VMware Cloud Web Security Configuration Guide

VMware Cloud Web Security 4.5

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

https://docs.vmware.com/

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

Copyright © 2021 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 VMware Cloud Web Security Configuration Guide 4

VMware Cloud Web Security Overview 4

Prerequisites 6

Configuring a SD-WAN Gateway for a Cloud Web Security Role 6

Creating a Security Policy 7

Configuring a Security Policy 9

Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended 30

Applying a Security Policy 37

Monitoring Cloud Web Security 40

2 Single Sign-On Guides (SAML) 43

Configuring Azure Active Directory (AD) as an Identity Provider (IdP) with VMware Cloud Web Security 43

Configuring Workspace ONE Access as an Identity Provider (IdP) with VMware Cloud Web Security 56

VMware Cloud Web Security Configuration Guide

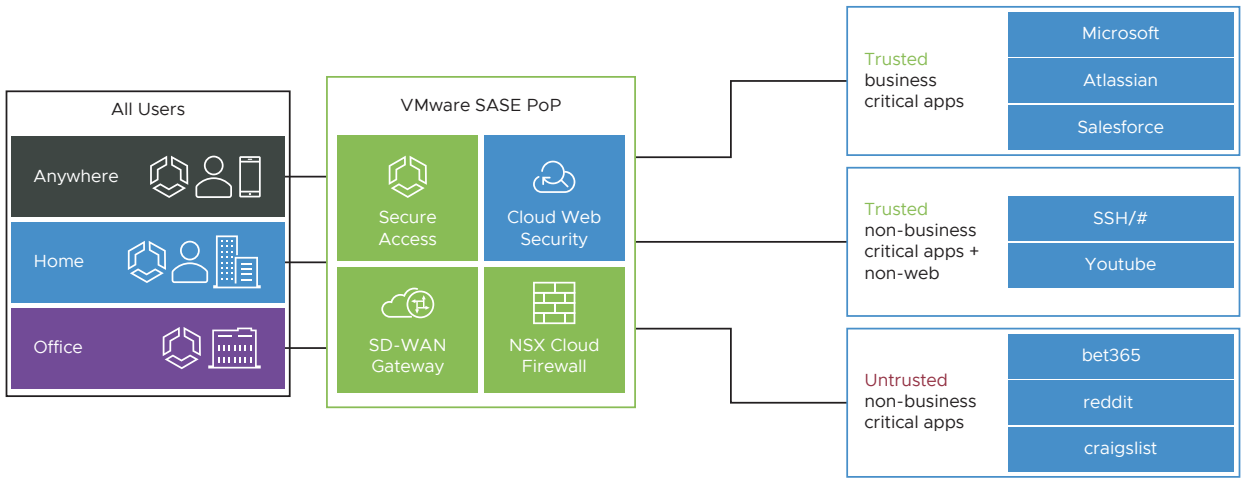
1

This chapter includes the following topics:

- VMware Cloud Web Security Overview
- Prerequisites
- Configuring a SD-WAN Gateway for a Cloud Web Security Role
- Creating a Security Policy
- Configuring a Security Policy
- Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended
- Applying a Security Policy
- Monitoring Cloud Web Security

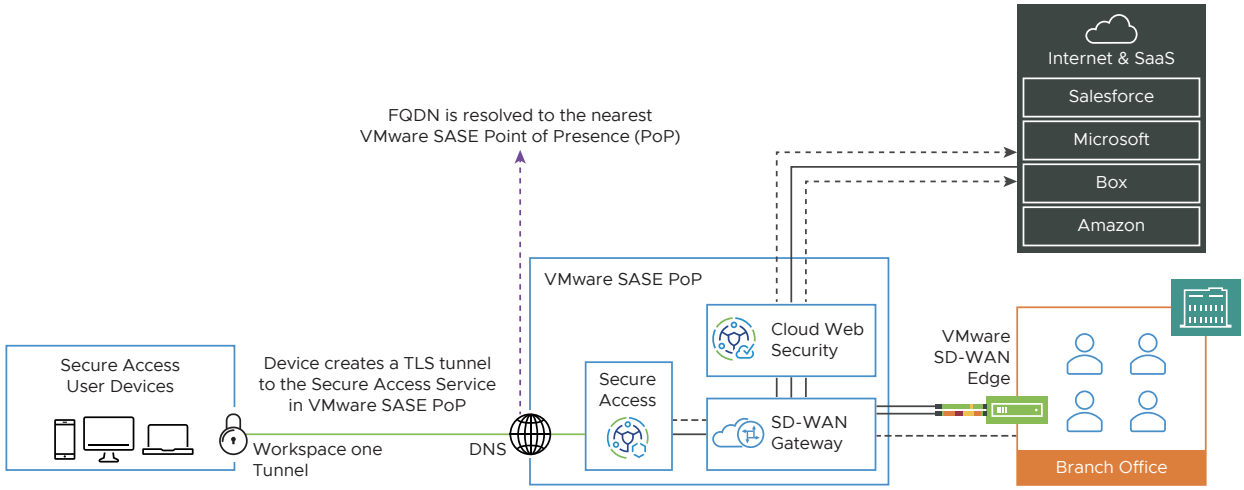
VMware Cloud Web Security Overview

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 (CWS) 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



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 or on a DIY basis and used by 150+ telecommunication partners and thousands of Value Added Resellers globally.

Prerequisites

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

- The customer enterprise must be hosted by a VMware SASE 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.
- The customer must have at least one VMware SD-WAN Edge using 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

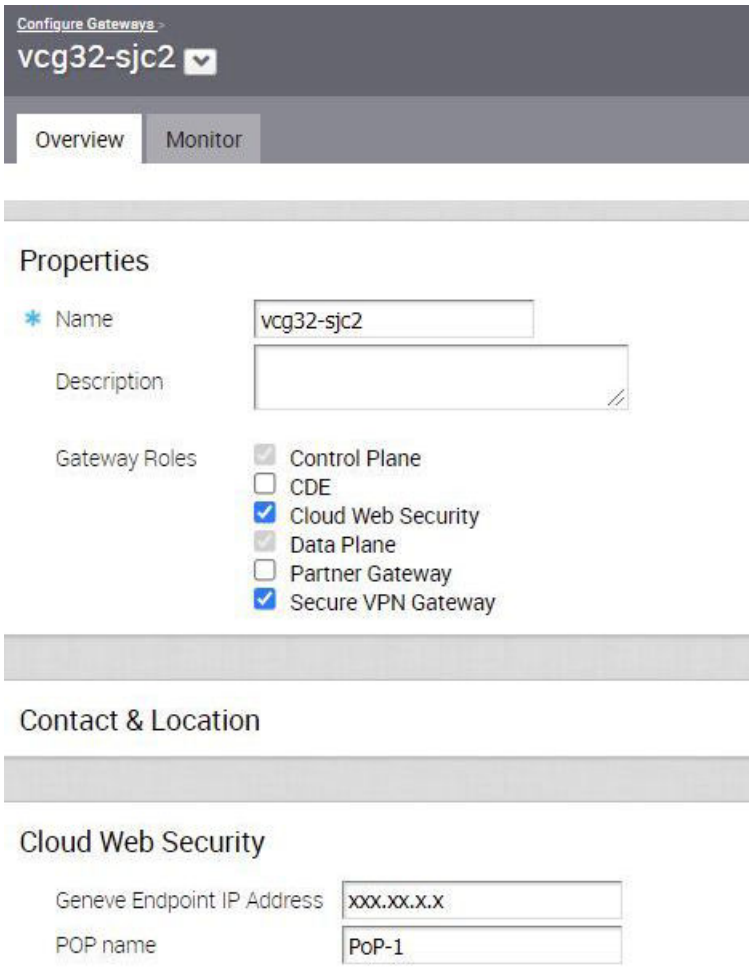
Only an Operator User with either a Superuser or Standard role can configure a SD-WAN Gateway for a Cloud Web Security role.

You can configure a Gateway for a Cloud Web Security role in the Old Orchestrator UI portal.

Procedure

1 In the Operator portal, click **Gateways**.

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



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

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 *Configure 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

- Creating a Security Policy

Creating 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.

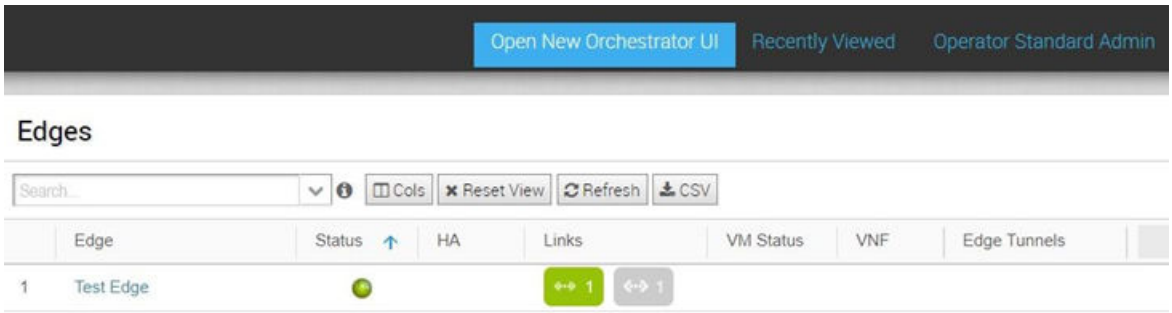
Prerequisites

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

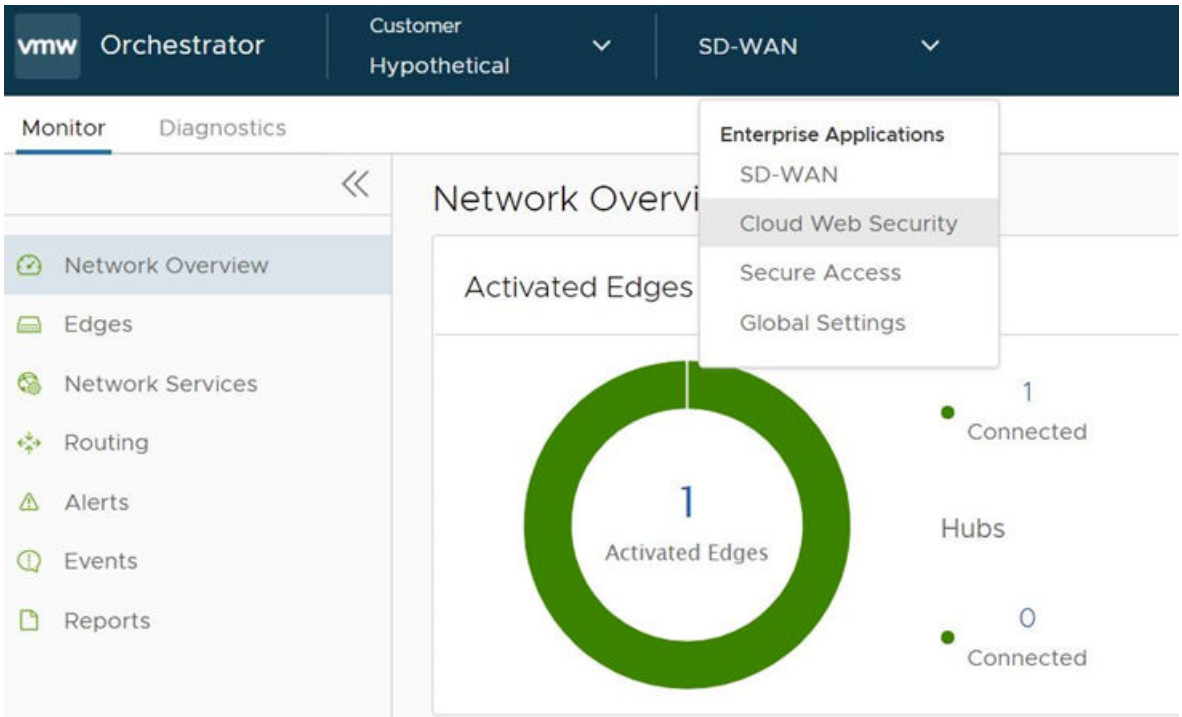
- An Operator with a superuser or standard roles.
- A Partner user with a superuser or standard role.
- A Customer user with a superuser, standard, or security admin role.

Procedure

1 In the Orchestrator portal, click the **Open New Orchestrator UI** option available at the top of the Window.

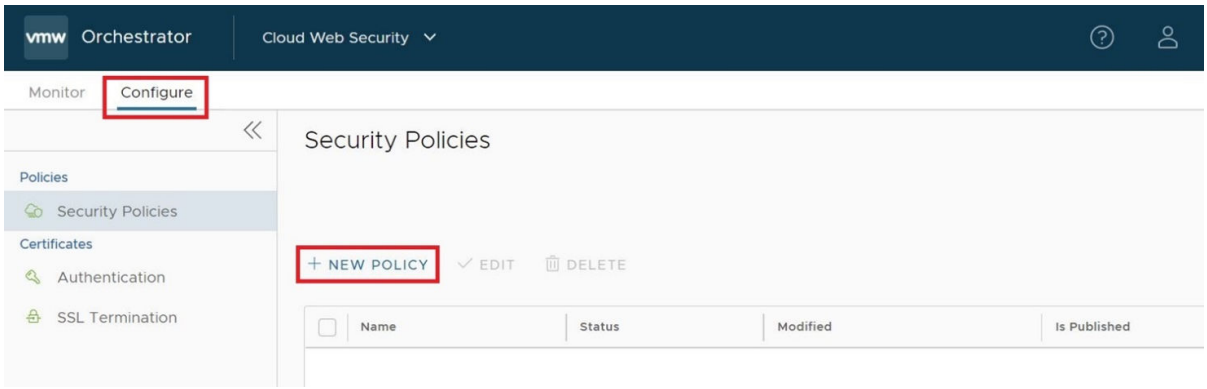


2 Click **Launch New Orchestrator UI** in the pop-up window. The UI opens in a new tab.



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

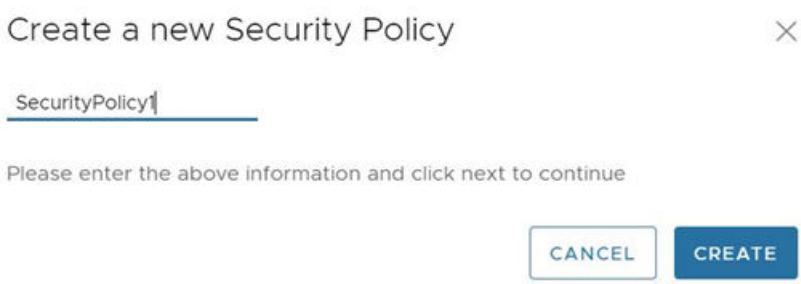
The **Cloud Web Security** page appears.



