy Active

Web Proxy Configuration | PAC Files

Enable Web Proxy: Active

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

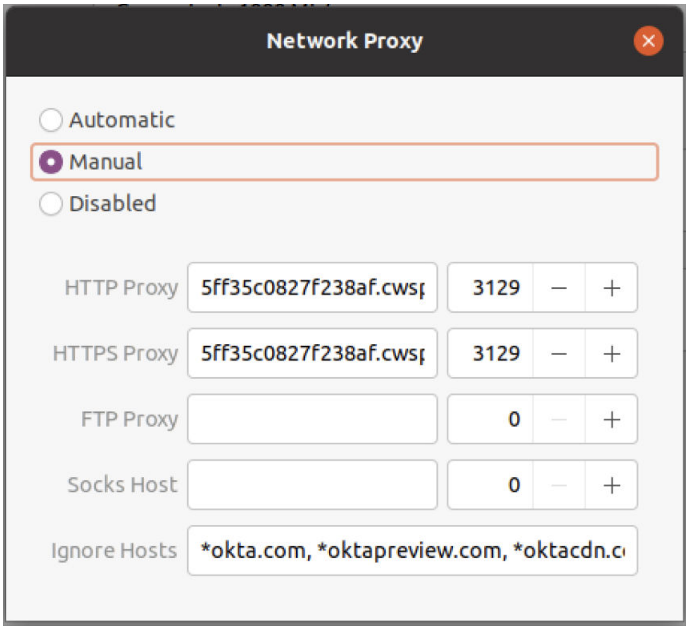
Proxy Mode: SSL + SSO

Associate CWS Policy

Select Cloud Web Security Policy: web-proxy-users

Optional

5 Paste the URL into the **HTTP Proxy** and **HTTPS Proxy** fields.



Network Proxy

○ Automatic

● Manual

○ Disabled

HTTP Proxy: 5ff35c0827f238af.cwsp | 3129

HTTPS Proxy: 5ff35c0827f238af.cwsp | 3129

FTP Proxy: | 0

Socks Host: | 0

Ignore Hosts: *okta.com, *oktapreview.com, *oktacdn.c

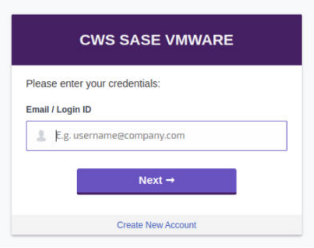
6 Set the port to **3129**, for both, **HTTP Proxy** and **HTTPS Proxy** fields. Users can copy and paste the port number from Cloud Web Security or enter it manually.

7. Close the dialog to apply the settings.

   Note For the SSO to work, ensure to bypass the domains associated with your identity provider. The below example shows three domains related to Okta. Additional IdP domains are also provided below. If users do not see their IdP, please consult the respective product documentation to determine which domains 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

8. Launch your web browser to see the Cloud Web Security login page.



CWS SASE VMWARE

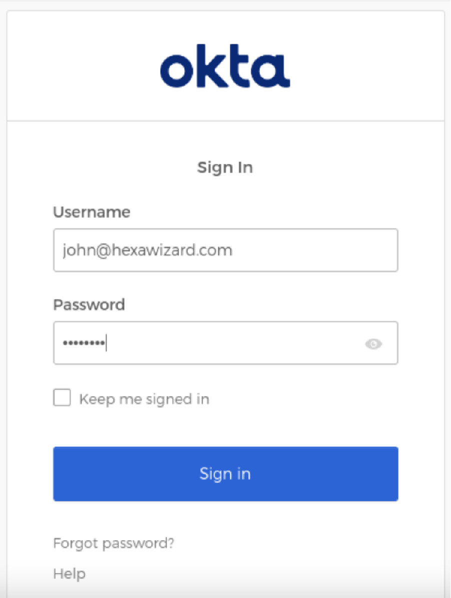
Please enter your credentials:

Email / Login ID

E.g. username@company.com

   Note If users have not installed the SSL Termination Certificate, a warning page "*Your connection is not private*" appears. Users may choose to install the certificate or accept the warning and proceed to the Cloud Web Security login page. For more information about how to install the certificate, see SSL Certificate.

9. Enter a valid email address configured in the IdP, and then click **Next**.
10. In the IdP's sign in page, enter your credentials, and then click **Sign In**.



Username: john@hexawizard.com

Password: ••••••••

11 Validate your internet connectivity and Cloud Web Security Policy.

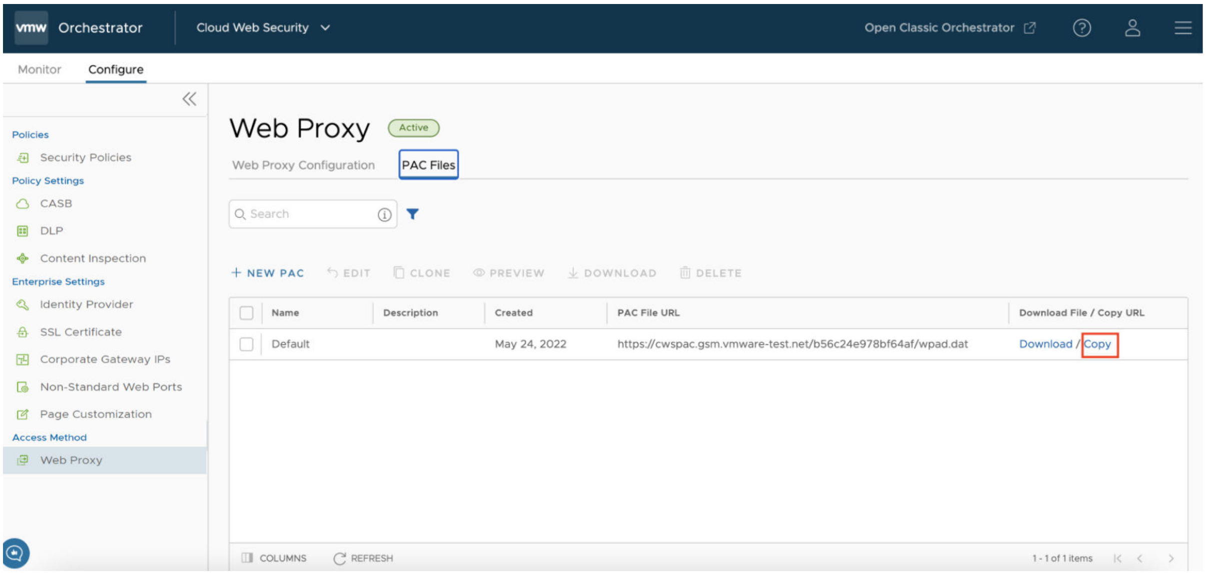
Automatic Proxy Settings

After configuring the manual proxy settings, 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.

Follow the below steps for automatic proxy configuration:

1 Navigate to **Cloud Web Security** > **Configure** > **Access Methods** > **Web Proxy** > **PAC Files**.

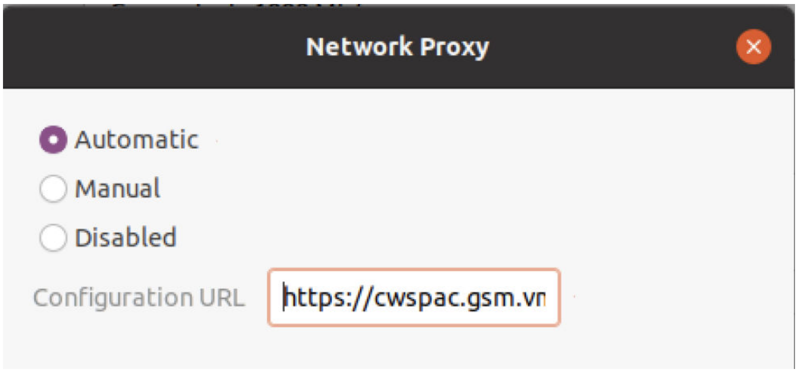
2 Click the **Copy** link corresponding to any PAC file.



☐	Name	Description	Created	PAC File URL	Download File / Copy URL
☐	Default		May 24, 2022	https://cwspac.gsm.vmware-test.net/b56c24e978bf64af/wpad.dat	Download / Copy

3 Go back to the host and change the proxy settings to **Automatic**.

4 Paste the copied URL in the **Configuration URL** field.



● Automatic
○ Manual
○ Disabled

Configuration URL https://cwspac.gsm.vn

5 Close the dialog to apply the settings.

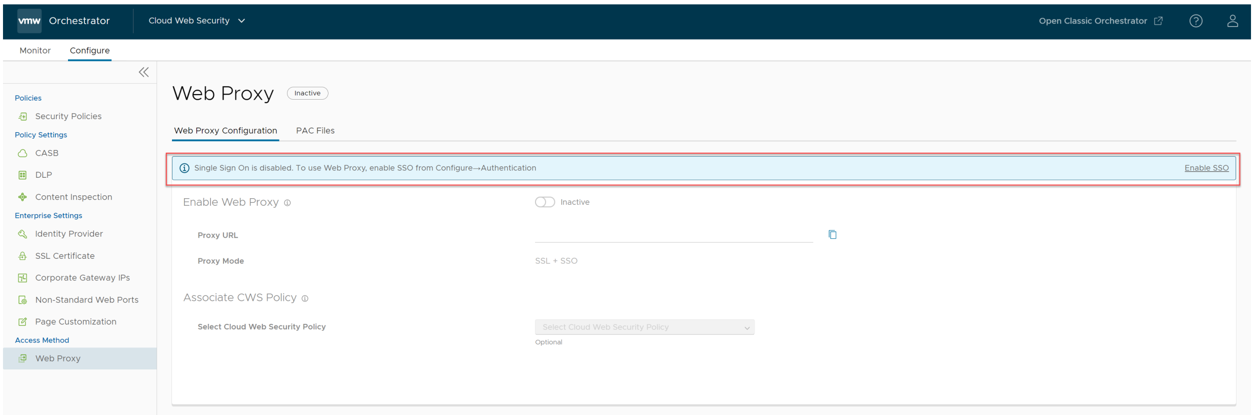
Refer to the respective product documentation on steps to configure these settings:

- **Windows**: To configure the settings on a Windows system, see https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/connectivity-navigation/use-proxy-servers-with-ie.
- **macOS**: To configure the settings on a macOS system, see https://support.apple.com/en-in/guide/mac-help/mchlp2591/mac#:~:text=Use%20the%20Proxies%20pane%20of,click%20Advanced%2C%20then%20click%20Proxies..
- **Android**: To configure these settings on an Android system, see https://support.google.com/pixelphone/answer/9655181?hl=en#zippy=%2Cset-up-a-proxy-to-connect-phones.

  Note The included reference is for a Google Pixel phone. Users may need to search for their specific model if the options are not the same.
- **iOS**: To configure these settings on an iOS system, see https://www.howtogeek.com/293676/how-to-configure-a-proxy-server-on-an-iphone-or-ipad/.

Troubleshoot Web Proxy

As stated in the pre-requisite checklist, SSO must be activated before setting up the Web Proxy. If you see a warning message stating "*Single Sign On is deactivated. To use Web Proxy, activate SSO from Configure → Authentication*", please refer to the pre-requisite section in this guide.



Single Sign On is disabled. To use Web Proxy, enable SSO from Configure→Authentication

Enable Web Proxy: Inactive

Proxy URL:

Proxy Mode: SSL + SSO

Select Cloud Web Security Policy: Select Cloud Web Security Policy

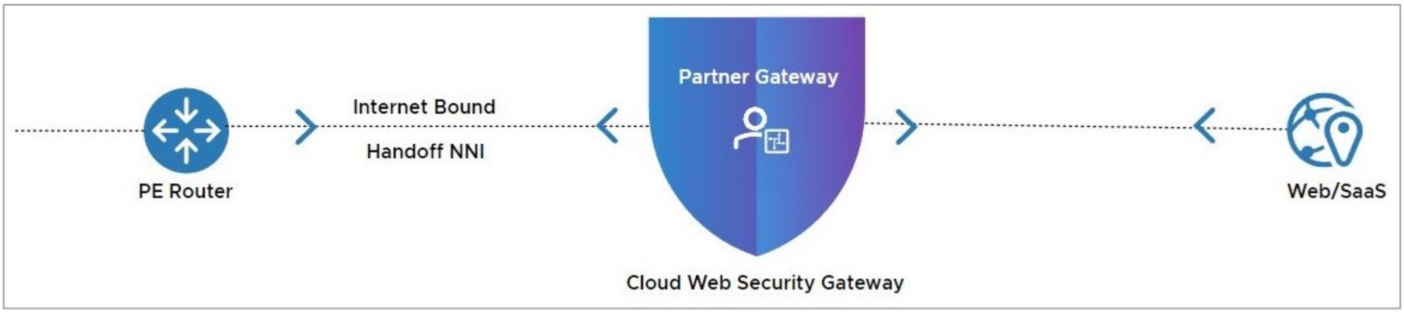
Partner Gateway for Cloud Web Security

10

This section covers the configuration of a Partner Gateway to use VMware Cloud Web Security.