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

4 To create a new Security Policy, click the **Configure** tab in the left hand corner of the page, and then click **NEW POLICY**.

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



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.

Results

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

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, a user must have first created, configured, and applied a Security Policy. For specific instructions on how to achieve this, see Creating a Security Policy.

About this Task:

In this section, a user will learn how configure the Security Policy that was created in the section titled, Creating a Security Policy. When creating a Security Policy, there are four rule categories that a user can configure: SSL Inspection, URL Filtering, Content Filtering, and Content Inspection.

Note 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 VMware 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 enabled and SSL Inspection is being performed, theis 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 disabled on the browser.

To block QUIC, configure a Cloud Web Security rule that blockes 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 enables SSL inspection without negatively impacting the user experience.

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

To disable 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.

Procedure:

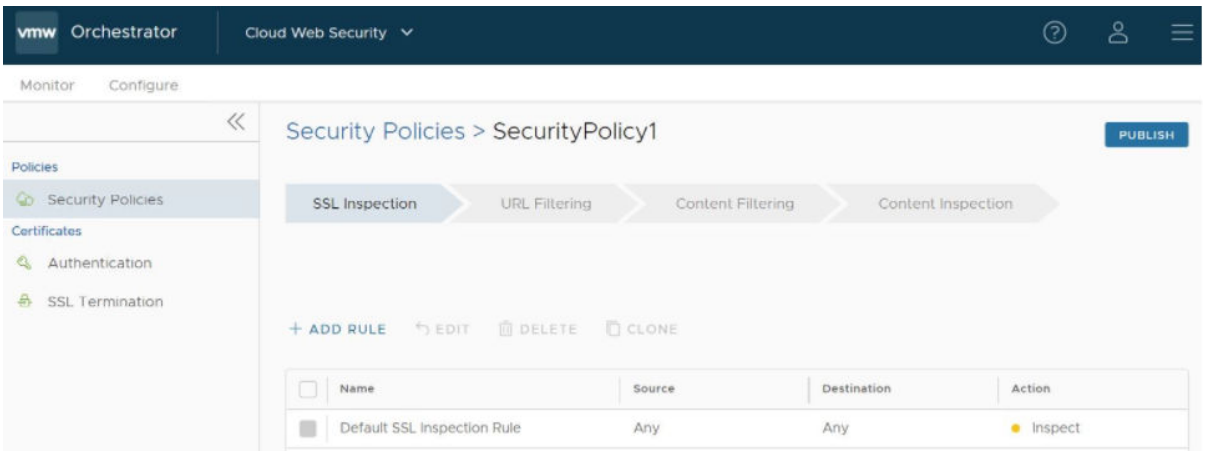
To configure a Security Policy:

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

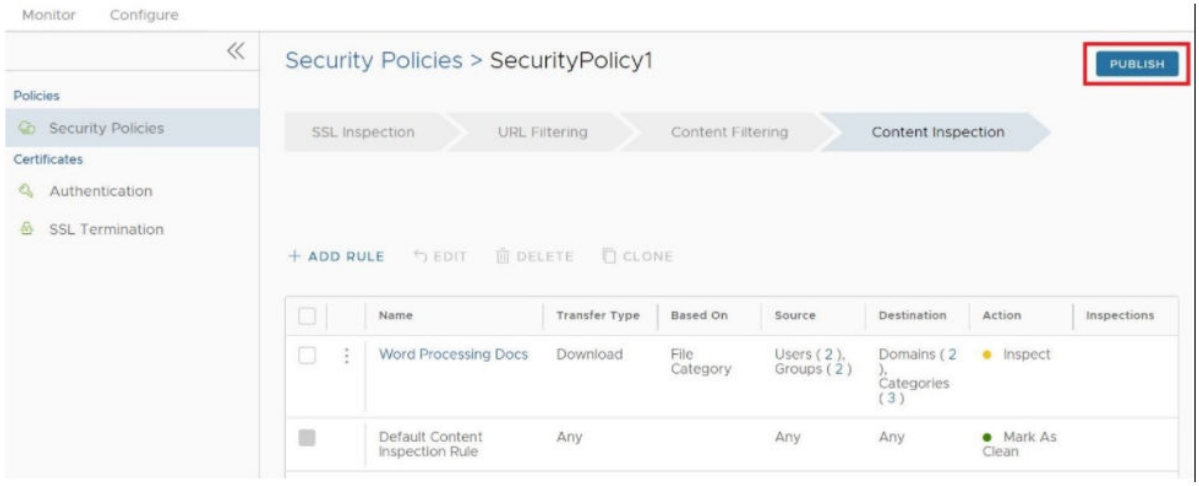
The **Security Policies** screen for the selected policy appears.

2 From the selected Security Policy page, a user can configure rules from the following four rule categories: SSL Inspection, URL Filtering, Content Filtering, and Content Inspection, as shown in the image below. See the Security Policy Categories section for a complete description of how to configure rules for each category (SSL Inspection Category, URL Filtering Category, Content Filtering Category, and Content Inspection Category).

Note By default, a Security Policy has “allow all” and “decrypt all” rules. By configuring any of the four rule categories listed above, a user is overriding default rules and creating a policy comprised of his or her own rules.



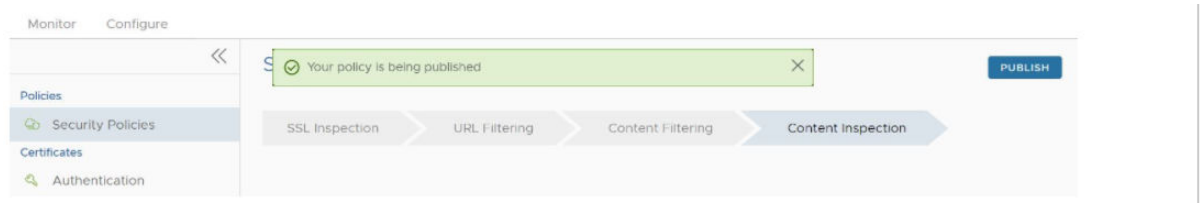
3 After configuring the Security Policy, click the **Publish** button to publish the Security Policy. See the image below.



The Publish Policy pop up dialog appears, as shown in the image below.

4 Click the **Yes** button to publish the policy.

A green banner appears on the top of the screen indicating that the Security Policy is being published, as shown in the image below.



Note A Security Policy can be published at any time in the configuration process, and be republished whenever the user revises it.

What to do next:

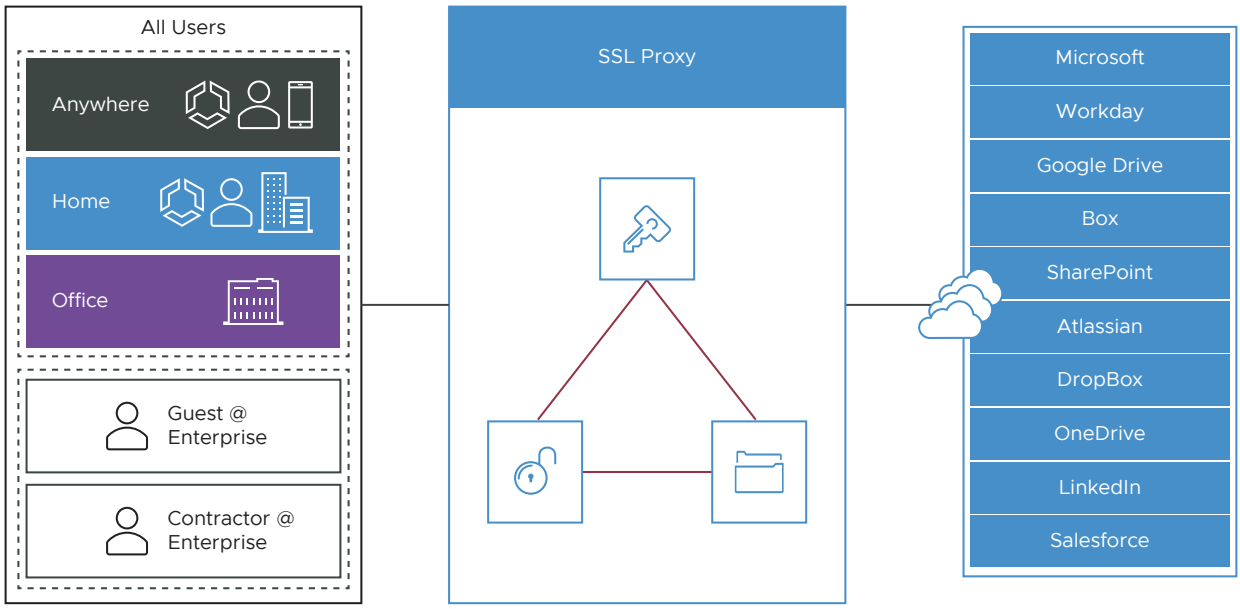
- Applying a Security Policy

Security Policy Categories

The sections below describe in detail the four rule categories a user can configure for a selected Security Policy, as mentioned in Step 2 in the 'Procedures' section above. By configuring any of these categories, a user is overriding default rules.

Note Before performing the steps in the individual sections listed below, a user must have completed Step 1 first, as described in the 'Procedures' section above.

SSL Inspection Category



Because 90 percent of Internet traffic is encrypted, there is a need to decrypt the traffic to inspect what is inside. 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, a user can configure exceptions to this default SSL Inspection rule, which would allow the traffic to bypass SSL Inspection.

Note 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 Termination on the left side of the Cloud Web Security > Configuration menu.

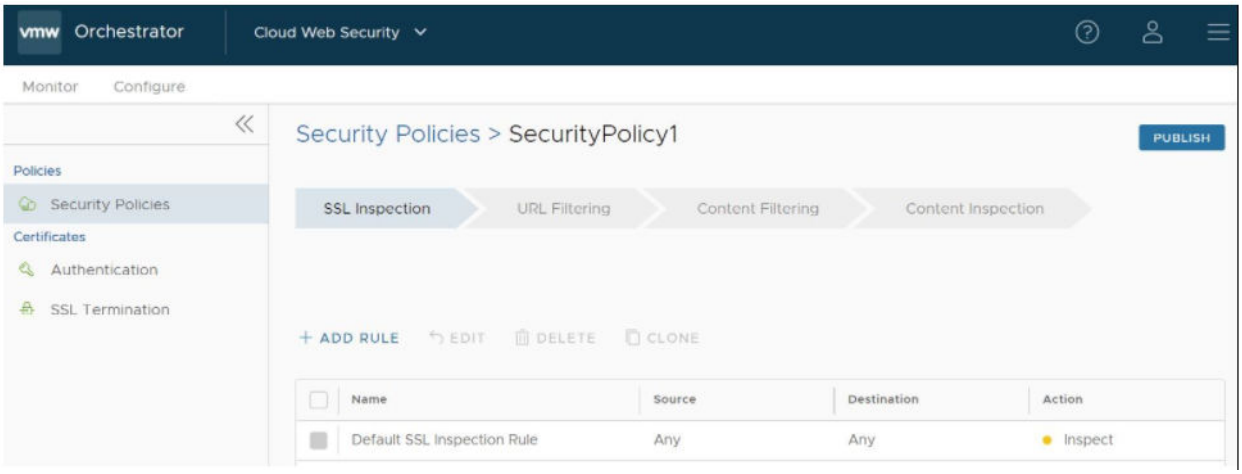
On the SSL Termination page is a downloadable VMware Cloud Web Security CA certificate used to perform SSL Inspection. To download the CA certificate:

1 Click the Certificate icon or link to download

2 Save file and note location

3 Note the Certificate thumbprint, for validation on import

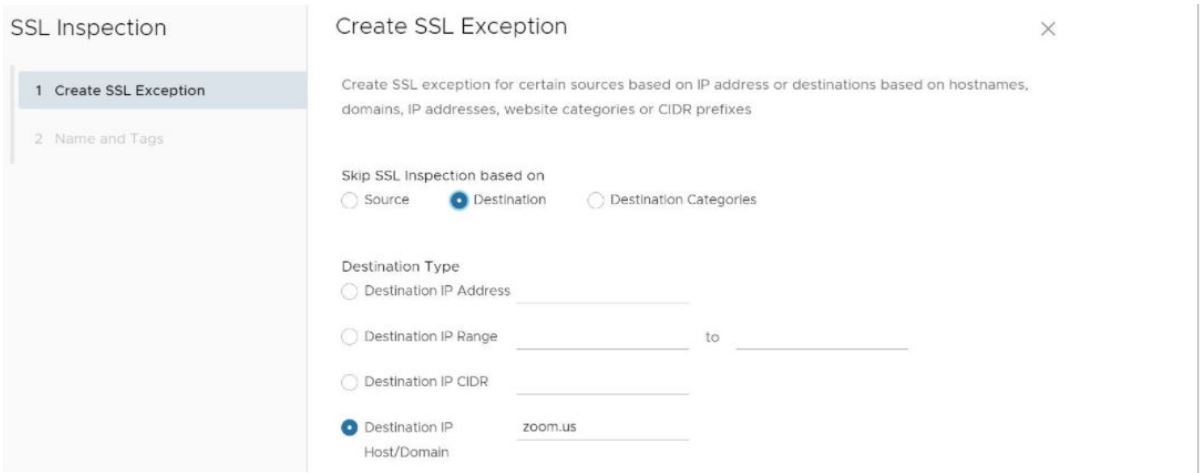
If a user wants to make an exception to the default rule and does not want Cloud Web Security to decrypt SSL encrypted packets, the user would make a rule for that traffic based on either source, destination, or destination categories (image below). Follow the steps below to make an exception to the default rule.



To configure an SSL Inspection rule:

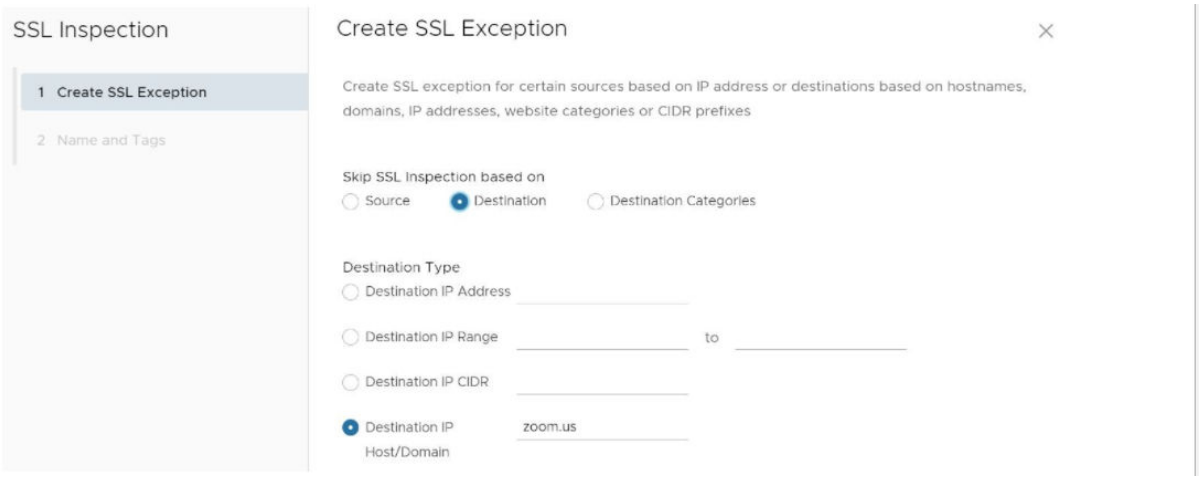
1 On the SSL Inspection tab of the Security Policies screen, select **+ ADD RULE**, as shown in the image above to configure the SSL Inspection Exception rule.

The **Create SSL Exception** screen appears. See image below.



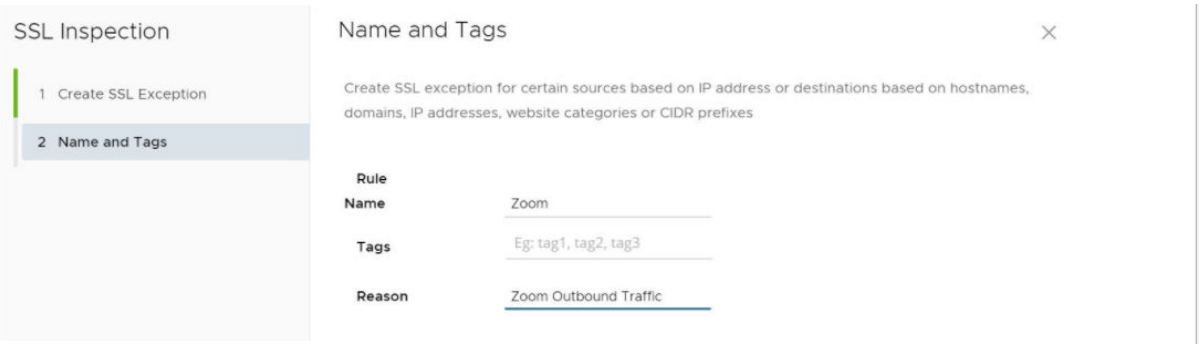
2 In the **Create SSL Exception** screen, the user chooses which type of traffic to bypass SSL Inspection by selecting either **Source**, **Destination**, or **Destination Categories**.

For example, the user could 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. See the image below for an illustration of this example.



3 Click the **Next** button.

4 In the **Name and Tags** screen, indicate the Rule Name, Tags, and if necessary, a Reason for why the bypass rule was created, as shown in the image below.



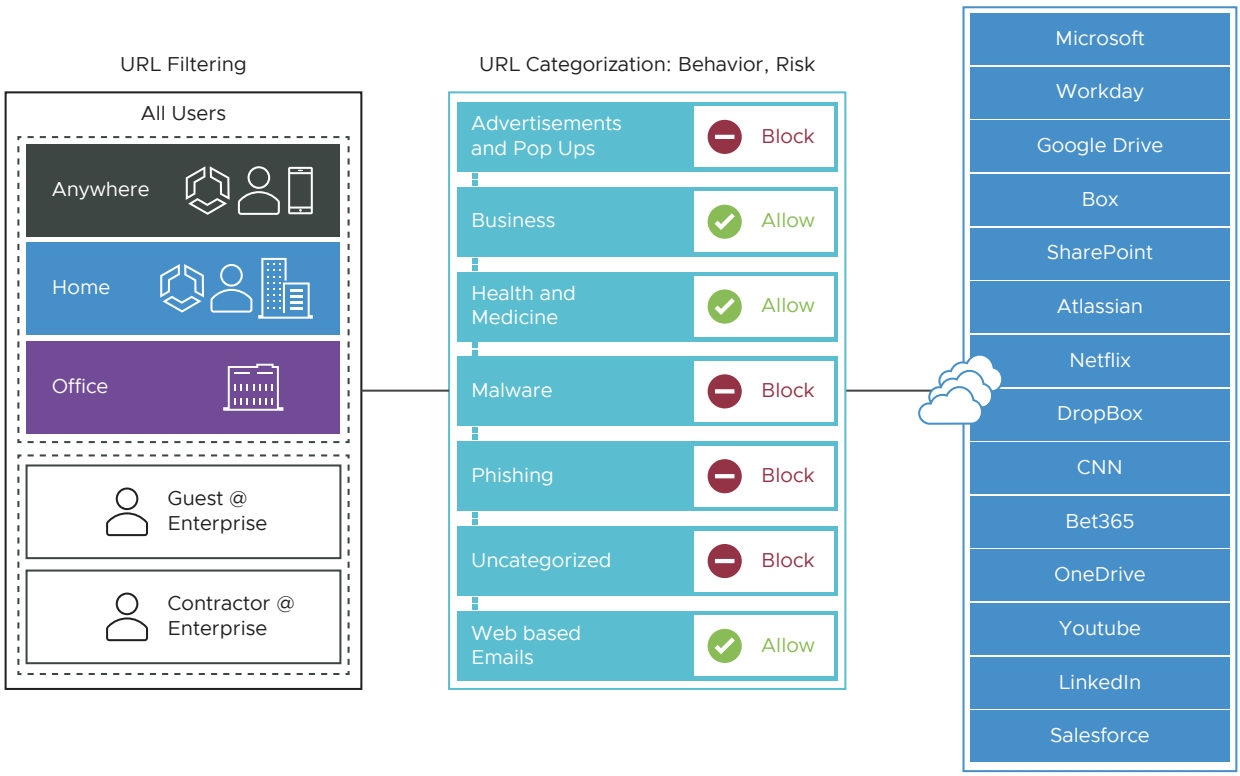
5 Click **Finish**.

The rule is now added to the Security Policy.

6 The user has 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.

7 After publishing the Security Policy, the user is ready to Applying a Security Policy.

URL Filtering Category



URL Filtering allows the user 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 the user to change the default behavior. In order to change the default behavior, the user can choose from three kinds of rules URL Filtering enforces: Category, Threat, and Domain. See the steps below to configure a Security Policy rule for URL Filtering.

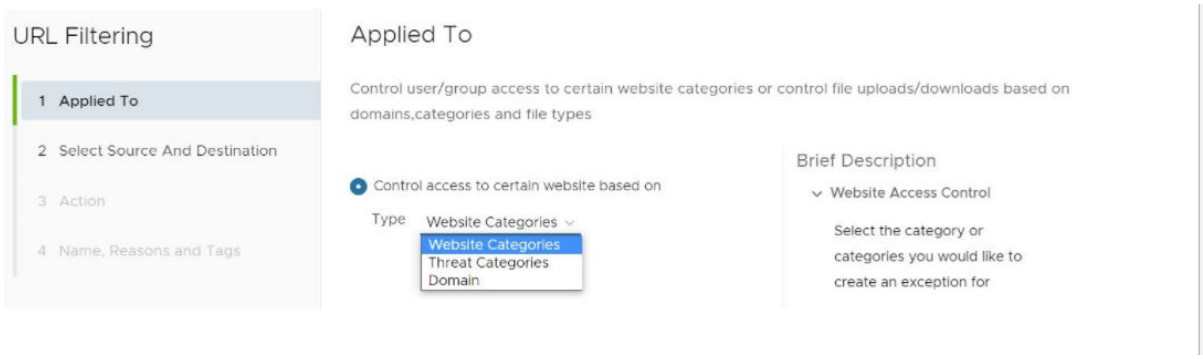
To configure a URL Filtering Rule:

1 In the selected **Security Policies** screen, click the **URL Filtering** tab, located at the top of the screen.

2 Select **+ ADD RULE** and click the **Next** button.

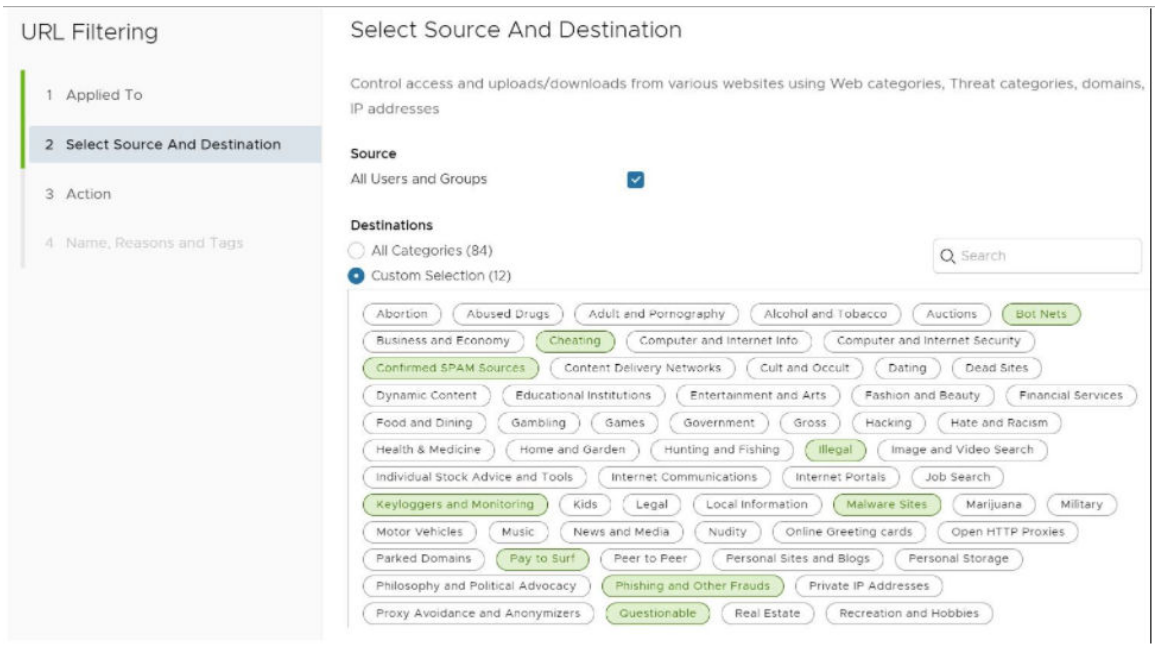
The **URL Filtering Applied To** screen appears, showing three options to choose from (Web Categories, Threat Categories, and Domain from the **Type** drop-down menu, as shown in the image below.

3 In the **Type** drop-down menu, choose one of three options (Website Categories, Threat Categories, or Domain), as shown in the image below. See the sub steps below for specific steps to follow for each category option.



a Website Categories Option: The user selects the **Website Categories** option to configure a rule based on pre-configured categories that comprise a large number of URLs. Follow the sub steps below to configure using this category.

The **Select Source and Destination** screen appears, as shown in the image below.



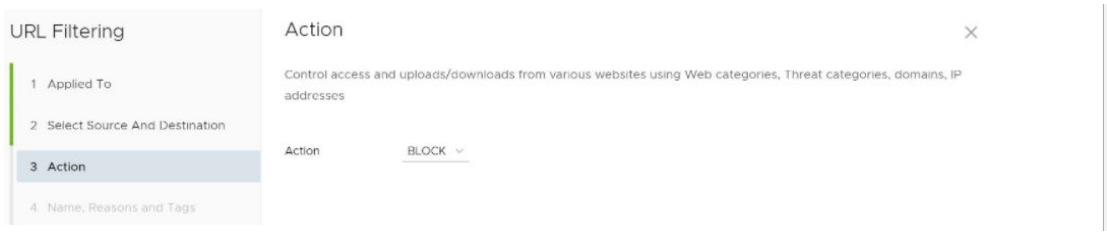
1 In the **Select Source and Destination** screen, under **Source**, check the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.