Overview

Cloud Web Security allows Service Providers to configure their own Partner Gateways to peer with VMware SASE Points of Presence (PoPs). As a result Service Provider customers can utilize Cloud Web Security services while being connected to a Partner Gateway. In addition, Partner Customer sites that are MPLS-only are not required to use a broadband connection to access Cloud Web Security services.



Prerequisites

A customer would need the following to configure a Partner Gateway for use with Cloud Web Security:

1 A Partner portal on a production VMware Cloud Orchestrator with Cloud Web Security activated.

2 The Partner must deploy at least one VMware SD-WAN Gateway as a Partner Gateway. To learn more about configuring a Gateway as a Partner Gateway see, Manage Gateways with New Orchestrator UI.

3 The Partner Gateway(s) must have the following:

   a The Partner Gateways must run Gateway software release 5.0.1.2 or later.

   b The Partner Gateway must be configured for a Cloud Web Security role (in other words, configured to be a SASE Point of Presence (PoP)).

   Note For more information about configuring a Gateway for a Cloud Web Security role, see Configuring a SD-WAN Gateway for a Cloud Web Security Role.

4 The Partner Gateway must be configured as a hand off for at least one customer enterprise that the Partner wants associated with Cloud Web Security. To learn more see, Configure Hand Off.

Configure a Partner Gateway for Cloud Web Security

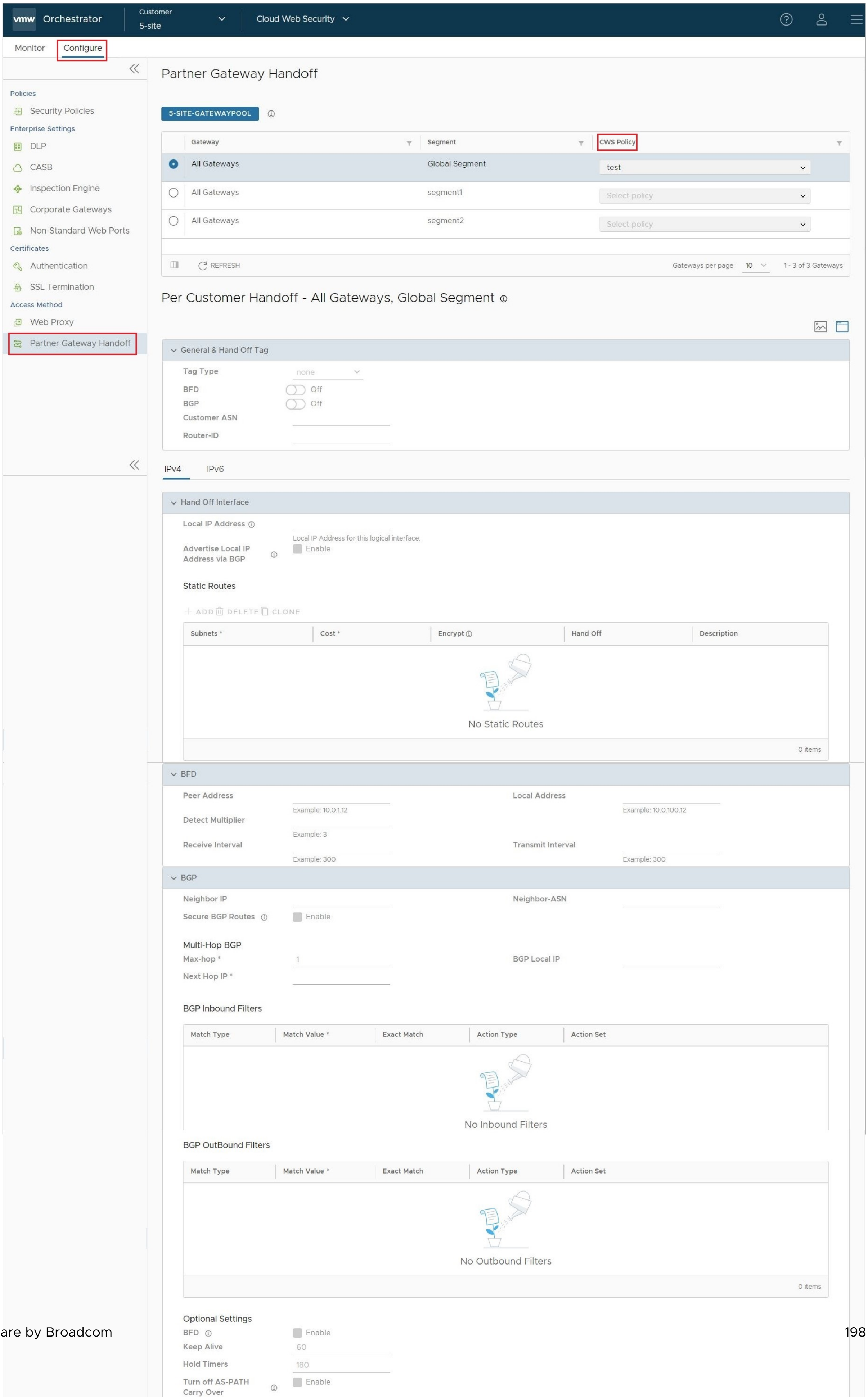
To configure a Partner Gateway for use with Cloud Web Security, perform the following steps:

1 Navigate to **Cloud Web Security > Configure > Partner Gateway Handoff**.

2 Select the Gateway(s) and Segment to be used.

3 Associate the selected Gateway(s) and Segment with a Security Policy.

   Note For more information on Creating a Security Policy, see Create a Security Policy.



Partner Gateway Handoff

5-SITE-GATEWAYPOOL

	Gateway	Segment	CWS Policy
●	All Gateways	Global Segment	test
○	All Gateways	segment1	Select policy
○	All Gateways	segment2	Select policy

REFRESH Gateways per page 10 1 - 3 of 3 Gateways

Per Customer Handoff - All Gateways, Global Segment

General & Hand Off Tag

Tag Type: none
BFD: Off
BGP: Off
Customer ASN
Router-ID

IPv4 IPv6

Hand Off Interface

Local IP Address
Local IP Address for this logical interface.
Advertise Local IP Address via BGP: ☐ Enable

Static Routes

+ ADD DELETE CLONE

Subnets *	Cost *	Encrypt	Hand Off	Description

No Static Routes

0 items

BFD

Peer Address: Example: 10.0.1.12
Local Address: Example: 10.0.100.12
Detect Multiplier: Example: 3
Receive Interval: Example: 300
Transmit Interval: Example: 300

BGP

Neighbor IP
Neighbor-ASN
Secure BGP Routes: ☐ Enable

Multi-Hop BGP
Max-hop *: 1
BGP Local IP
Next Hop IP *

BGP Inbound Filters

Match Type	Match Value *	Exact Match	Action Type	Action Set

No Inbound Filters

BGP OutBound Filters

Match Type	Match Value *	Exact Match	Action Type	Action Set

No Outbound Filters

0 items

Optional Settings
BFD: ☐ Enable
Keep Alive: 60
Hold Timers: 180
Turn off AS-PATH Carry Over: ☐ Enable

4 Configure the General & Hand Off Tag. This needs to match the configuration you have for the respective Partner Gateway Handoff.

5 Under either/or or both IPv4 and IPv6 configure the additional parameters as they were configured for the Partner Gateway and its handoff: the **Hand Off Interface**, **BFD Parameters**, and **BGP Parameters** including inbound and outbound filters.

6 Click **Save Changes** to complete the Partner Gateway Handoff configuration.

Monitoring Partner Gateway Handoff

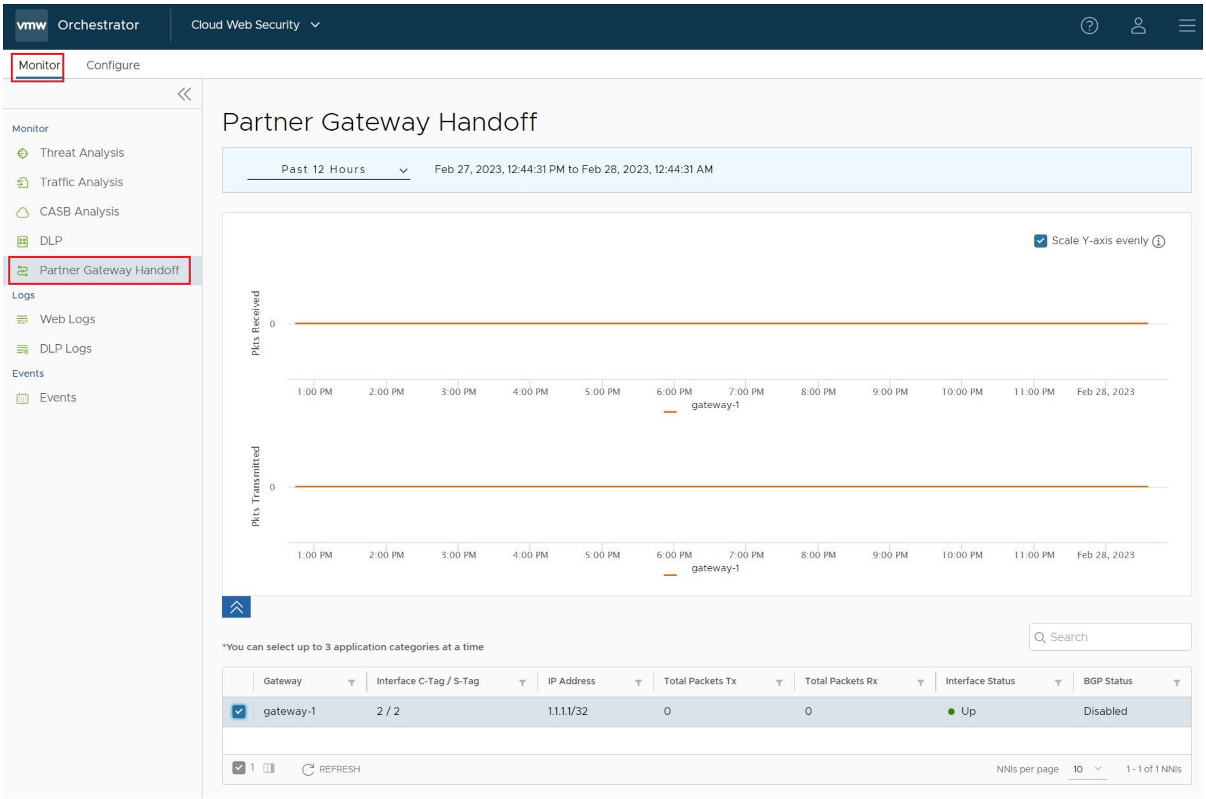
This section covers the monitoring available for Partner Gateway that is specific to Cloud Web Security. Cloud Web Security monitors the quantity of packets both received and transmitted through a Partner Gateway which is destined for the Cloud Web Security service.

Note Monitoring for packets that traverse a Partner Gateway using Cloud Web Security is a feature available in VMware SASE Orchestrators using Release 5.2.0 and later. Orchestrators using an earlier release will not have this feature available.

To view the Monitoring for Partner Gateways using Cloud Web Security, do the following:

1 Navigate to **Cloud Web Security > Monitor > Partner Gateway Handoff**.

2 Select the Gateway(s) to be monitored.



Partner Gateway Handoff

Feb 27, 2023, 12:44:31 PM to Feb 28, 2023, 12:44:31 AM

*You can select up to 3 application categories at a time

	Gateway	Interface C-Tag / S-Tag	IP Address	Total Packets Tx	Total Packets Rx	Interface Status	BGP Status
☑	gateway-1	2 / 2	1.1.1.1/32	0	0	● Up	Disabled

3 A user can view how many packets are being received and sent through the Partner Gateway to the Cloud Web Security service. Like all monitoring graphs, a user can select from a menu of time blocks (for example, 12 hours, 24 hours, last seven days) or use a calender and time selector to find specific particular time periods.

Monitor Cloud Web Security

11

User can view the results of the configured Security policies for an Enterprise from the **Monitor** tab in the Cloud Web Security page in the VMware Cloud Orchestrator UI portal.