2 In the **Select Source and Destination** screen, under **Destinations**, 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 the user to specify which categories to apply to the rule by clicking on each category, as shown in the image above.

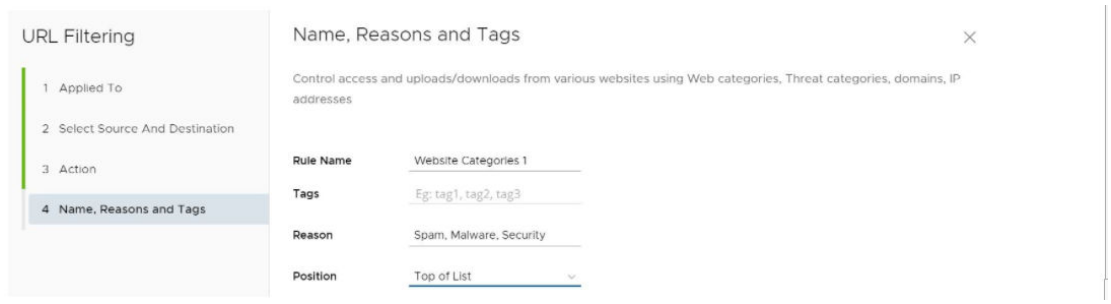
3 Click the **Next** button.

4 **In the URL Filtering Action** screen, choose **Block** or **Allow** from the drop-down menu to determine if the rule is for blocking URL's or allowing them. (See image below).

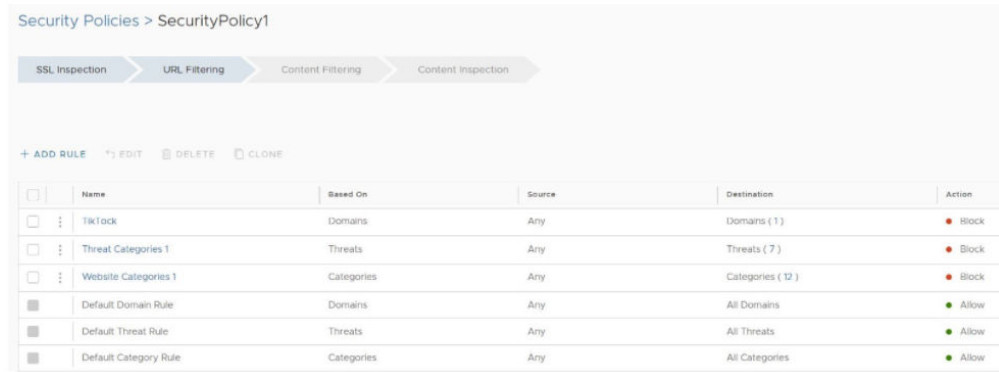
5 Click the **Next** button.



6 In the **Name, Reasons, and Tags** screen, enter information in the following fields: Rule Name, Tags, Reason, and Position. NOTE: The Position field designates the rule's position on the list of URL filtering rules.



7 Click the **Finish** button and the rule will be posted on the URL Filtering list. The main **URL Filtering** screen appears.

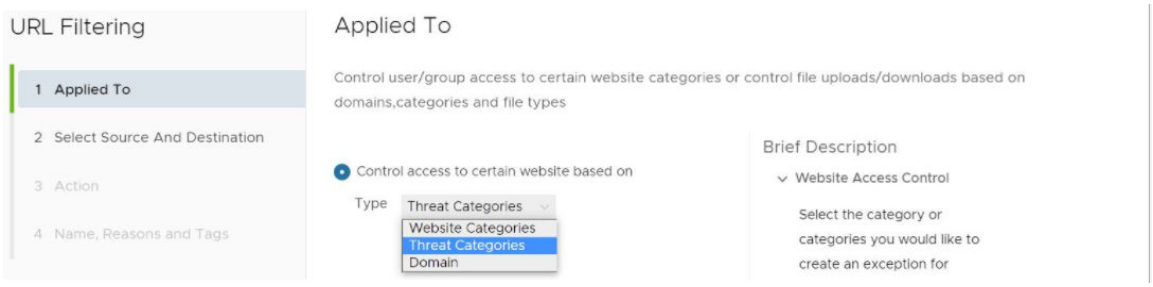


8 The user has the following options: configure another SSL Inspection rule, configure a different Security Policy category, or if finished, click the **Publish** button to publish the Security Policy.

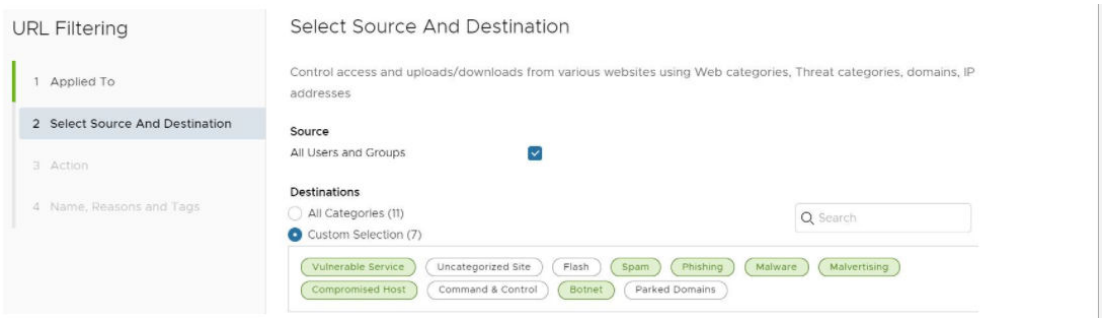
9 After publishing the Security Policy, the user is ready to Applying a Security Policy

b Threat Category Option: The user selects the Threat Categories option from the drop-down menu to apply threat types (based on updated information from cybersecurity firms), follow the sub steps below. See image below.

c Click the **Next** button.



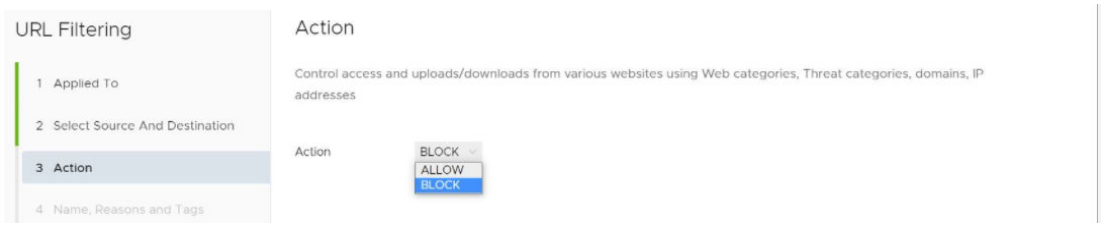
1 In the **Select Source and Destination** screen, under **Source**, check the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.



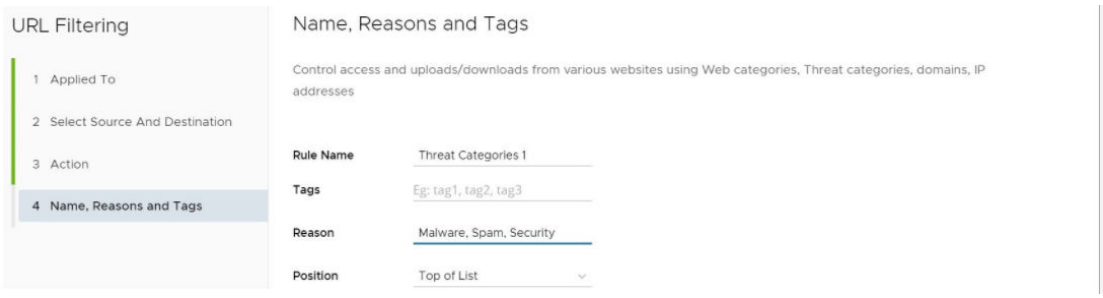
2 In the **Select Source and Destination** screen, under **Destinations**, select either **All Categories** or **Custom Selection**. The **All Categories** option highlights all available categories and applies them to the rule. The **Custom Selection** option allows the user to specify which categories to apply to the rule by clicking on each category, as shown in the image above.

3 Click the **Next** button.

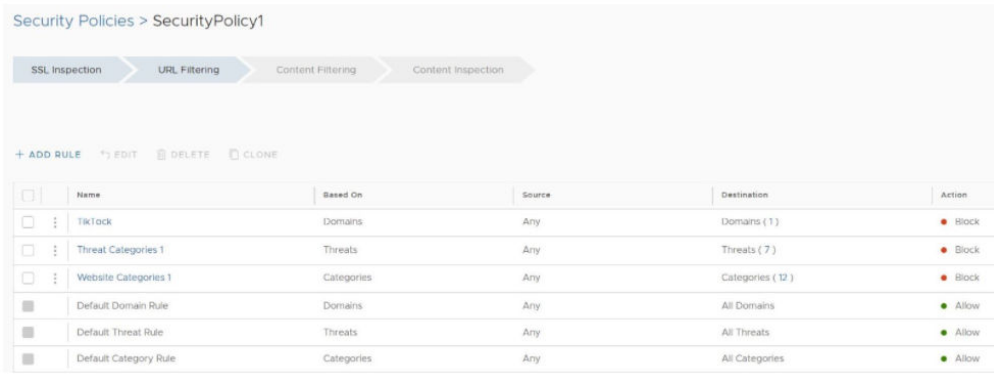
4 In the **URL Filtering Action** screen, specify if the specific threats are to be blocked or allowed. See image below.



5 In the **Name, Reasons and Tags** screen, enter information in the following fields: Rule Name, Tags, Reason, and Position. NOTE: The Position field designates the rule's position on the list of URL filtering rules.



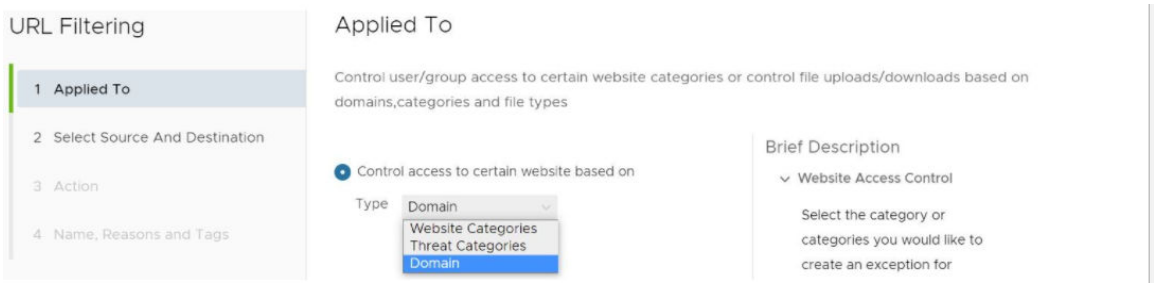
6 Click the **Finish** button and the rule will be posted on the URL Filtering list. The main **URL Filtering** screen appears.



7 The user has 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.

8 After publishing the Security Policy, the user is ready to Applying a Security Policy

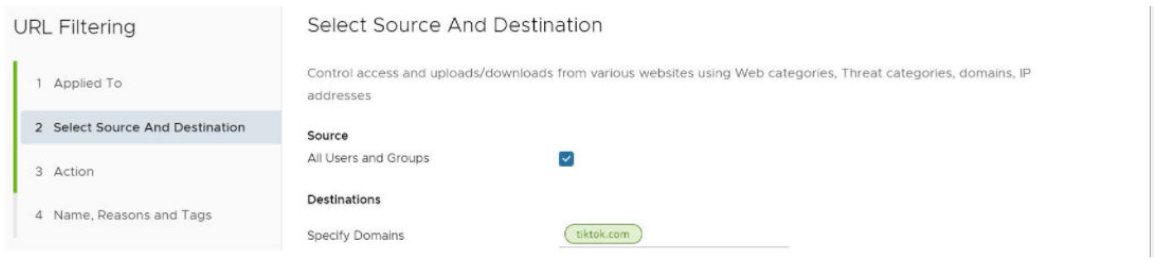
d Domain Option: The user selects the Domain option from the drop-down menu to configure domain(s), IP addresses, IP ranges, and CIDRs to be filtered per the rule. (See image below).



Note A user can specify multiple domains per rule by separating each domain with a comma.

Click the **Next** button.

The **Select Source and Destination** screen appears, as shown in the image below.



Follow the sub steps below to configure the Domain option.

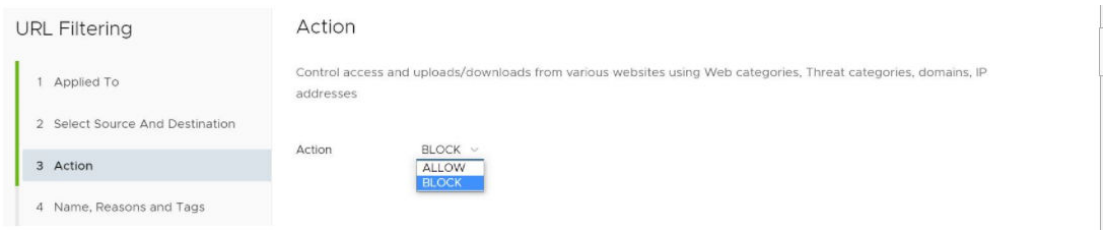
1 In the **Select Source and Destination** screen, under **Source**, check the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.

2 Click the **Next** button.

3 Under **Destinations**, enter the domains in the **Specify Domains** text field (e.g., google.com). A user specifies which domain(s) are to be filtered per the rule. A user can specify multiple domains per rule by separating each domain with a comma.

4 Click **Next**.

5 In the **URL Filtering Action** screen, specify if this rule exception is for blocking the traffic or allowing it, and then click the **Next** button.