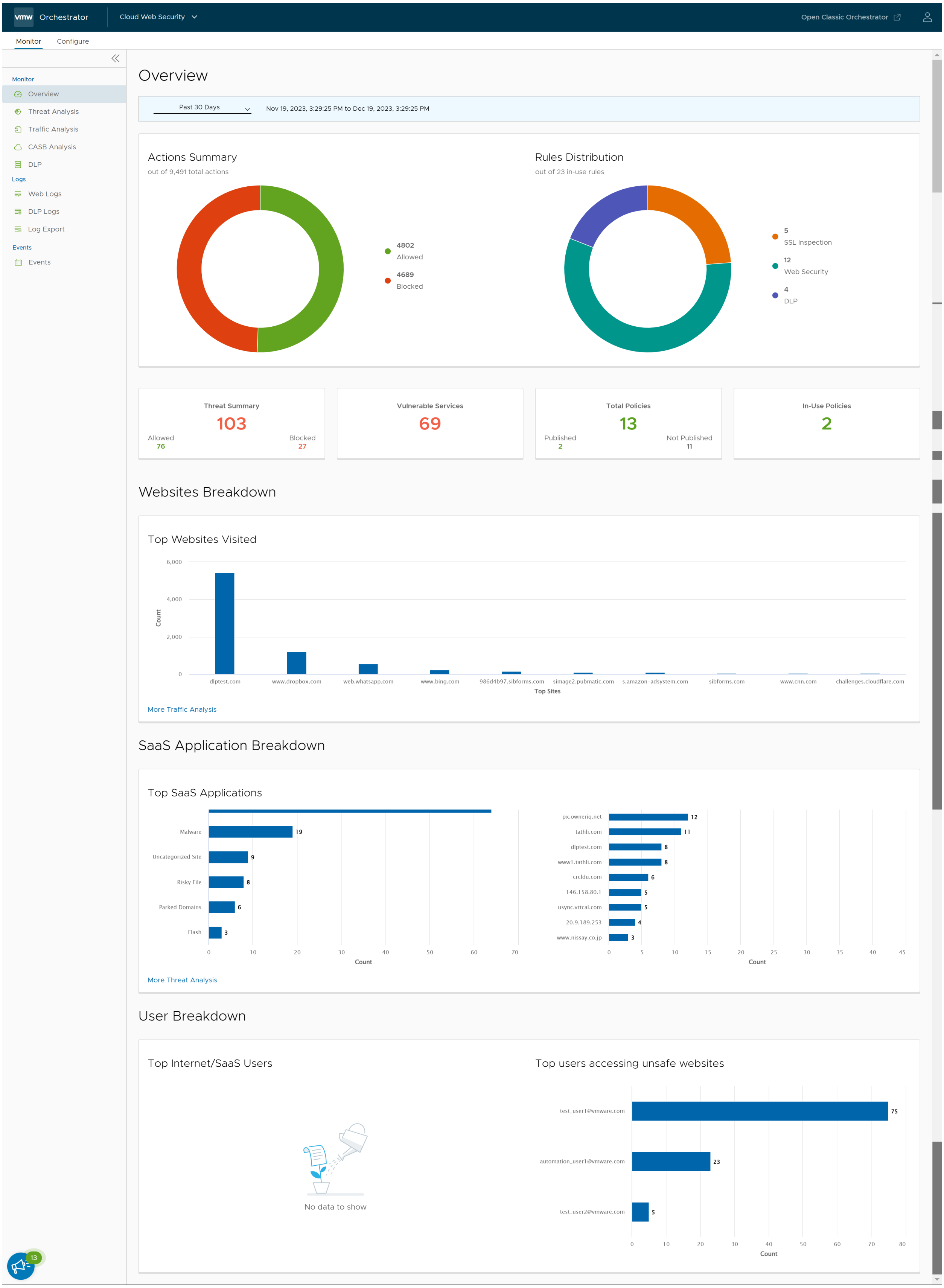
To monitor Cloud Web Security, perform the following steps:

1. In the VMware Cloud Orchestrator UI portal, from the **SD-WAN** drop-down menu, select **Cloud Web Security**. The **Cloud Web Security** page appears.
2. Click the **Monitor** tab.
3. Under the **Monitor** section of **Cloud Web Security** page, Users can view the following monitoring options:
   - Overview
   - Threat Analysis
   - Traffic Analysis
   - CASB Analysis
   - DLP
   - Logs (Web and DLP)
   - Log Export
   - Events

Overview

The **Overview** dashboard presents a cleaner, more accessible presentation of critical information on a single page, while also pointing the user to more detailed information for each data category. The top graphs provide a user with the Cloud Web Security **Actions Summary** (actions taken over the configured time period), and the current **Rules Distribution** for that customer.

In addition, a user can scroll further and see at-a-glance graphs for **Top Websites Visited**, **Top SaaS Applications**, **Threat Breakdown**, and **User Breakdown**.

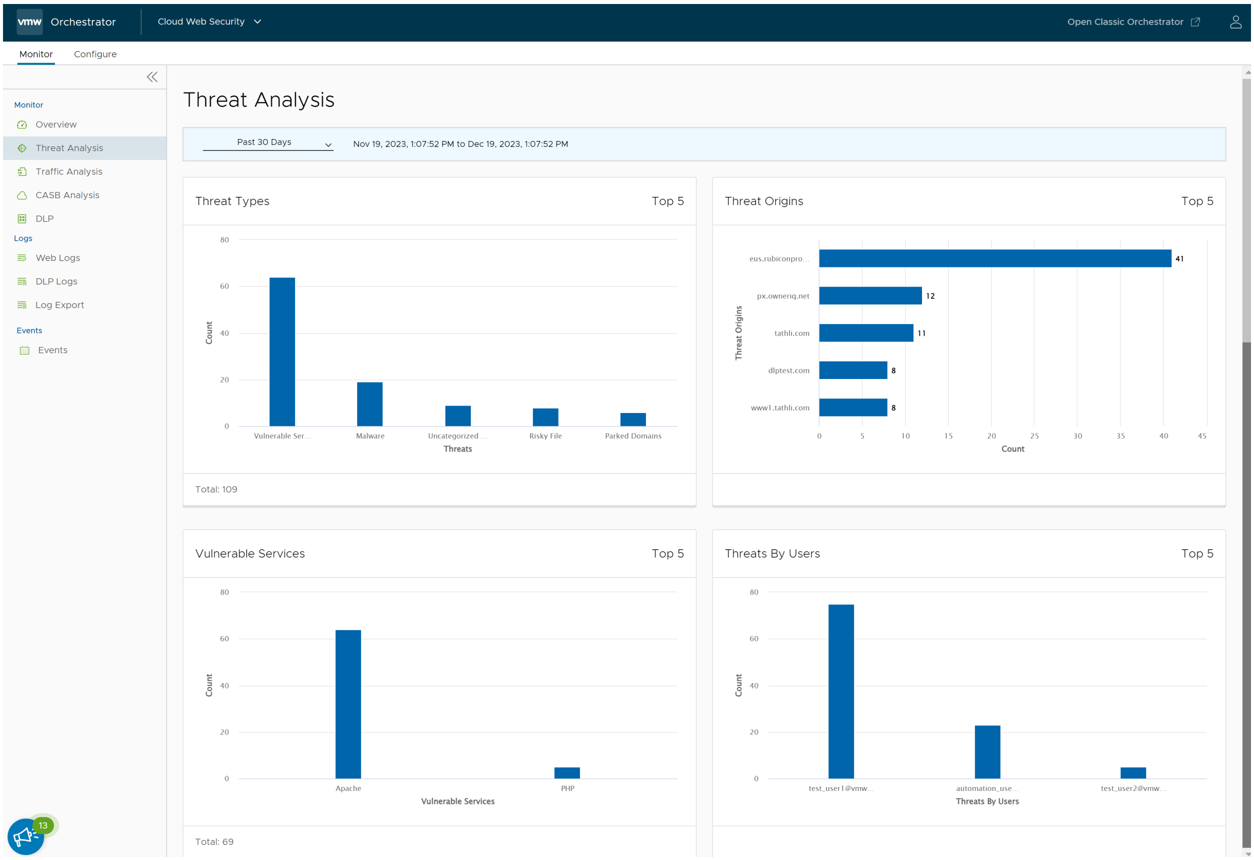

vmw Orchestrator
Cloud Web Security
Open Classic Orchestrator
Monitor
Configure
Monitor
Overview
Threat Analysis
Traffic Analysis
CASB Analysis
DLP
Logs
Web Logs
DLP Logs
Log Export
Events
Events
Overview
Past 30 Days
Nov 19, 2023, 3:29:25 PM to Dec 19, 2023, 3:29:25 PM
Actions Summary
out of 9,491 total actions
4802
Allowed
4689
Blocked
Rules Distribution
out of 23 in-use rules
5
SSL Inspection
12
Web Security
4
DLP
Threat Summary
103
Allowed
76
Blocked
27
Vulnerable Services
69
Total Policies
13
Published
2
Not Published
11
In-Use Policies
2
Websites Breakdown
Top Websites Visited
6,000
4,000
2,000
0
Count
dlptest.com
www.dropbox.com
web.whatsapp.com
www.bing.com
986d4b97.sibforms.com
simage2.pubmatic.com
s.amazon-adsystem.com
sibforms.com
www.cnn.com
challenges.cloudflare.com
Top Sites
More Traffic Analysis
SaaS Application Breakdown
Top SaaS Applications
Malware 19
Uncategorized Site 9
Risky File 8
Parked Domains 6
Flash 3
0 10 20 30 40 50 60 70
Count
px.owneriq.net 12
tathli.com 11
dlptest.com 8
www1.tathli.com 8
crcldu.com 6
146.158.80.1 5
usync.vrtcal.com 5
20.9.189.253 4
www.nissay.co.jp 3
0 5 10 15 20 25 30 35 40 45
Count
More Threat Analysis
User Breakdown
Top Internet/SaaS Users
No data to show
Top users accessing unsafe websites
test_user1@vmware.com 75
automation_user1@vmware.com 23
test_user2@vmware.com 5
0 10 20 30 40 50 60 70 80
Count
13

Threat Analysis

The **Threat Analysis** dashboard provides a detailed visibility into threats. The dashboard displays:

- Threat Types
- Threat Origins
- Vulnerable Services
- Threats By Users

Users can choose a specific time period from the drop-down list, to view the threats for the selected duration (for example, Past 31 Days).


Past 30 Days

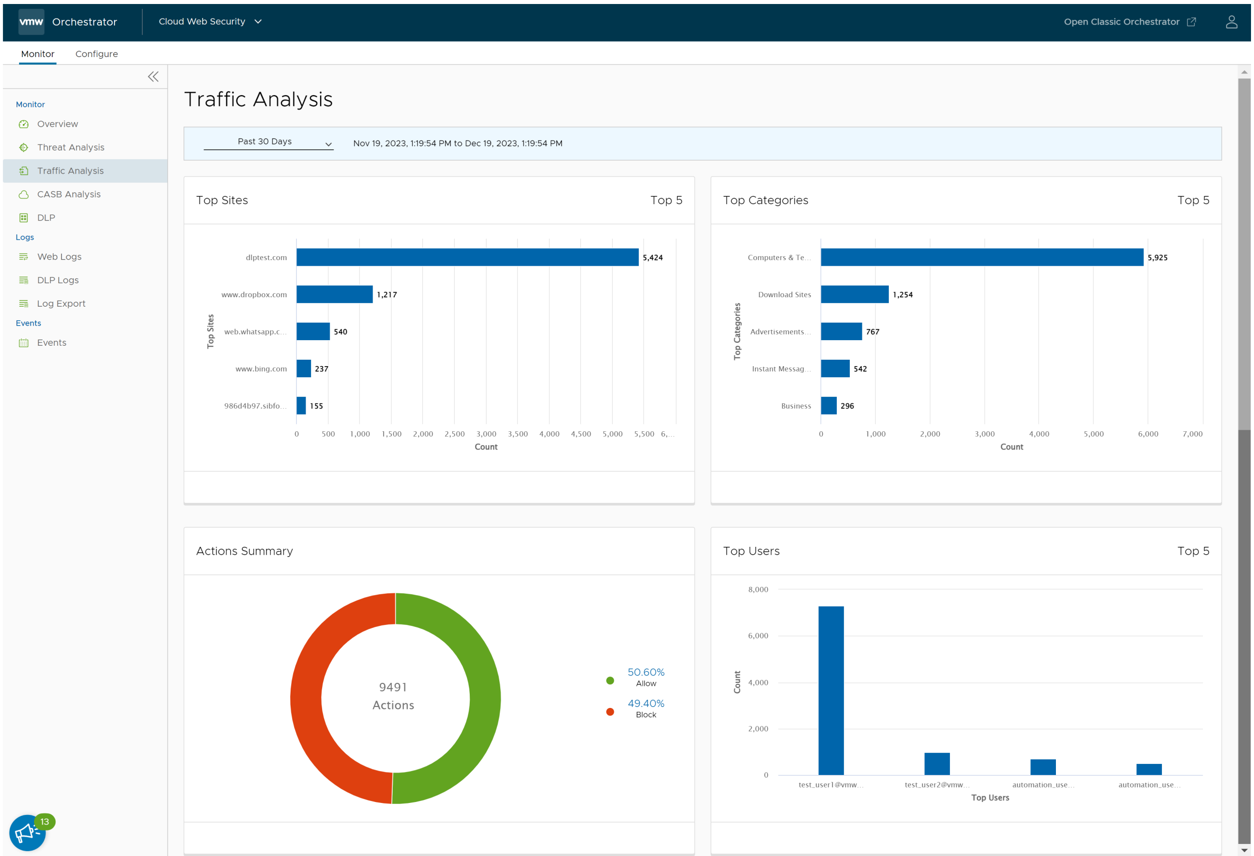
Nov 19, 2023, 1:07:52 PM to Dec 19, 2023, 1:07:52 PM

Traffic Analysis

The **Traffic Analysis** dashboard provides a detailed visibility into user traffic. The dashboard displays:

- Top Sites being visited by users
- Top Categories for traffic
- Actions Summary, the percentage of traffic being allowed/blocked
- Top Users

Users can choose a specific time period from the drop-down list, to view the user traffic data for the selected duration (for example, Past 31 Days).