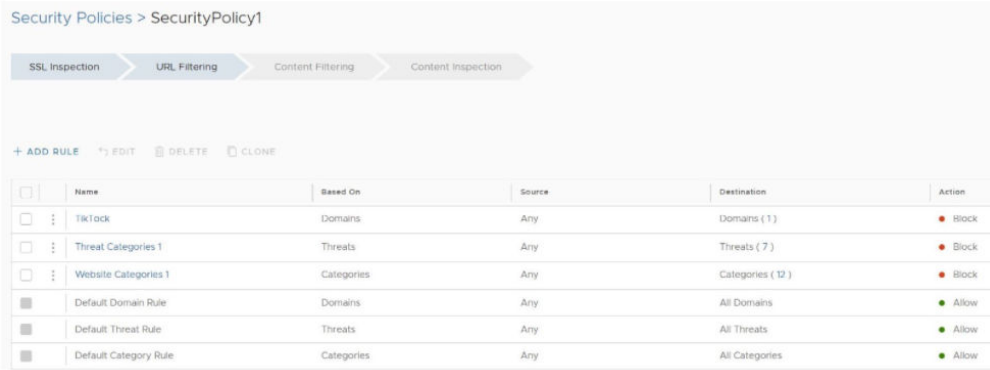


6 Click **Next**.

7 In the **Name, Reasons and Tags** screen, enter information in the following fields: Rule Name, Tags, Reason, and Position. NOTE: The Position field designates the rule's position on the list of URL filtering rules.

8 Click **Finish**.

9 After completing all the URL Filtering rules, a user may view the full list.

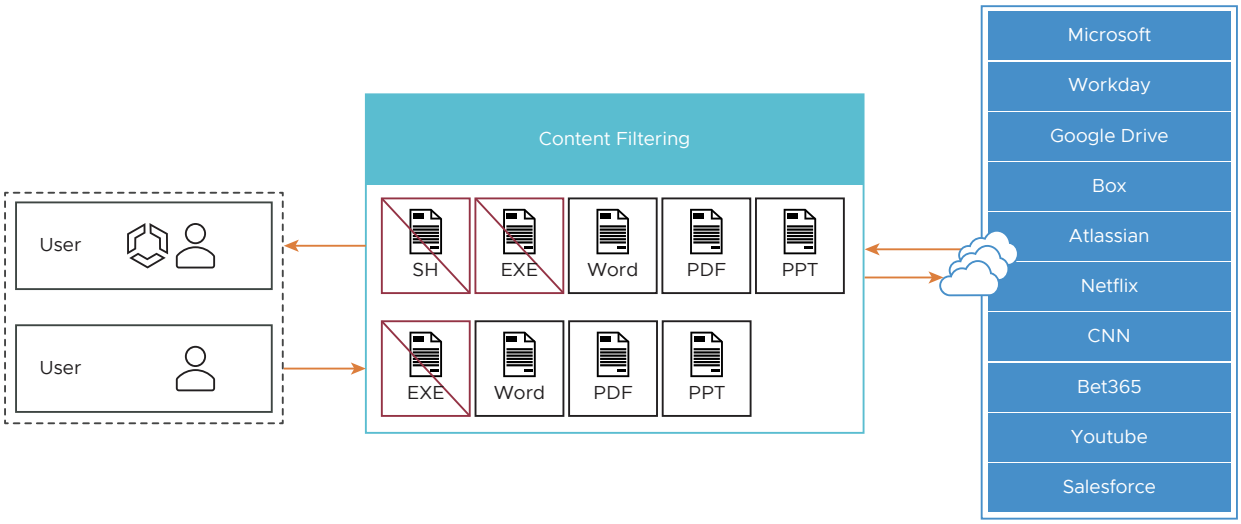


10 Click the **Finish** button and the rule will be posted on the URL Filtering list. The main **URL Filtering** screen appears.

11 The user has the following options: configure another URL Filtering rule, configure a different Security Policy category, or if finished, click the **Publish** button to publish the Security Policy.

12 After publishing the Security Policy, the user is ready to Applying a Security Policy

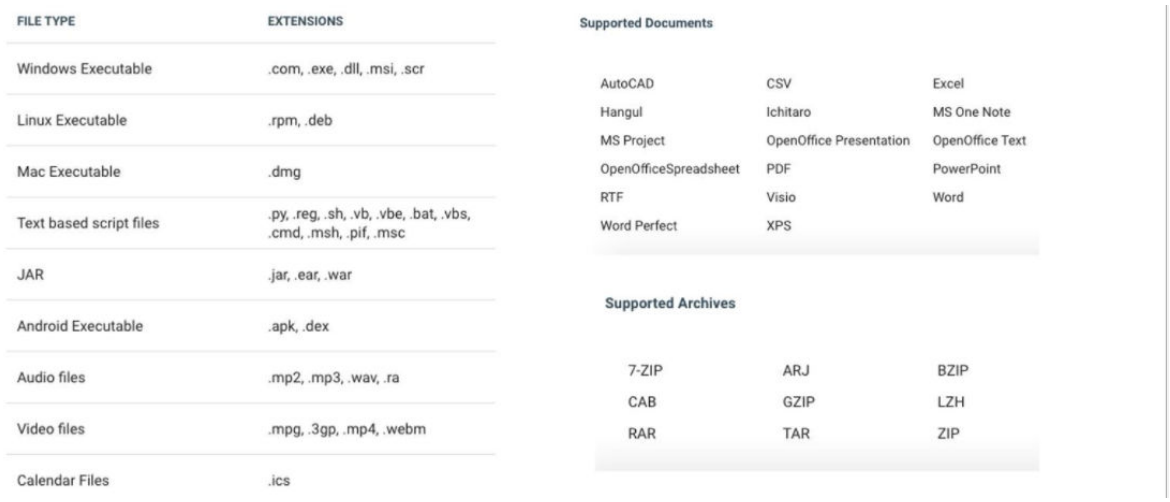
Content Filtering Category



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

The default rules for Content Filtering are:

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

To configure Content Filtering:

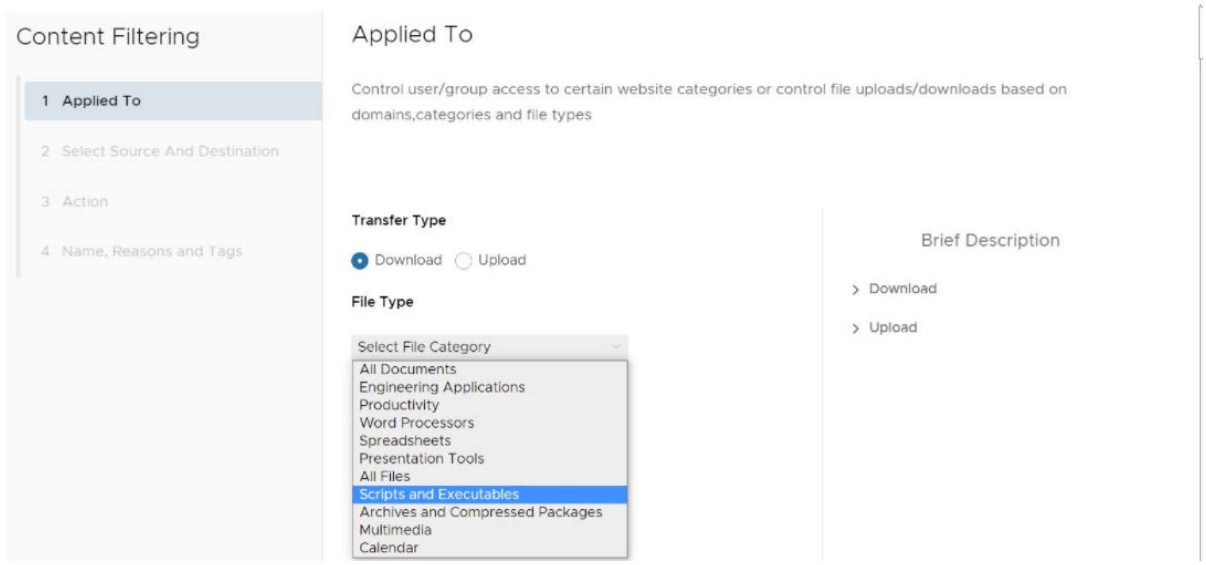
1 In the selected **Security Policy** screen, click the **Content Filtering** tab, located at the top of the screen.

2 Select **+ ADD RULE**.

The **Content Filtering Applied To** screen appears.

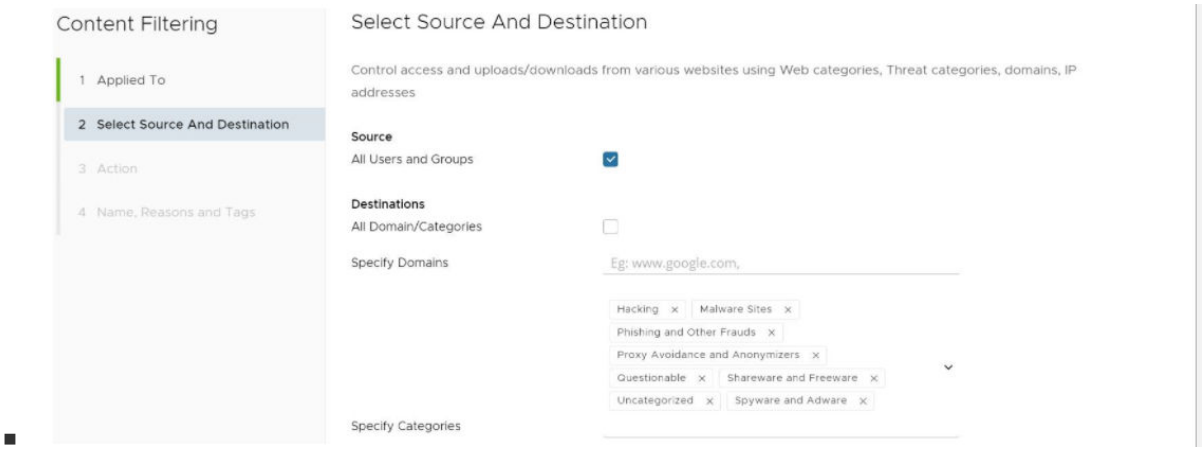
3 Under **Transfer Type**, choose either the **Download** or **Upload** radio dial. The user cannot select both options. If the user wants both a download and upload rule, two separate rules are required.

4 Under **File Type**, select a category from the drop-down menu, as shown in the image below.



5 Click **Next**.

The **Select Source and Destination** appears, as shown in the image below.



6 In the **Select Source and Destination** screen, under **Source**, a user can check 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.

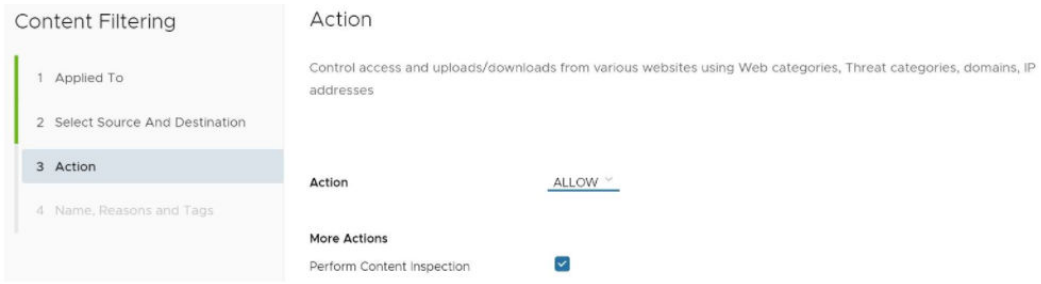
7 Under **Destinations**, a user can check the **All Domains/Categories** check box to apply the rule to all domains and categories, or deselect the check box to configure individual domains or specify web categories from a drop-down menu.

8 Click **Next**.

9 In the **Content Filtering Action** screen, choose **Block** or **Allow** from the drop-down menu to determine if the rule is for blocking URL's or allowing them, as described in the sub steps below.

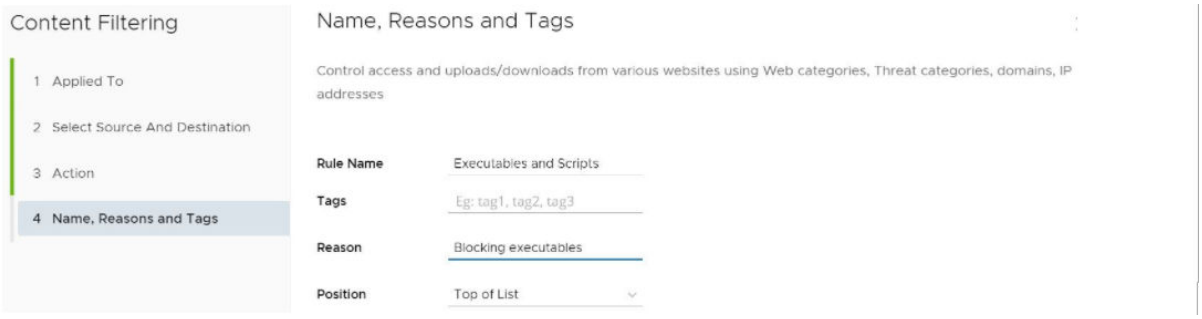
a If **Block** is chosen, then any of the specified file types with matching domain/categories would be blocked for the specified users/groups, as shown in the image below.

b If **Allow** is chosen, the content is allowed on the network.



c Click the **Next** button.

10 In the **Content Filtering Name, Reasons, and Tags** screen, enter information for the following text fields: Rule Name, Tags, and Reason. For the **Position** text field, indicate where the rule should be placed on the Content Filtering rule list.