Past 30 Days

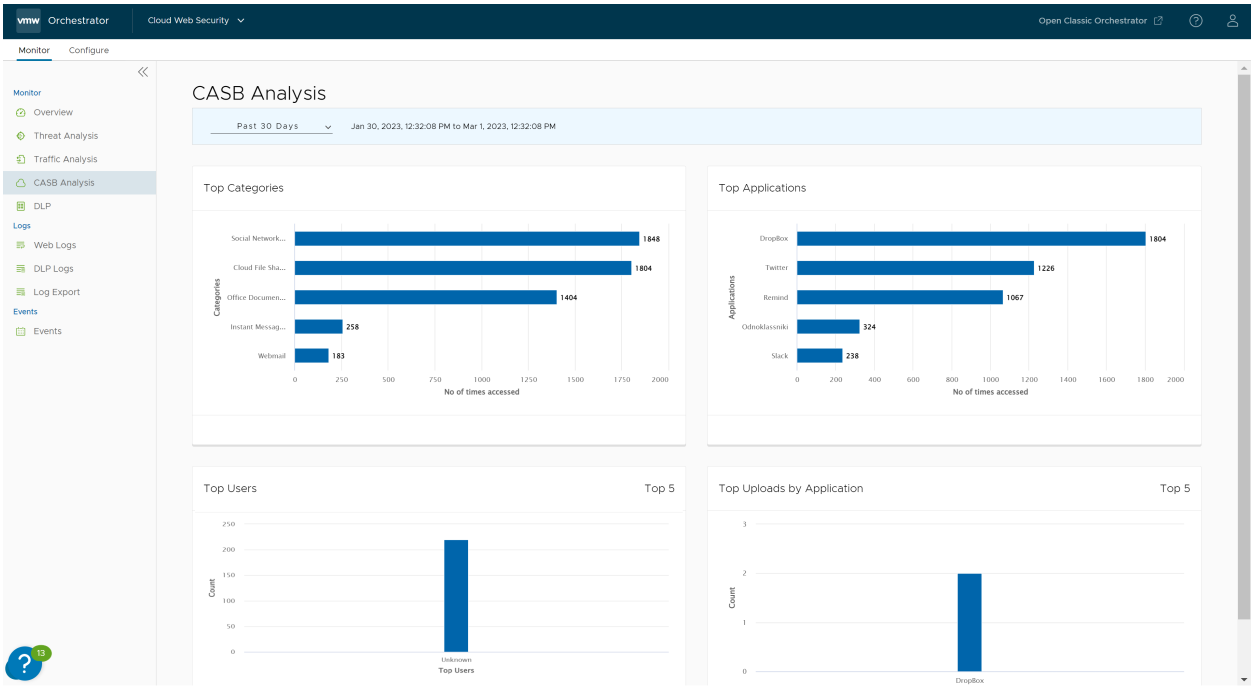
Nov 19, 2023, 1:19:54 PM to Dec 19, 2023, 1:19:54 PM

CASB Analysis

The **CASB Analysis** dashboard provides a detailed visibility into user and application traffic. The dashboard displays:

- Top Categories for traffic
- Top Applications
- Top Users
- Top Uploads by Applications

Users can choose a specific time period from the drop-down list, to view the CASB data for the selected duration (for example, Past 31 Days).

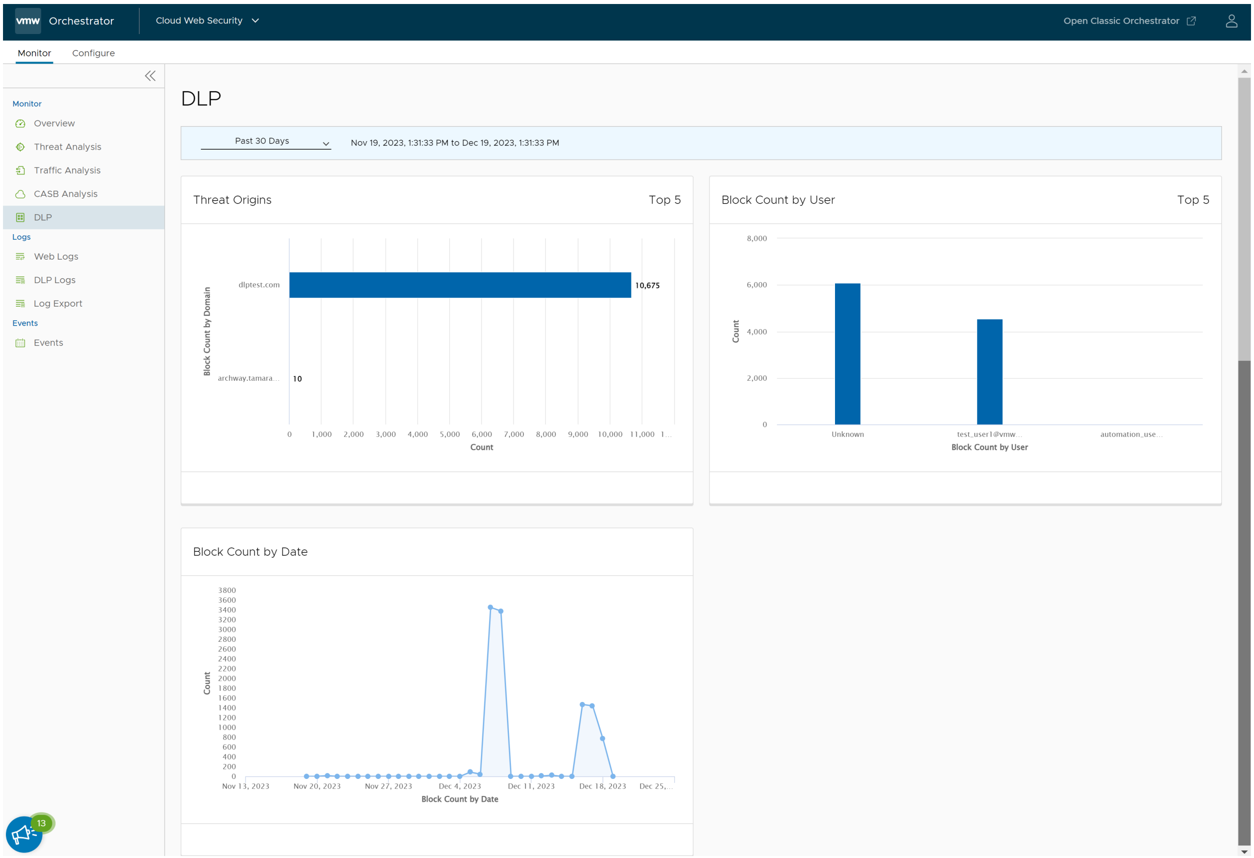


DLP

The **DLP** dashboard provides a detailed visibility into threat origins and blocked traffic. The dashboard displays:

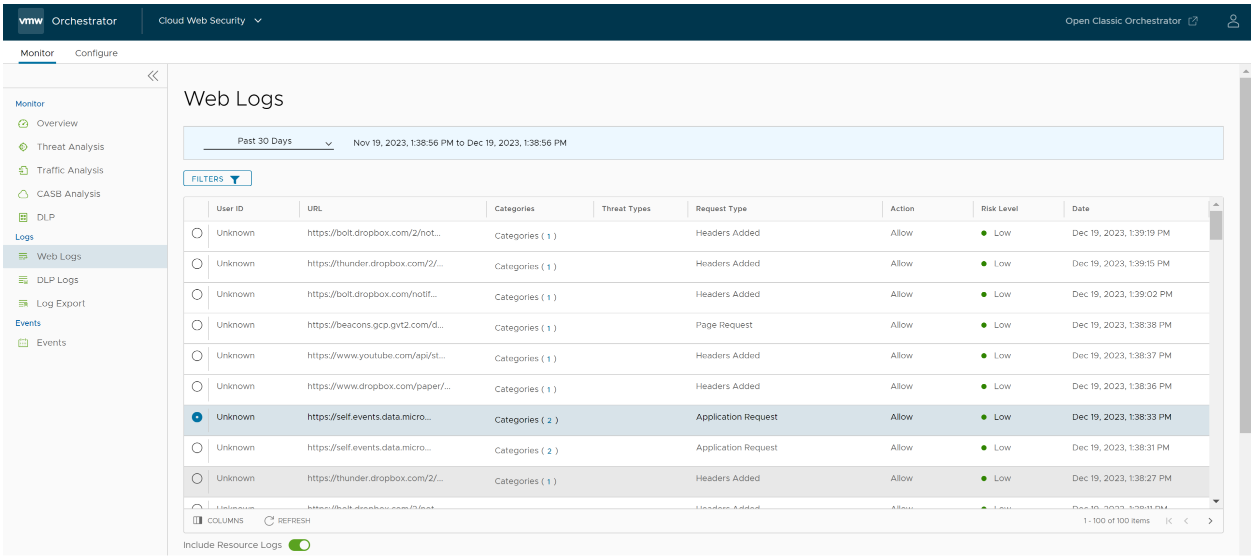
- Threat Origins
- Block Count by User
- Block Count by Date

Users can choose a specific time period from the drop-down list, to view the DLP data for the selected duration (for example, Past 31 Days).



Web Logs

The **Web Logs** page logs every Web session and threat. Users can view a list of Web logs, scrolling through the full list. Users can choose a specific time period from the drop-down list, to view the logs for the selected duration (for example, Past 31 Days).



Web Logs

Past 30 Days

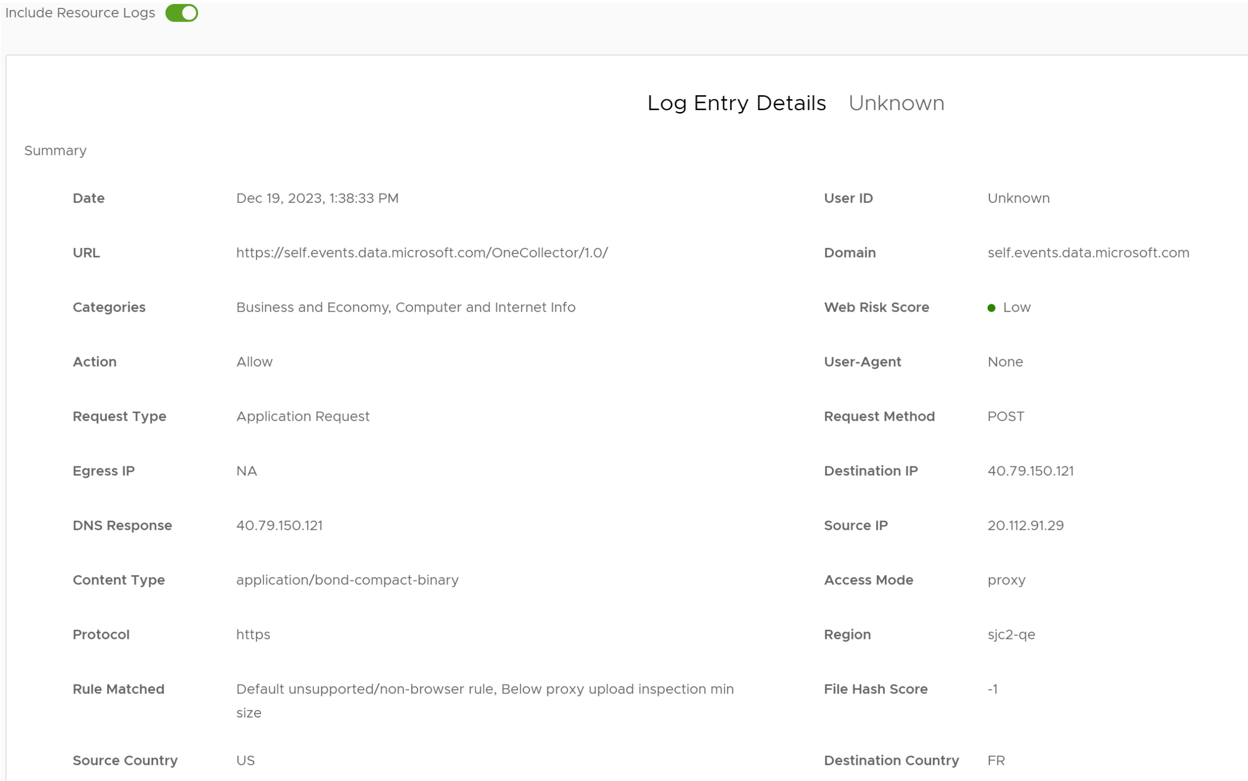
Nov 19, 2023, 1:38:56 PM to Dec 19, 2023, 1:38:56 PM

	User ID	URL	Categories	Threat Types	Request Type	Action	Risk Level	Date
○	Unknown	https://bolt.dropbox.com/2/not...	Categories (1)		Headers Added	Allow	● Low	Dec 19, 2023, 1:39:19 PM
○	Unknown	https://thunder.dropbox.com/2/...	Categories (1)		Headers Added	Allow	● Low	Dec 19, 2023, 1:39:15 PM
○	Unknown	https://bolt.dropbox.com/notif...	Categories (1)		Headers Added	Allow	● Low	Dec 19, 2023, 1:39:02 PM
○	Unknown	https://beacons.gcp.gvt2.com/d...	Categories (1)		Page Request	Allow	● Low	Dec 19, 2023, 1:38:38 PM
○	Unknown	https://www.youtube.com/api/st...	Categories (1)		Headers Added	Allow	● Low	Dec 19, 2023, 1:38:37 PM
○	Unknown	https://www.dropbox.com/paper/...	Categories (1)		Headers Added	Allow	● Low	Dec 19, 2023, 1:38:36 PM
●	Unknown	https://self.events.data.micro...	Categories (2)		Application Request	Allow	● Low	Dec 19, 2023, 1:38:33 PM
○	Unknown	https://self.events.data.micro...	Categories (2)		Application Request	Allow	● Low	Dec 19, 2023, 1:38:31 PM
○	Unknown	https://thunder.dropbox.com/2/...	Categories (1)		Headers Added	Allow	● Low	Dec 19, 2023, 1:38:27 PM

1 - 100 of 100 items

Include Resource Logs

Click on a Web log entry to view granular details about the selected entry. A **Log Entry Details** screen displays detailed information about the entry.



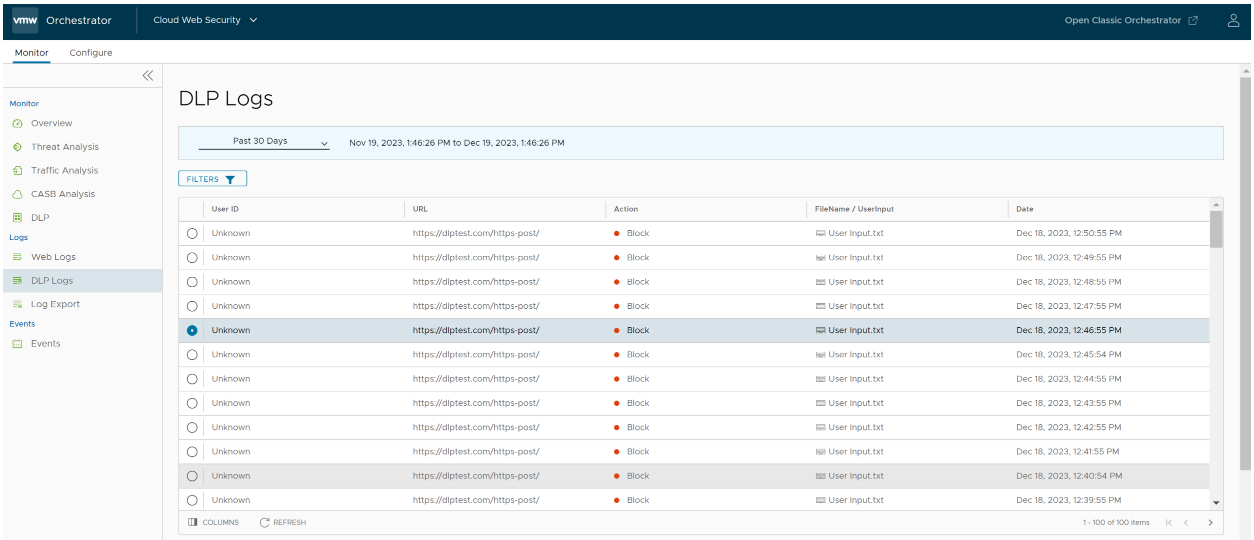
Log Entry Details Unknown

Summary

Date	Dec 19, 2023, 1:38:33 PM	**User ID**	Unknown
URL	https://self.events.data.microsoft.com/OneCollector/1.0/	**Domain**	self.events.data.microsoft.com
Categories	Business and Economy, Computer and Internet Info	**Web Risk Score**	● Low
Action	Allow	**User-Agent**	None
Request Type	Application Request	**Request Method**	POST
Egress IP	NA	**Destination IP**	40.79.150.121
DNS Response	40.79.150.121	**Source IP**	20.112.91.29
Content Type	application/bond-compact-binary	**Access Mode**	proxy
Protocol	https	**Region**	sjc2-qe
Rule Matched	Default unsupported/non-browser rule, Below proxy upload inspection min size	**File Hash Score**	-1
Source Country	US	**Destination Country**	FR

DLP Logs

The **DLP Logs** page logs every DLP session and threat. Users can view a list of DLP logs, scrolling through the full list. Users can choose a specific time period from the drop-down list, to view the logs for the selected duration (for example, Past 31 Days).



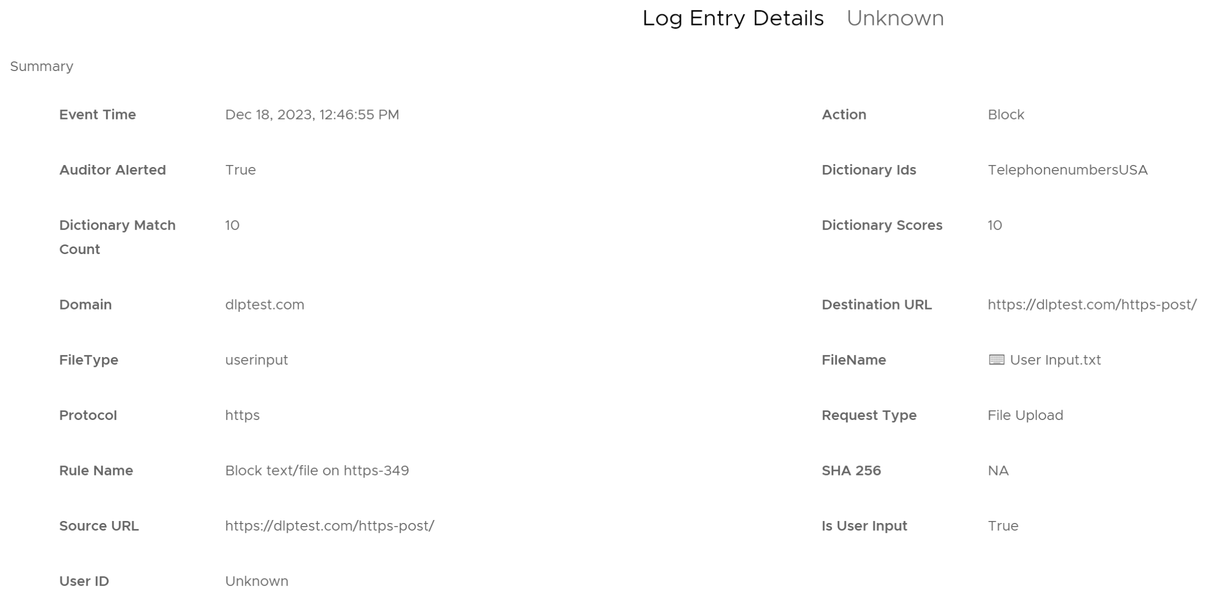
DLP Logs

Past 30 Days Nov 19, 2023, 1:46:26 PM to Dec 19, 2023, 1:46:26 PM

	User ID	URL	Action	FileName / UserInput	Date
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:50:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:49:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:48:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:47:55 PM
●	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:46:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:45:54 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:44:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:43:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:42:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:41:55 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:40:54 PM
○	Unknown	https://dlptest.com/https-post/	● Block	User Input.txt	Dec 18, 2023, 12:39:55 PM

1 - 100 of 100 items

Click on a DLP log entry to view granular details about the selected entry. A **Log Entry Details** screen displays detailed information about the entry.



Log Entry Details Unknown

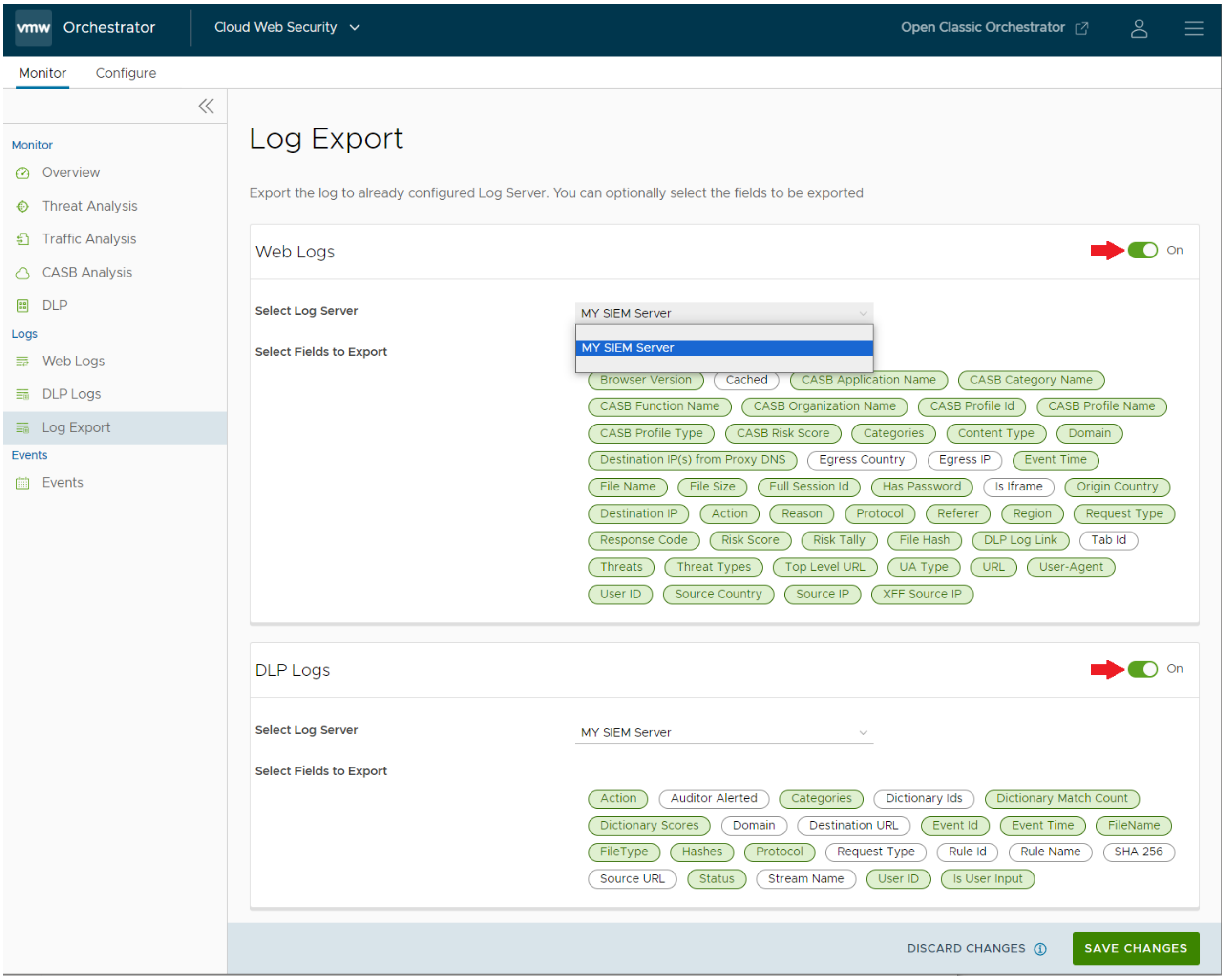
Summary

Event Time	Dec 18, 2023, 12:46:55 PM	**Action**	Block
Auditor Alerted	True	**Dictionary Ids**	TelephonenumbersUSA
Dictionary Match Count	10	**Dictionary Scores**	10
Domain	dlptest.com	**Destination URL**	https://dlptest.com/https-post/
FileType	userinput	**FileName**	⌨ User Input.txt
Protocol	https	**Request Type**	File Upload
Rule Name	Block text/file on https-349	**SHA 256**	NA
Source URL	https://dlptest.com/https-post/	**Is User Input**	True
User ID	Unknown		

Log Export

The **Log Export** feature enables a customer to forward near-realtime logs about Cloud Web Security activities to a customer-controlled SIEM (Security information and event management) endpoint for storage and analysis.