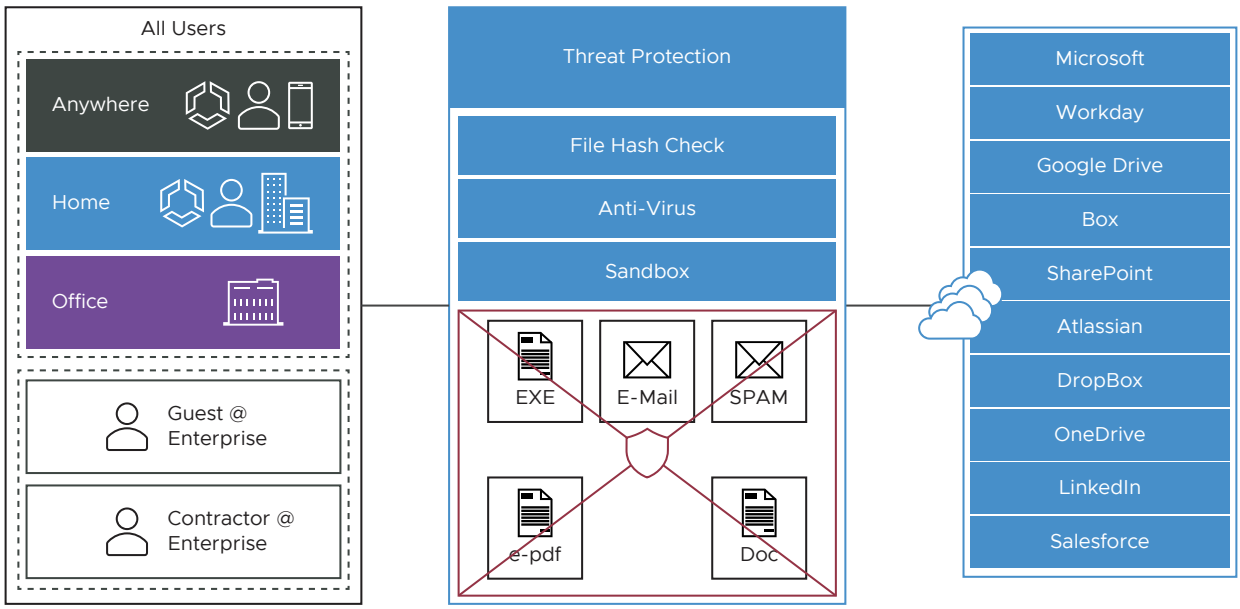
11 Click **Finish**.

The rule is now added to the Security Policy and the user can continue to the security feature.

12 The user has 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.

13 After publishing the Security Policy, the user is ready to Applying a Security Policy

Content Inspection Category



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

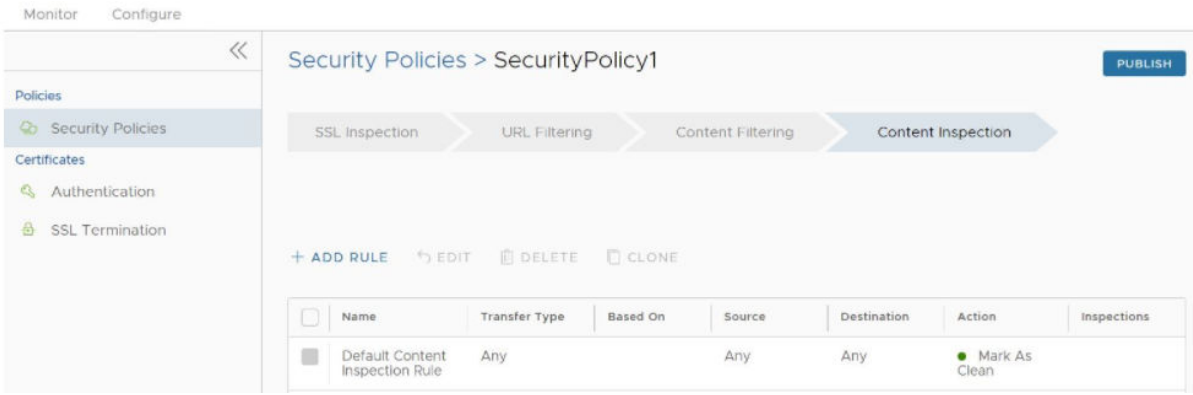
There are three options for Content Inspection:

- 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.
- 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.
- 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.

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

To configure Content Inspection:

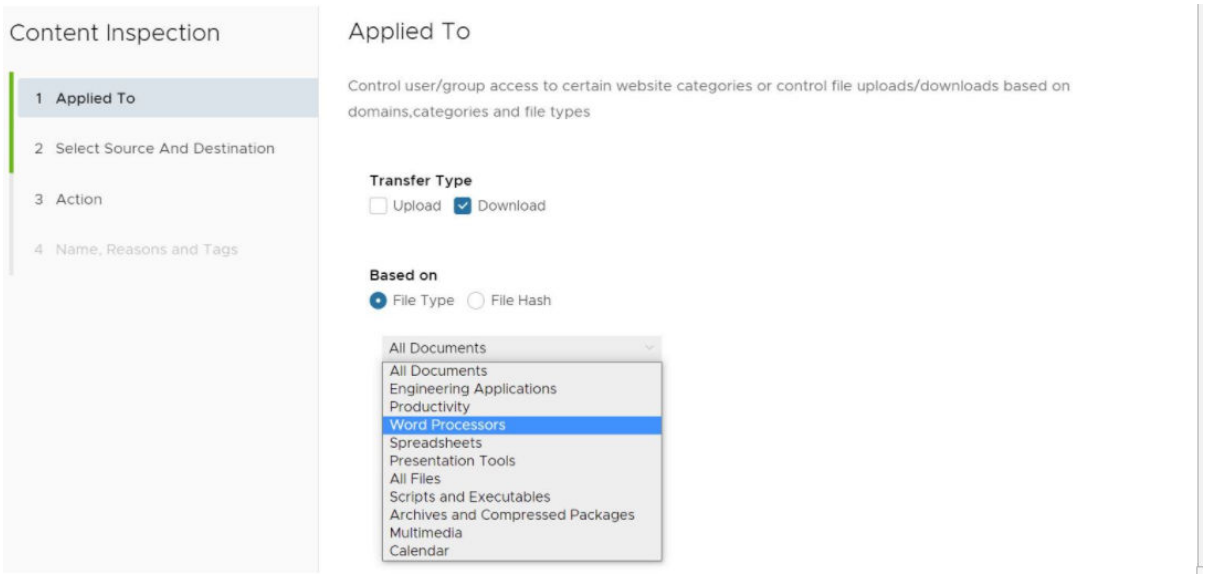
1 In the selected **Security Policies** screen, click the **Content Inspection** tab, located at the top of the screen, as shown in the image below.



2 Select **+ ADD RULE**.

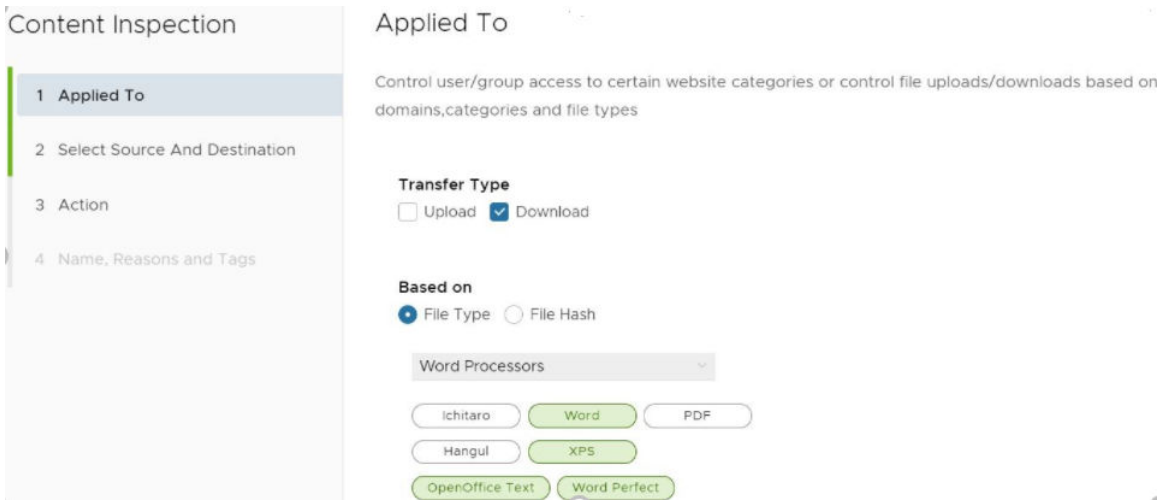
The **Applied To Content Inspection** screen appears.

3 Under **Transfer Type**, choose either the **Download** or **Upload** radio dial, or choose both types.



4 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. (A user cannot choose both).

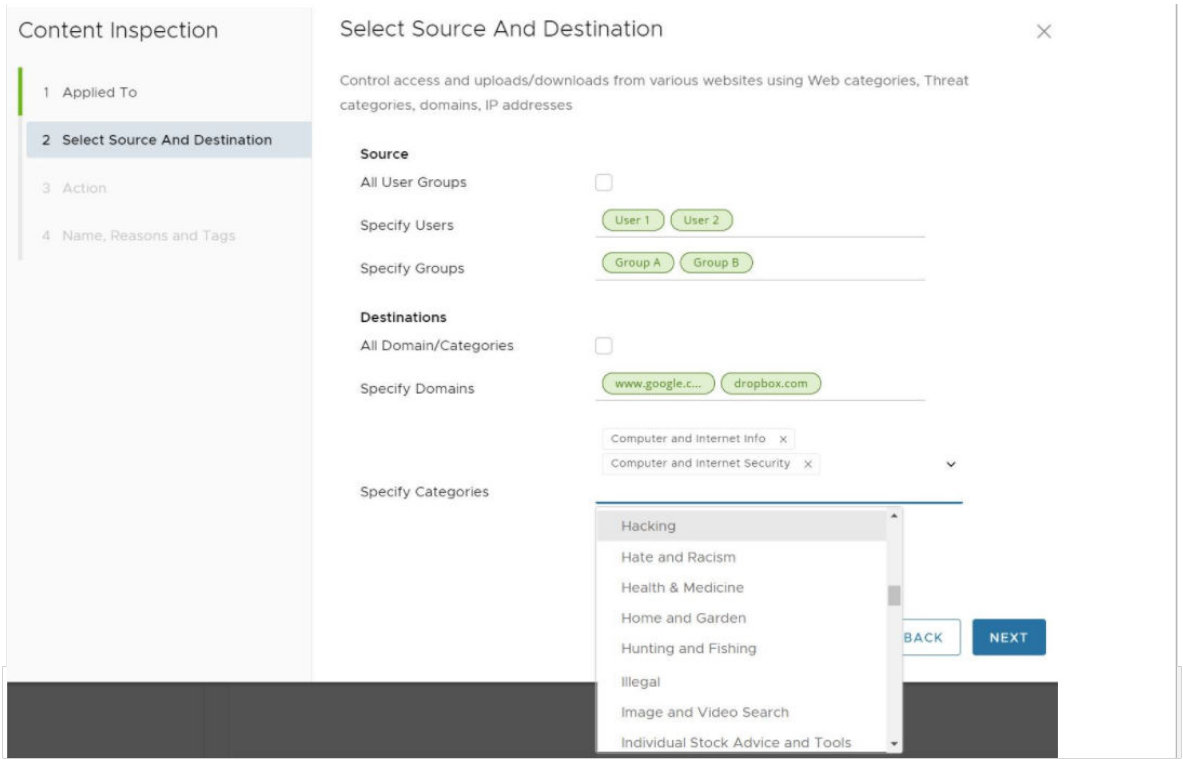
a If the user selects **File Type**, choose a category from the drop-down menu, as shown in the image above. For example, as shown in the image below, a user can configure a rule to inspect downloaded files that match the listed Word Processor file types: Word, XPS, OpenOffice Text, and Word Perfect.



b If a user selects **File Hash**, enter a SHA-256 hash in the appropriate text box.

5 Click the **Next** button.

The **Content Inspection Source and Destination** screen appears, as shown in the image below.



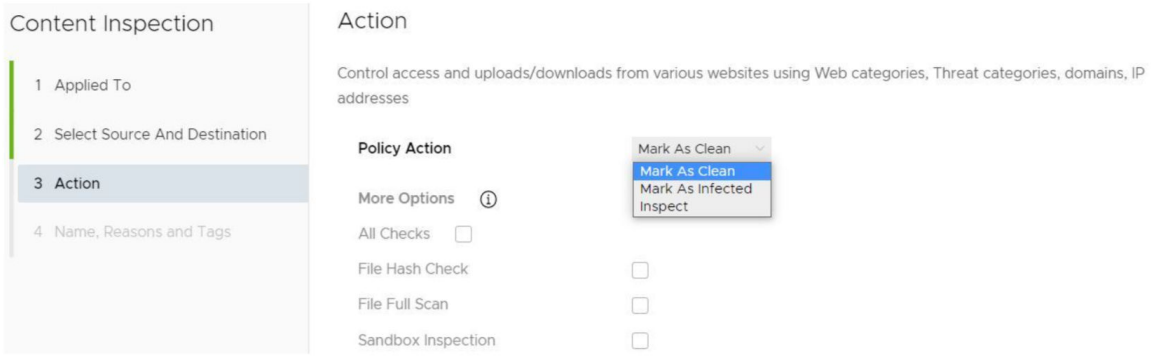
6 In the **Select Source and Destination** screen, under **Source**, a user can check the **All Users and Groups** check box to apply the rule to all users and groups, or deselect that check box to specify Users and Groups.

7 Under **Destinations**, enter the domains in the **Specify Domains** text field (e.g., google.com). A user specifies which domain(s) are to be filtered per the rule. A user can specify multiple domains per rule by separating each domain with a comma.