The **Log Export** page allows users to export the logs to a configured Log Server. Optionally, you can also select the type of logs (Web or DLP) to be exported. For more information, see Chapter 12 Log Export.



Log Export

Export the log to already configured Log Server. You can optionally select the fields to be exported

Web Logs: On

Select Log Server: MY SIEM Server

Select Fields to Export

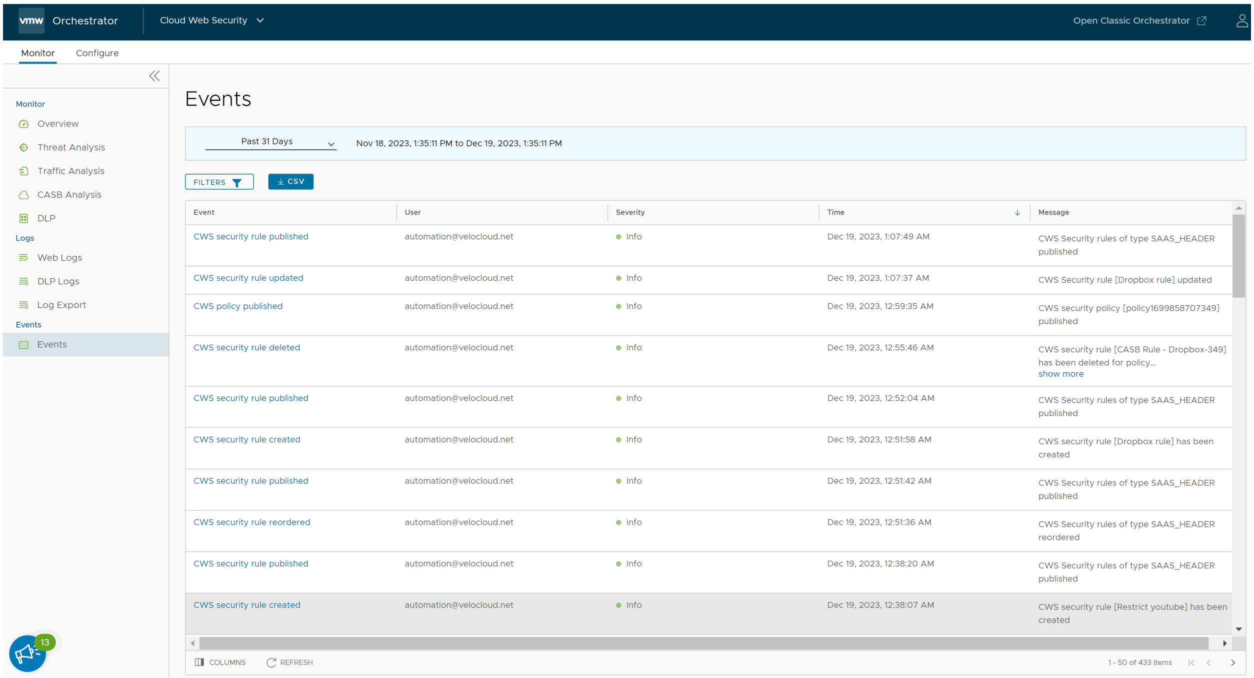
DLP Logs: On

Select Log Server: MY SIEM Server

Select Fields to Export

Events

The **Events** page displays all the events generated by the VMware Cloud Orchestrator. Click the link to an event name to view more details about the specific event.



Events

Past 31 Days   Nov 18, 2023, 1:35:11 PM to Dec 19, 2023, 1:35:11 PM

Event	User	Severity	Time	Message
CWS security rule published	automation@velocloud.net	● Info	Dec 19, 2023, 1:07:49 AM	CWS Security rules of type SAAS_HEADER published
CWS security rule updated	automation@velocloud.net	● Info	Dec 19, 2023, 1:07:37 AM	CWS Security rule [Dropbox rule] updated
CWS policy published	automation@velocloud.net	● Info	Dec 19, 2023, 12:59:35 AM	CWS security policy [policy1699858707349] published
CWS security rule deleted	automation@velocloud.net	● Info	Dec 19, 2023, 12:55:46 AM	CWS security rule [CASB Rule - Dropbox-349] has been deleted for policy... show more
CWS security rule published	automation@velocloud.net	● Info	Dec 19, 2023, 12:52:04 AM	CWS Security rules of type SAAS_HEADER published
CWS security rule created	automation@velocloud.net	● Info	Dec 19, 2023, 12:51:58 AM	CWS security rule [Dropbox rule] has been created
CWS security rule published	automation@velocloud.net	● Info	Dec 19, 2023, 12:51:42 AM	CWS Security rules of type SAAS_HEADER published
CWS security rule reordered	automation@velocloud.net	● Info	Dec 19, 2023, 12:51:36 AM	CWS Security rules of type SAAS_HEADER reordered
CWS security rule published	automation@velocloud.net	● Info	Dec 19, 2023, 12:38:20 AM	CWS Security rules of type SAAS_HEADER published
CWS security rule created	automation@velocloud.net	● Info	Dec 19, 2023, 12:38:07 AM	CWS security rule [Restrict youtube] has been created

1 - 50 of 433 items

Users can choose a specific time period from the drop-down list, to view the events for the selected duration (for example, Past 31 Days).

To view details related to specific events, use the **Filter** optiona. Click the **Filter** button to filter the list of events based on the following options: Event, User, Severity, Event Detail, and Message.

Click the **CSV** button to download a report of the events in CSV format.

The **Events** page displays the following details:

Option	Description
Event	Name of the event.
User	Name of the user who performed the event action.
Severity	Severity of the event. The available options are Alert, Critical, Debug, Emergency, Error, Info, Notice, and Warning.
Time	Date and time of the event.
Message	A brief description of the event.

Log Export

12

The **Log Export** feature enables a customer to forward near-realtime logs about Cloud Web Security activities to a customer-controlled SIEM (Security information and event management) endpoint for storage and analysis.

Read the following topics next:

- Configure a Log Export Server
- Configure Log Export for Cloud Web Security
- Log Export Field Reference

Configure a Log Export Server

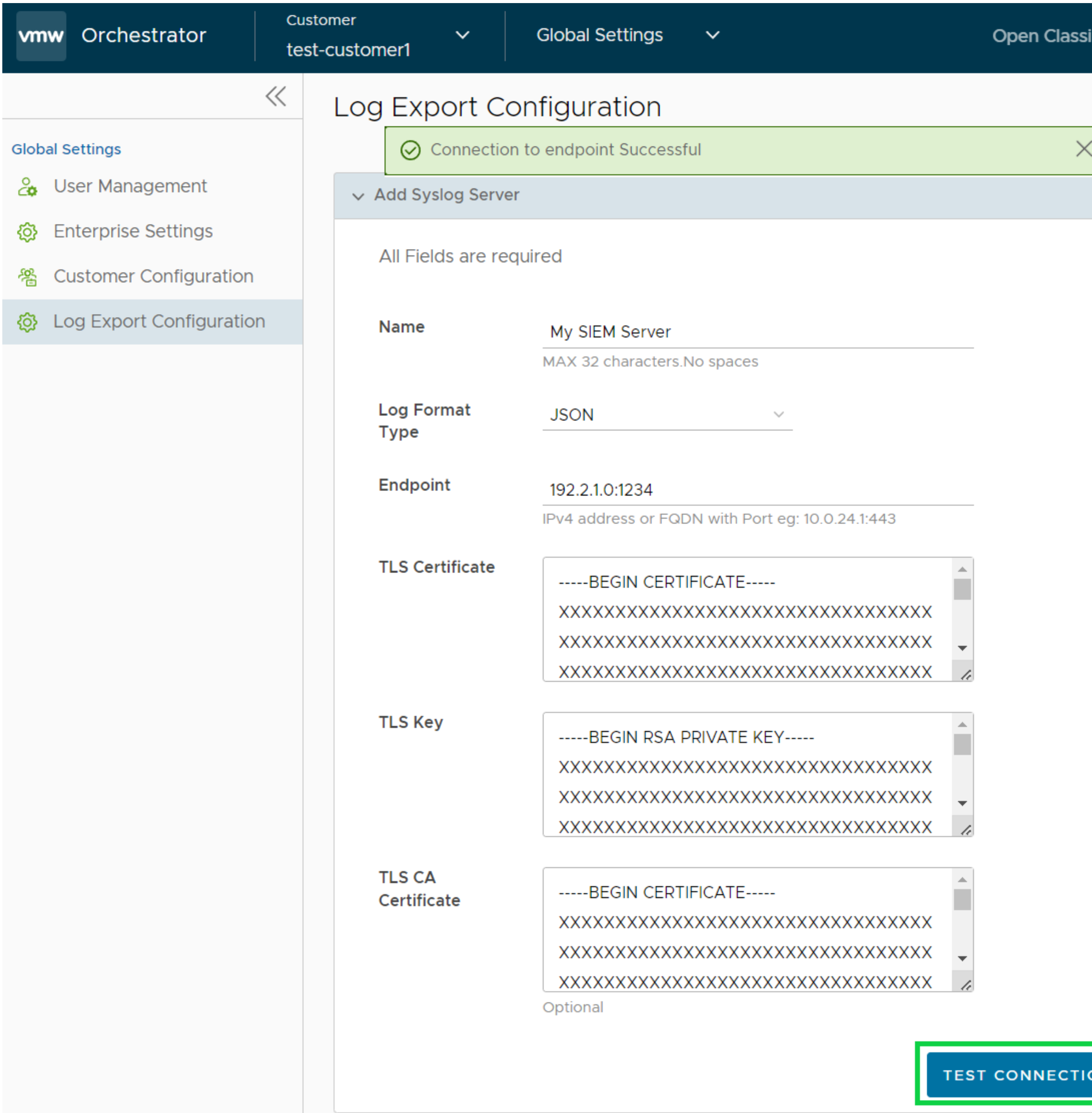
The section covers configuring a Log Export Server, a prerequite for using the Cloud Web Security Log Export.

Before you can configure the Cloud Web Security Log Export feature, you must first configure a Log Export Server. The Log Export Server is configured at a global level and can be used not only for Cloud Web Security but for any SASE service that includes a log export feature.

Add or Edit a Log Export Server

To view or create a Log Export server, go to **Global Settings > Log Export Configuration**. The page to configure is titled **Add Syslog Server**.

Figure 12-1. Global Settings > Log Export Configuration



Connection to endpoint Successful

All Fields are required

Name: My SIEM Server
MAX 32 characters.No spaces

Log Format Type: JSON

Endpoint: 192.2.1.0:1234
IPv4 address or FQDN with Port eg: 10.0.24.1:443

TLS Certificate:
```
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

TLS Key:
```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

TLS CA Certificate:
```
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```
Optional

Table 12-1.

Log Export Configuration	
Name	Whatever name you want to assign to this endpoint.
Log Format Type	You can select from three different log format types: **LEEF**, **JSON**, and **CEF**. For the purposes of configuring a l Cloud Web Security, you must select **JSON** as Cloud Web Security only sends fields names with the JSON form

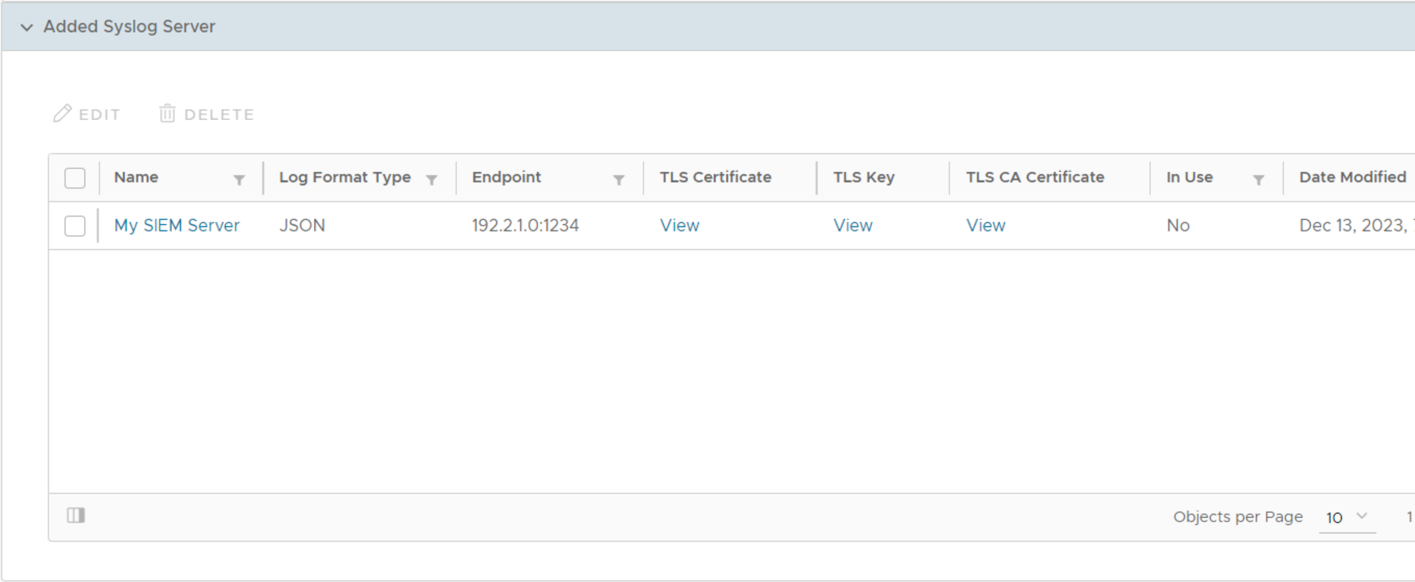
Table 12-1. (continued)

Log Export Configuration	
Endpoint	The server endpoint must be either an IPv4 address or an FQDN with a port.
TLS Certificate	Fill in (or paste) the Transport Layer Security (TLS) Certificate.
TLS Key	Fill in (or paste) the Transport Layer Security (TLS) Key.
TLS CA Certificate	This field is optional as some Syslog Server providers do not provide a TLS Certificate Authority (CA) Certificate one, fill in (or paste) it here.
Test Connection	Clicking this button checks to see that VMware can connect to your server successfully. A successful connectio Orchestrator UI showing a green banner that reads "Connection to endpoint Successful". Should the connection fail, you would see an error in a red banner that includes the wording "An error occurred to endpoint..." with specific details and error code. Using this information, please review your settings and corre needed.

When you have completed all required fields and confirmed a successful connection test, click **Add Endpoint** and your server is then added to your list of Syslog Servers.

Once the server is added you can then view it on the lower down on the **Log Export Configuration** page under Added Syslog Server. Once added to this section, you can both review and edit the endpoint configuration.

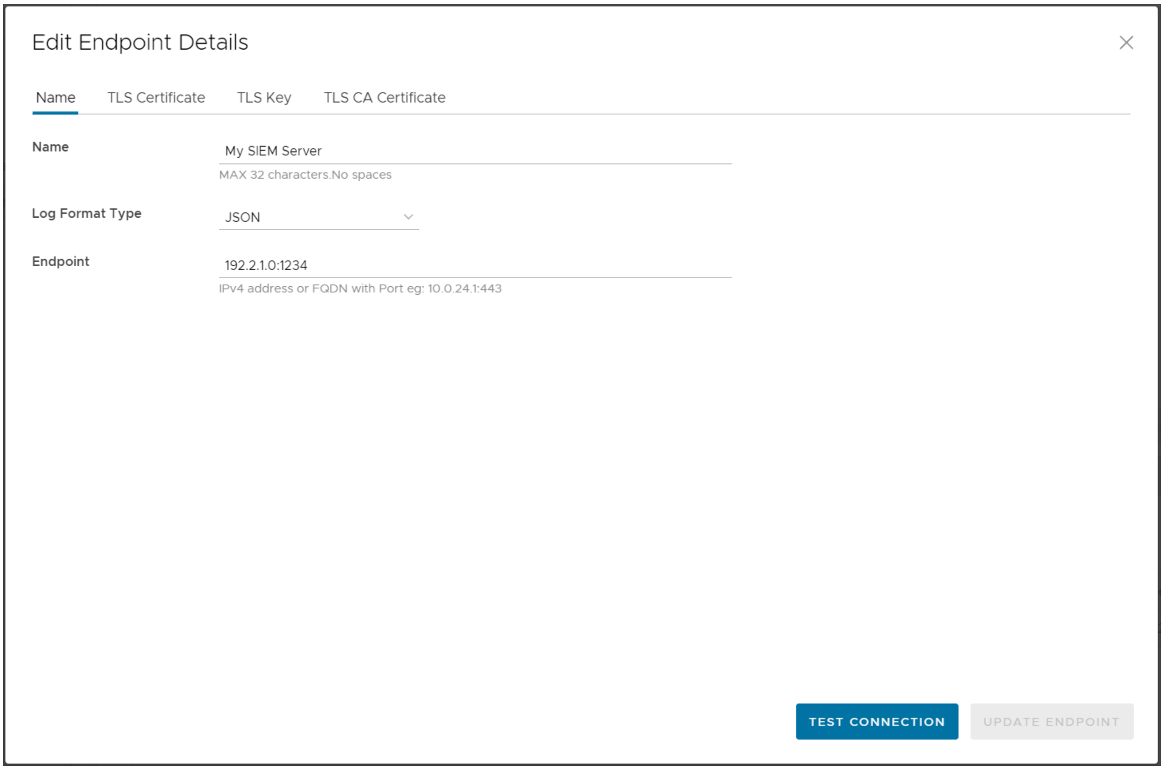
Figure 12-2. Added Syslog Server table



☐	Name	Log Format Type	Endpoint	TLS Certificate	TLS Key	TLS CA Certificate	In Use	Date Modified
☐	My SIEM Server	JSON	192.2.1.0:1234	View	View	View	No	Dec 13, 2023,

You can either click on the name of your server or check the left-hand box and then click **EDIT** to open the **Edit Endpoint Details** page:

Figure 12-3. Edit Endpoint Details



Name: My SIEM Server
MAX 32 characters.No spaces

Log Format Type: JSON

Endpoint: 192.2.1.0:1234
IPv4 address or FQDN with Port eg: 10.0.24.1:443

Once satisfied that your server is properly configured and can connect to the VMware side, you can proceed to configuring the server to receive Cloud Web Security logs.

Configure Log Export for Cloud Web Security

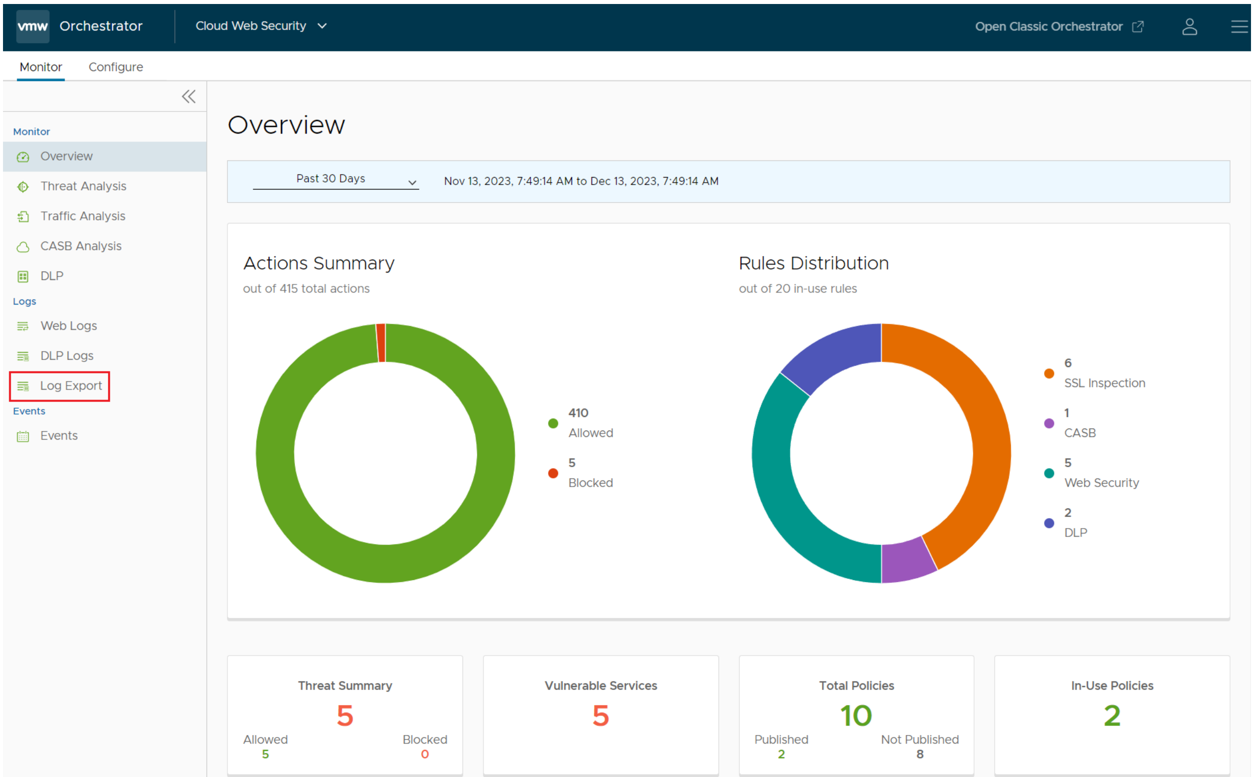
This section covers the configuration of Log Export for Cloud Web Security.

To configure the Log Export feature for Cloud Web Security logs, follow these steps:

1. Navigate to Cloud Web Security > Monitor > Log Export

On the Orchestrator, select **Cloud Web Security** which takes you to the **Cloud Web Security > Monitor** section by default. On the **Monitor** page, select **Log Export** on the left-side menu to view or edit this feature.

Figure 12-4. Cloud Web Security > Monitor - Click on Log Export.



2. Configure Log Export

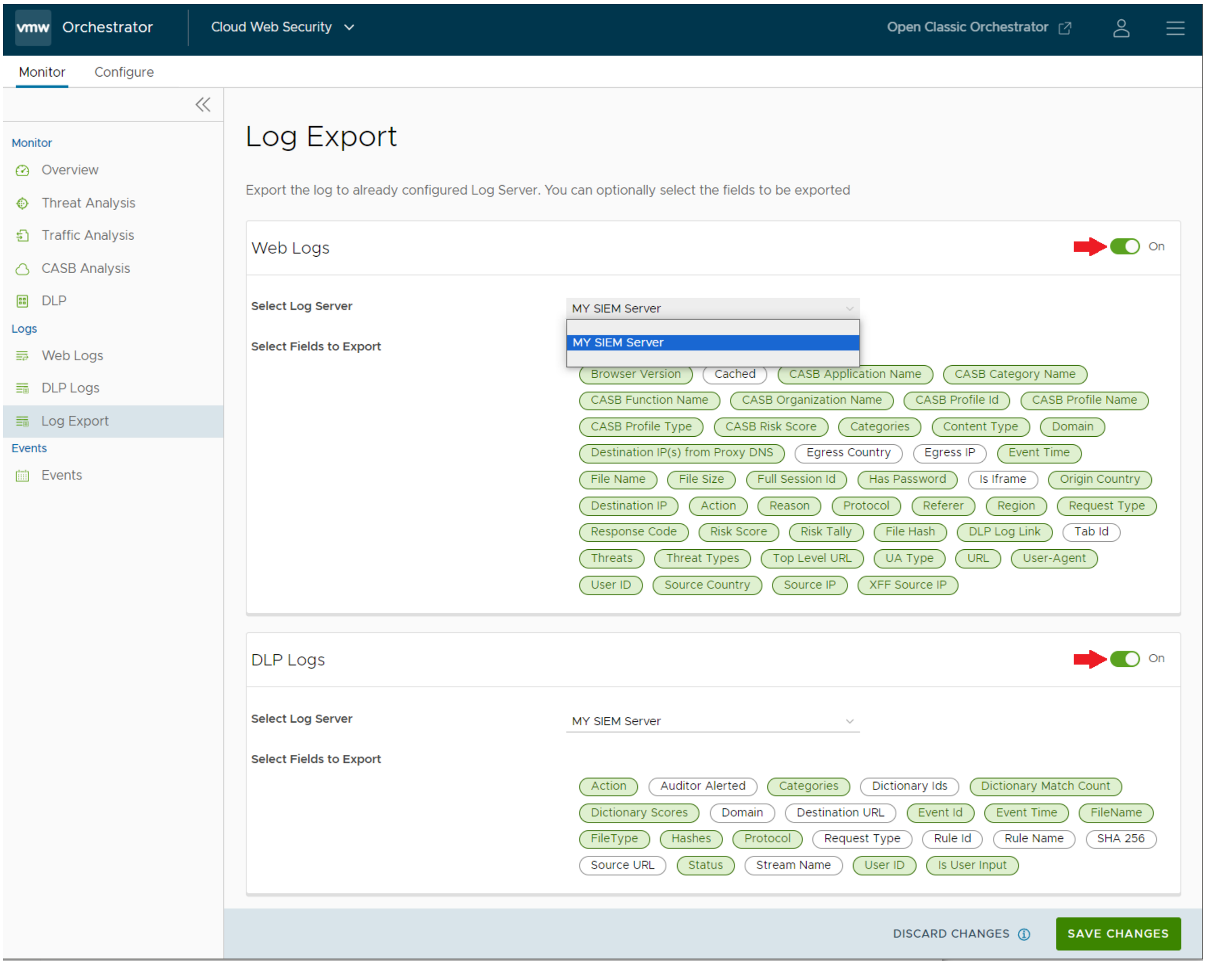
1 On the **Log Export** page, you must first choose which type of logs to export:

   a **Web Logs** derived from CASB, Web Security, and Web Application rules.

   b **DLP Logs** derived from DLP rules.

   For the log types you want exported toggle the **On/Off** slider in the upper right corner.

Figure 12-5. Log Export Configuration Page



Export the log to already configured Log Server. You can optionally select the fields to be exported

Web Logs

Select Log Server: MY SIEM Server

Select Fields to Export

DLP Logs

Select Log Server: MY SIEM Server

Select Fields to Export

2 Once you have chosen which log types to export, you must select a log server under **Select Log Server**. The drop down menu will includes all the log servers you configured under **Global Settings > Log Export Configuration**.

3 In the **Select Fields to Export** section, click on the fields you want exported to your log server.

Note Cloud Web Security only exports these fields in a JSON format and the selected Log Server must be configured to use the JSON format.

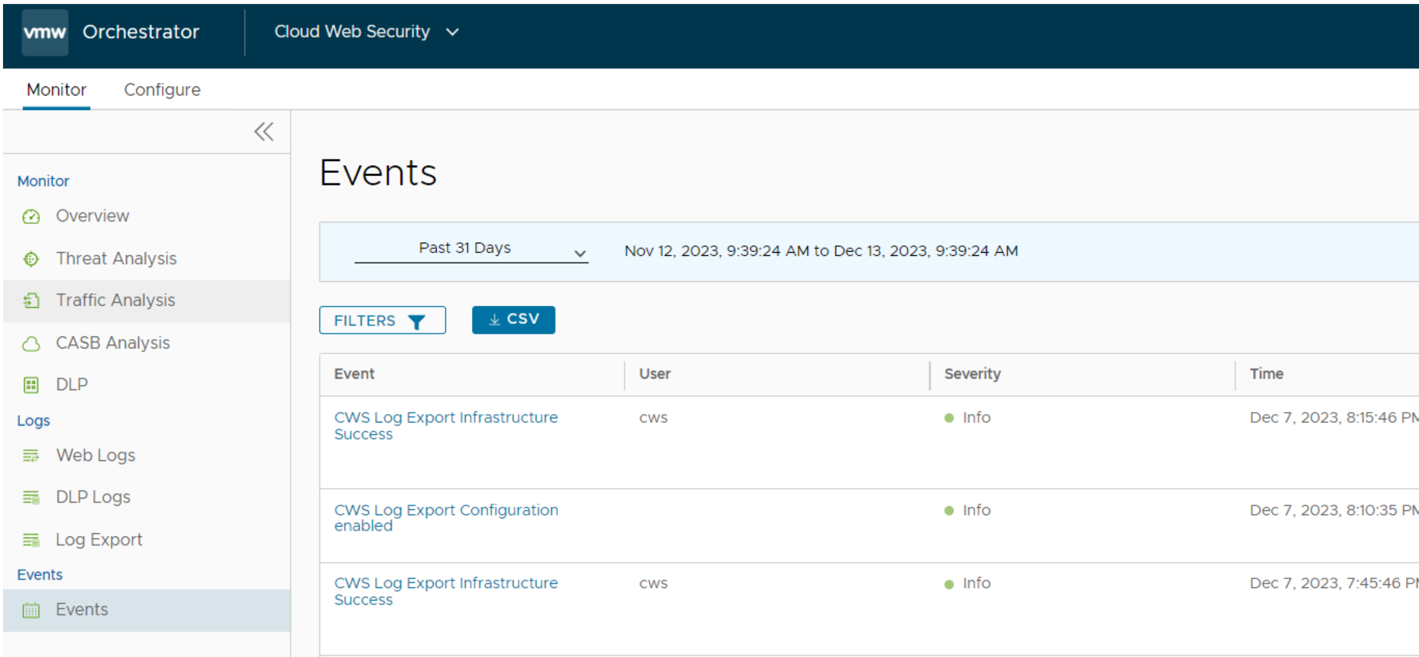
4 Click **Save Changes** to complete the configuration.

Confirm a Successful Configuration

Once you have saved your configuration for **Log Export**, navagate to the **Events** page using the left-hand menu.

On Events, look for or filter for the events shown in the following screen: **CWS Log Export Configuration enabled**, and **CWS Log Export Infrastructure Success**. These events confirm the configuration for the log types and that Cloud Web Security has successfully connected to the log server and can export logs.

Figure 12-6. Confirm a Succesful Configuration on the Events Page



Events

Past 31 Days

Nov 12, 2023, 9:39:24 AM to Dec 13, 2023, 9:39:24 AM

Event	User	Severity	Time
CWS Log Export Infrastructure Success	cws	● Info	Dec 7, 2023, 8:15:46 PM
CWS Log Export Configuration enabled		● Info	Dec 7, 2023, 8:10:35 PM
CWS Log Export Infrastructure Success	cws	● Info	Dec 7, 2023, 7:45:46 PM

Notes Regarding Log Export

- After you complete the initial configuration, it will take from 2-5 minutes for Cloud Web Security to export the first logs.
- Later configuration changes like adding or removing log fields will also take from 2-5 minutes to take effect.
- Syslog entries are sent in batches, not individually.
- Logs are sent continuously, but not instantaneously. Expect up to a 2 minutes delay from the time a log is generated to Cloud Web Security Sending it to your server.

Log Export Field Reference

This section provides information regarding the fields exported for Web Security and DLP logs using the **Log Export** feature for Cloud Web Security.

This section is divided into two sections with tables for Web Logs and for DLP Logs that are exported using Log Export.

Web Security Log Fields

This table includes the log fields when **Log Export** is configured to export Web Security logs.

Table 12-2. Web Security Log Fields

Parameter	Description	Example
browser_and_version	The client browser and its version. Non-browser returns a response of undefined_undefined.	Chrome_65
cached	Indicates whether the resource was obtained from the isolated browser's cache (True) or by downloading from the origin server (False).	True
casb_app_name	Summary of the log source group's function or its contents.	DropBox
casb_cat_name	Cloud application name (for CASB events).	Cloud File Sharing
casb_fun_name	Application category ID.	upload
casb_org_name	Application function name.	Dropbox Inc.
casb_profile_id	Cloud Web Security CASB profile ID.	e47cecae-721f...
casb_profile_name	Cloud Web Security CASB profile name attached to application or exception rule.	upload block
casb_profile_type	Cloud Web Security CASB profile type (sanctioned/unsanctioned/unclassified).	unclassified
casb_risk_score	Cloud Web Security risk score for application (0-10).	3
categories	Category Rules Category type classification (e.g., General, Education, Download Sites, etc.).	Education
content-type	Page type.	text/html; charset=iso-8859-1