8 Click the **Next** button.

9 In the **Content Inspection Action** screen, choose an action from the **Policy Action** drop-down menu (Mark as Clean, Mark as Infected, or Inspect). See the table below for a description of these policy actions, and see the sub steps below for a description of each Policy Action.

a If the user chooses either the **Mark As Clean** or **Mark As Infected** policies, the Inspection Options (All Checks, File Hash Check, File Full Scan, Sandbox Inspection) are not available.



b If the user chooses the **Inspect** Policy Action, he or she can select up to three Inspection Options (All Checks, File Hash Check, File Full Scan, Sandbox Inspection). NOTE: The **All Checks** options means all three options are selected.

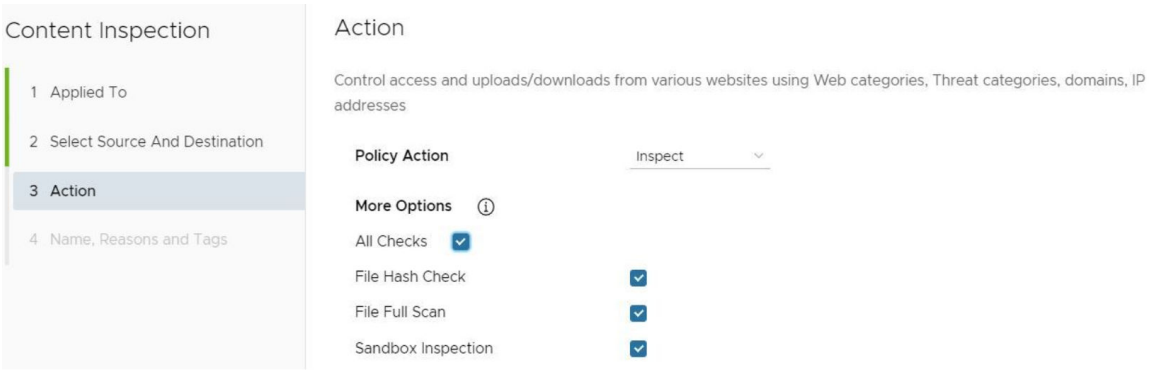
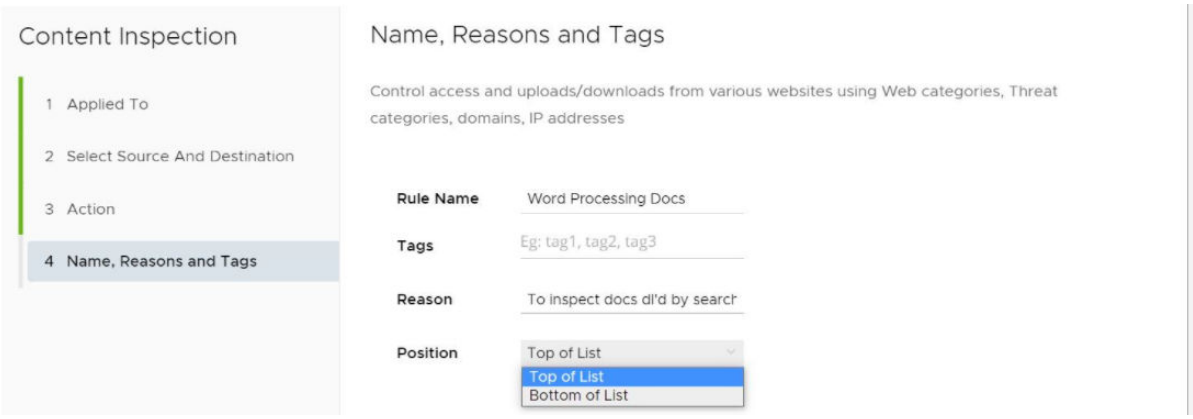


Table 1-1. Policy Action Description

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.

10 Click **Next**.

11 In the **Content Inspection Name, Reasons and Tags** screen, enter information for the following text fields: Rule Name, Tags, and Reason. For the **Position** text field, indicate where the rule should be placed on the Content Filtering rule list.



12 Click **Finish**.

The rule is now added to the Security Policy and the user can continue to the security feature.

13 The user has the following options: configure another rule under Content Inspection, configure a different Security Policy category, or if finished, click the **Publish** button to publish the Security Policy.

14 After publishing the Security Policy, the user is ready to Applying a Security Policy

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.

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.

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

Table of Contents

- **Applications**
  - Adobe
  - 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 assocated 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
```

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 you prefer to not include an exemption for every application covered in this document, you 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
```

Applying a Security Policy

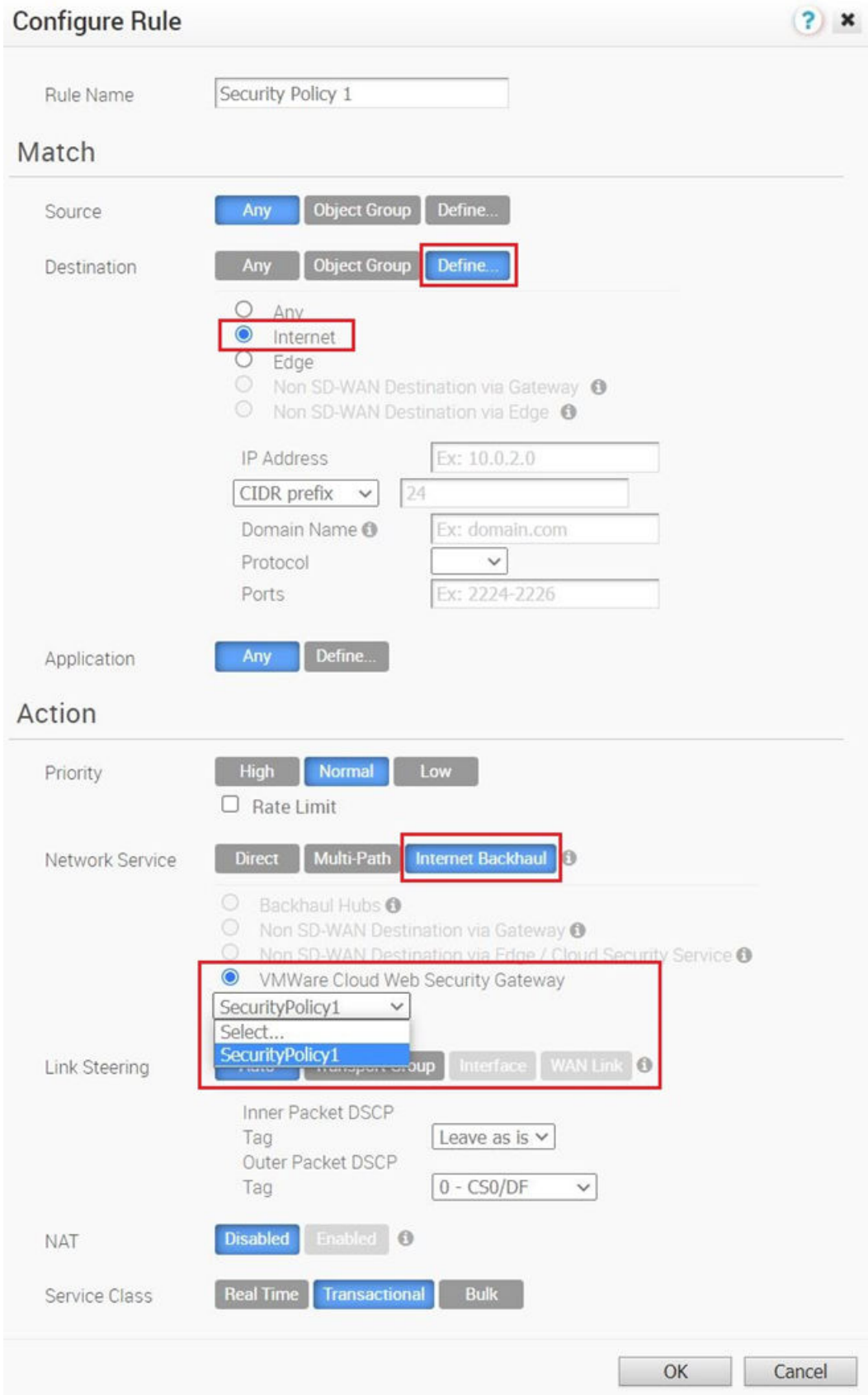
Once a Security Policy is configured and published, a user can then apply the Security Policy to a Profile or an Edge through the use of a Business Policy. Business Policies may be configured at either the Profile or Edge level.

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, go to **Configure** > **Profiles** > **Business Policy**.

2 Under **Business Policy** area, click **New Rule**. The **Configure Rule** dialog box appears.



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

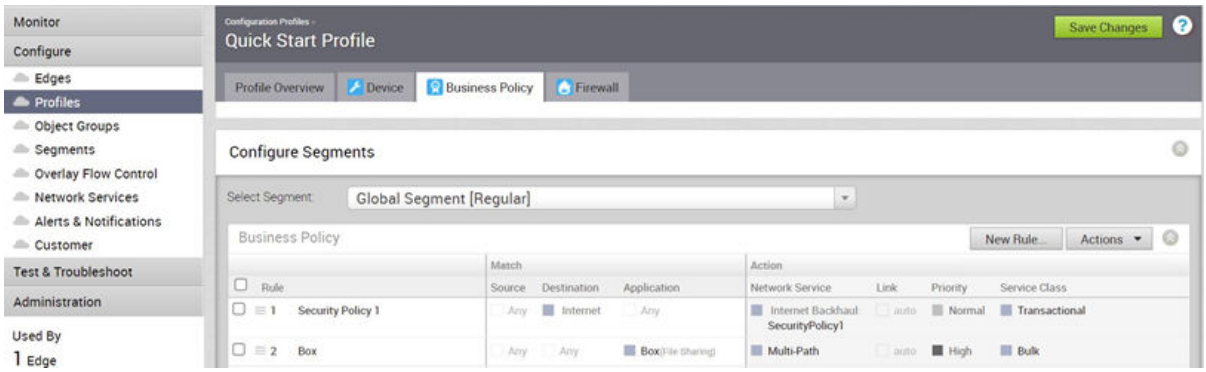
4 Under the **Match** area, configure the match conditions for the traffic flow by defining the matching criteria for the **Destination** traffic to **Internet**.

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

- Set the **Network Service** to **Internet Backhaul**. The **Internet Backhaul** network service is enabled only if the **Destination** is set as **Internet**.
- Click the **VMware Cloud Web Security Gateway** network service and select a published Security Policy to be applied to the Business policy rule.

6 Click **OK**. The selected Security Policy is applied for the selected profile and it appears under the **Business Policy** area of the **Profile Business Policy** page.

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



What to do next

- Monitoring Cloud Web Security

Monitoring Cloud Web Security

View the results of the configured Cloud Web Security policies for an enterprise from the **Monitor** tab in the **Cloud Web Security** page in the New Orchestrator UI portal.

Procedure

1 In the Orchestrator portal, click the **Open New Orchestrator UI** option available at the top of the Window.

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.

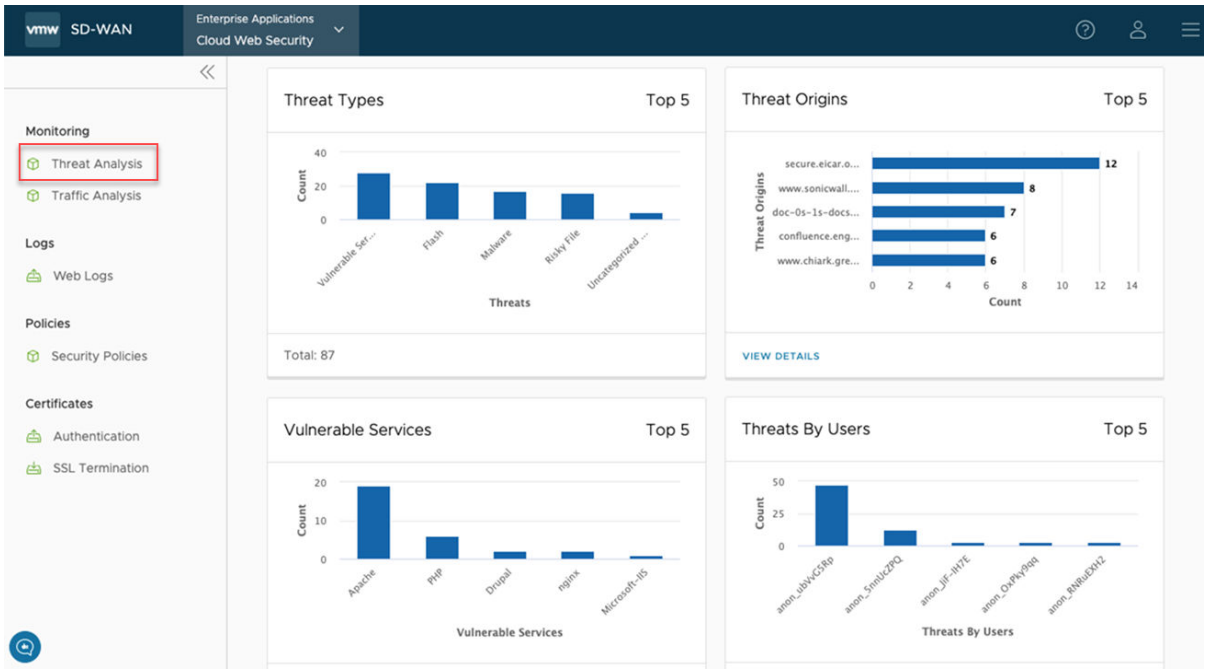
4 Click the **Monitor** tab.