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
domain	Domain part of the URL.	example.com
dst	Destination IP that proxy DNS lookup resolved to (may sometimes be a list of IP addresses).	130.65.255.101
egress_country	Egress IP country (isolation instance).	US
egress_ip	IP address for outbound flow (typically from a private network to the Internet).	54.111.221.123
event_time	The access initiate date and time.	2018-04-10T21:00:40.548000
filename	The filename of the file being uploaded or downloaded.	NA
file_size	The size (in bytes) of a file in a file upload/download event.	NA
full_session_id	Unique ID for a page load (used as a correlation ID for other events: uploads/downloads/etc.).	KbJQIDPS-1
hashes	pagingIdentifier object hashes used to find and delete duplicate data from duplicate log fetch api calls.	
has_password	Presence of password in form POST request.	false
is_iframe	Is inline frame (iframe) element (true/false).	true
name	Request type.	page request
next_time	Log pagination uses this field as the start time for query. If no time is present, the original start and end time is used.	
origin_country	Country of actual IP address of the destination server (origin_ip).	FR
origin_ip	Actual IP address of the destination server.	130.65.255.101

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	
pe_action	The Cloud Web Security action taken for the session (Isolate, Allow, Block, or Direct). Direct actions are external application links that a user may click to launch through their web browser (e.g., anchor links, javascript navigations and mailto links).	isolate
pe_reason	Web policy rule ID responsible for the Cloud Web Security action. This can be empty for some cases.	6c6ea27d-5350
product	The Cloud Web Security product.	CWS
protocol	The protocol used for the session (http or https).	http
referer	Page request referer address.	https://www.adobe.com
region	AWS region and availability zone.	us-west-1b
request_type	The method type for the request (GET, PUT, POST, etc.).	GET
response_code	HTTP response status code.	200
risk_score	Risk calculated for URL.	low
risk_tally	Cout of risks encountered.	4
sbox	Sandbox Inspection Result	Infected

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
sbox_mal_act	List of malicious activities found	- Signature:EICARtestfiledetection. - Signature:Trigger

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
		smalware detections by Sophos Anti-Virus. - Suspicious: A

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
		n executable with low reputation
severity	The severity level for the session. This is currently fixed at 5.	5
sha256	SHA256 hash of this file or document or text. This provides a cryptographically unique identifier.	fd1aee67...
soph	Full file scan result.	Clean (Sandbox Required)
soph_dlp_ref	DLP log link.	NA
tab_id	Tab creation number within a surrogate (used to track how an individual tab is navigated by a user).	1

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
threats	Threat type identified by Cloud Web Security internal data (what the Risks field is set to).	cats_Phishing&Fraud
threat_types	Top level risk.	Phishing
timestamp	Start time of the requesting log. This is internal to the log database.	2023-04-10T21:00:02.599Z
top_url	Top level URL (in case of iframe).	https://example.com
ua_type	The type of user agent (supported/unsupported/non browser).	supported_browser
url	The Destination URL	https://example.com

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
user-agent	The software (software agent) acting on behalf of a user (commonly a web browser).	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
userid	The User ID for the log (in Anonymous mode, this is anon-xxx).	admin@vmware.com
vendor	The product vendor name (Cloud Web Security).	Cloud Web Security
version	The Cloud Web Security product version.	1.16.0

Table 12-2. Web Security Log Fields (continued)

Parameter	Description	Example
virus_details	Virus detail.	EICAR-NOT-A-VIRUS
x-client-country	Country for IP request from user.	US
x-client-ip	Source IP.	12.206.221.226

DLP Log Fields

This table includes the log fields when **Log Export** is configured to export DLP logs.

Table 12-3. DLP Log Fields

Parameter	Description	Example
action	Action taken for session (block or log).	block
alerted	Whether or not an email alert was sent to a DLP Auditor profile.	false
categories	Category Rules Category type classification (e.g., General, Education, Download Sites, etc.).	Download Sites
ccl_ids	Name of DLP dictionary that was violated. If there are multiple violations, this will be an array of strings.	Credit...
ccl_match_counts	Number of matches of the string that caused the violation. If there are multiple violations, this will be an array of match counts in the same order as the list of dictionaries from ccl_ids field.	1
ccl_scores	DLP score from the dictionary that caused the violation. If there are multiple violations, this will be an array of DLP scores in the same order as the list of dictionaries from ccl_ids field.	1
domain	Domain part of the URL.	tinyupload.com

Table 12-3. DLP Log Fields (continued)

Parameter	Description	Example
dst_url	Destination URL.	http://tinyupload.com
event_id	Unique identifier for the DLP request (corresponds to the file_id in web log if this is a file upload).	a4c216...
event_time	The access initiate date and time.	2023-03-09T17:16:22.227000
filename	The name of the file that triggered the DLP violation (for file uploads).	credit_cards.csv
file_type	Type of file that triggered the DLP violation.	CSV
hashes	pagingIdentifier object hashes used to find and delete duplicate data from duplicate log fetch api calls.	
name	Request type.	file_upload
next_time	Log pagination uses this field as the start time for query. If no time is present, the original start and end time is used.	
pagingIdentifiers	Identifier used for log pagination if needed to download all log entries (i.e., the request returned more than 1000 records).	
product	The Cloud Web Security Product.	CWS
protocol	The protocol used for the session (http or https).	http
request_type	The method type for the request (GET, PUT, POST, etc.).	POST
rule_id	DLP policy rule identifier responsible for the action taken.	1f3ef32...
rule_name	Name of the DLP policy rule that was violated.	Credit card block rule

Table 12-3. DLP Log Fields (continued)

Parameter	Description	Example
severity	The severity level for the session. This is currently fixed at 5.	5
sha256	SHA256 hash of this file or document or text. This provides a cryptographically unique identifier.	fd1aee67...
src_url	Source URL.	http://tinyupload.com/
status	Result from the DLP engine (currently fixed at dirty).	dirty
stream_name	Internal name used for the file (usually working_file) or text stream (uid).	1a856c756fea
timestamp	Start time of the requesting log. This is internal to the log database.	2023-03-09T17:16:22.227Z
userid	User ID for the log (in Anonymous mode, this is anon-xxx).	admin@vmware.com
user_input	Whether or not this event was generated as a result of user form input.	false
vendor	The product vendor name (Cloud Web Security)	Cloud Web Security
version	The Cloud Web Security product version.	1.16.0