Under the **Monitoring** section of Cloud Web Security, you can view the following three monitoring options:

- Threat Analysis
- Traffic Analysis
- Web Logs

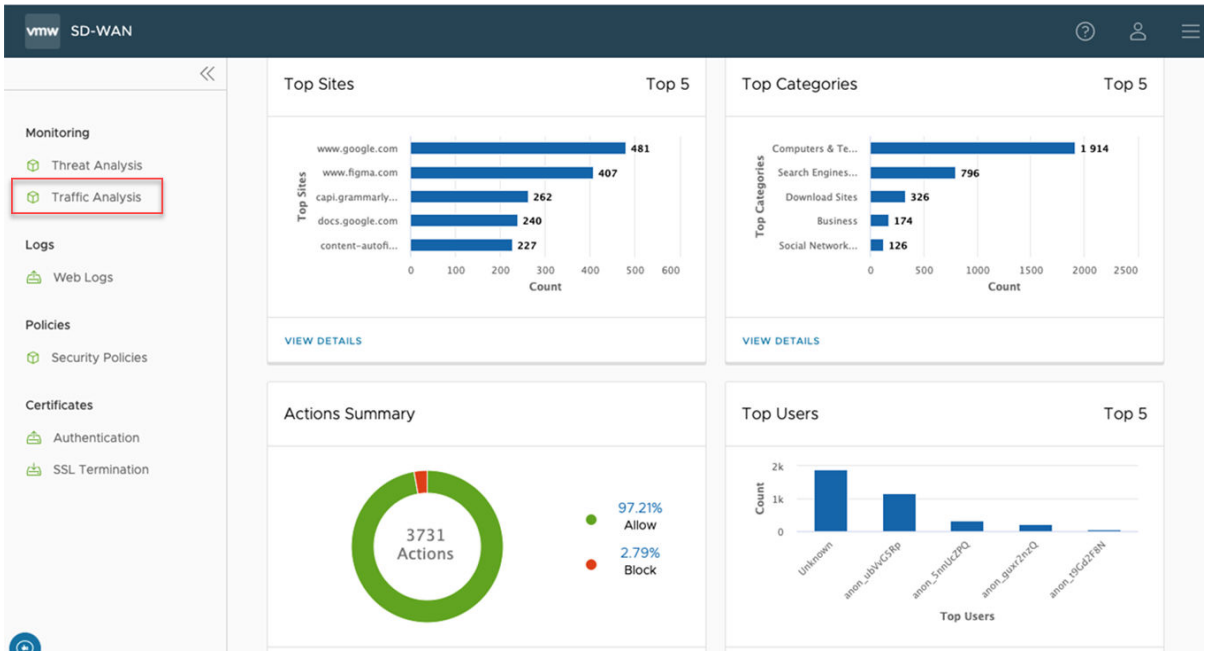
The **Threat Analysis** dashboard ensures that a user can get detailed visibility into threats. The dashboard displays:

- Threat Types
- Threat Origins
- Vulnerable Services
- Threats By Users



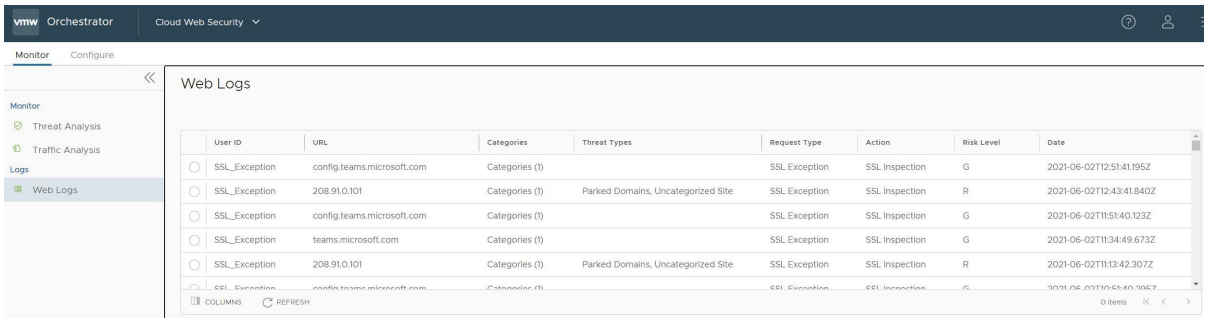
The **Traffic Analysis** dashboard ensures that a user can get detailed visibility into user traffic. The dashboard displays:

- Top Sites being visited by users
- Top Categories for traffic
- Actions Summary, the percentage of traffic being allowed/blocked
- Top Users

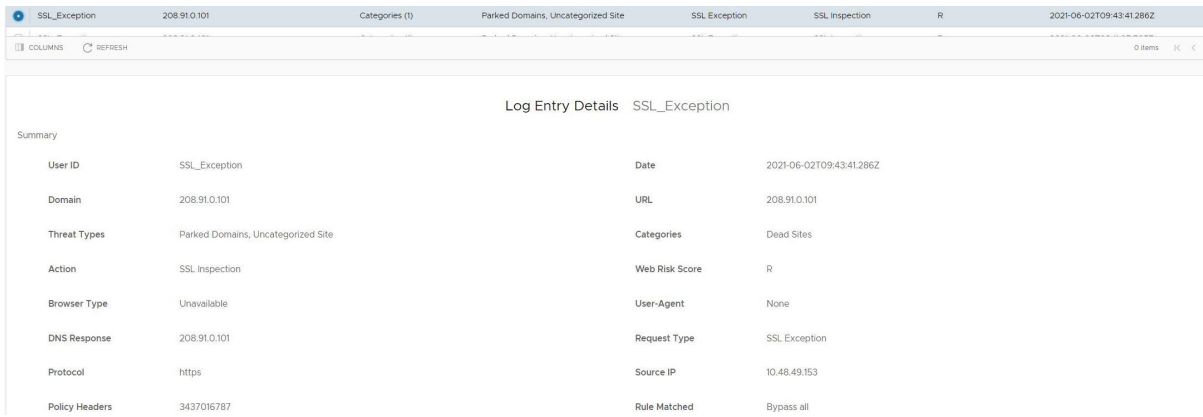


Web Logs

Cloud Web Security logs every session and threat. On the **Web Logs** page, a user may view a list of logs, scrolling through the full list.



Any log entry may be selected and a **Log Entry Details** screen will populate below the **Web Logs** list, giving granular detail on that particular log entry.



Single Sign-On Guides (SAML) 2

This chapter includes the following topics:

- 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 VMware Cloud Web Security. Doing so 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 SASE Orchestrator configuration.

Prerequisites

A user needs the following to configure an Azure Active Directory as an identity provider with VMware Cloud Web Security:

1 An Azure account

2 An Azure Active Directory (AD) tenant

> **Note** The process for creating an Azure AD tenant is documented here.

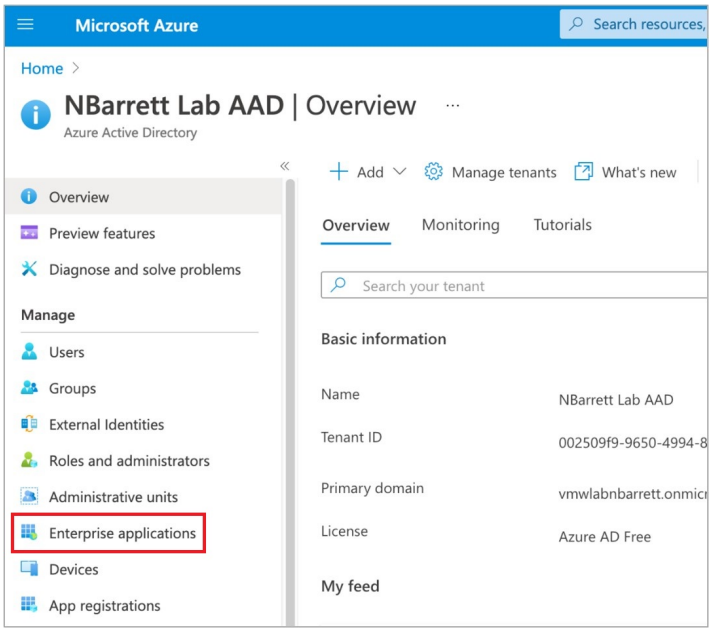
3 A customer enterprise on a production VMware SASE Orchestrator with Cloud Web Security Enabled. The Orchestrator must use Release 4.5.0 or later.

Azure Configuration

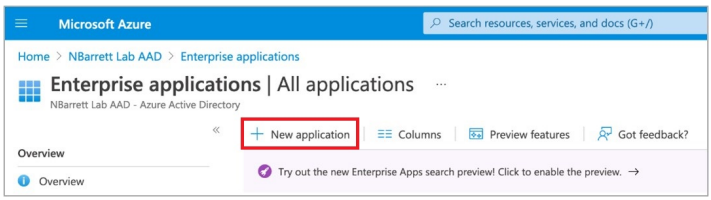
1 Log into the Azure portal https://portal.azure.com/ using either your Enterprise credentials or a local user to your Azure AD tenant.

2 Access the **Azure Active Directory** service by searching for active directory in the top search bar.

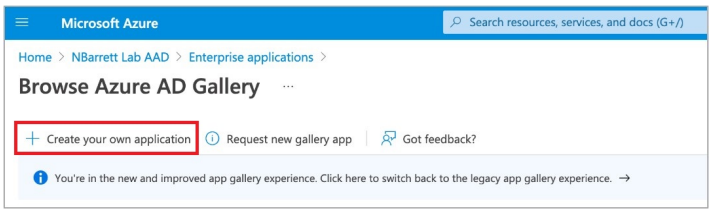
3 Click on **Enterprise Applications** in the left-hand side panel:



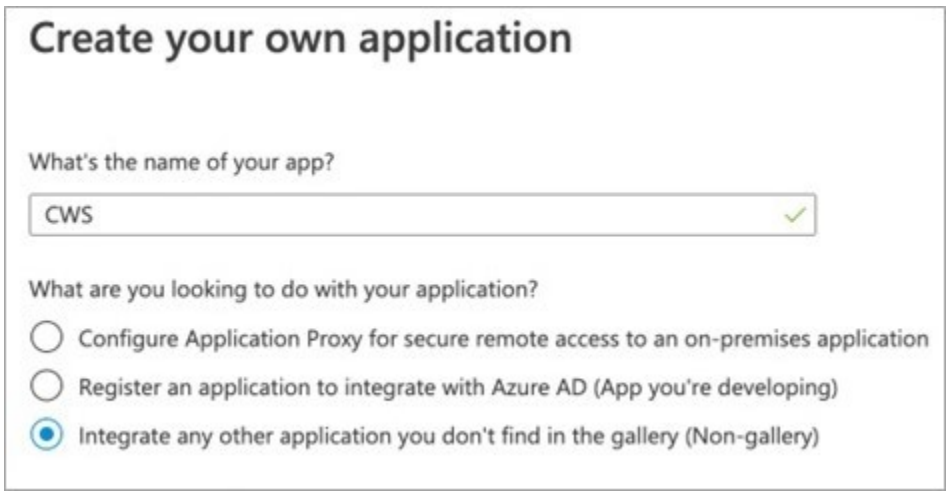
4 Click on **New application** at the top of the **Enterprise Applications** panel:



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

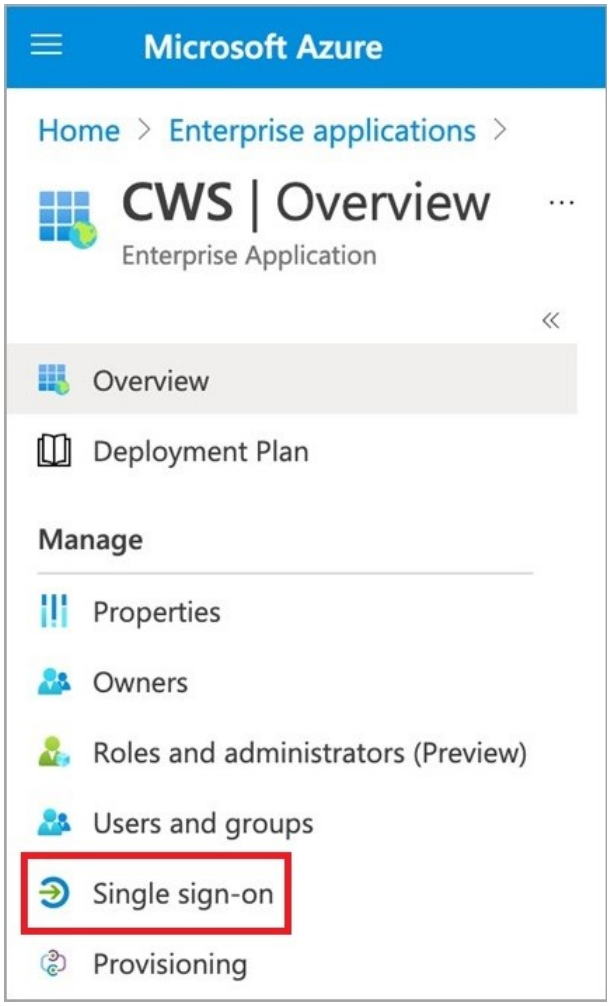


6 Enter a name (for example, Cloud Web Security, or CWS) and ensure that the **Non-gallery** radio option is selected.

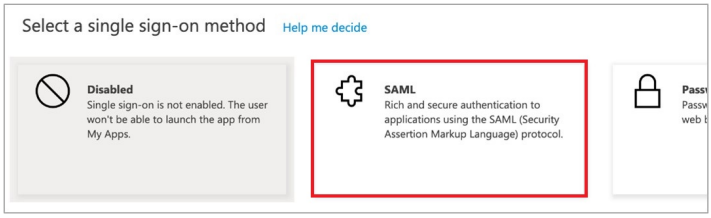


7 Click **Create** at the bottom of the **Create Your Own Application** form.

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.



10 Fill in section (1) using the upper-right edit pencil icon as show below. Once all the fields are filled in, click **Save** at the top of the pop-over pane.

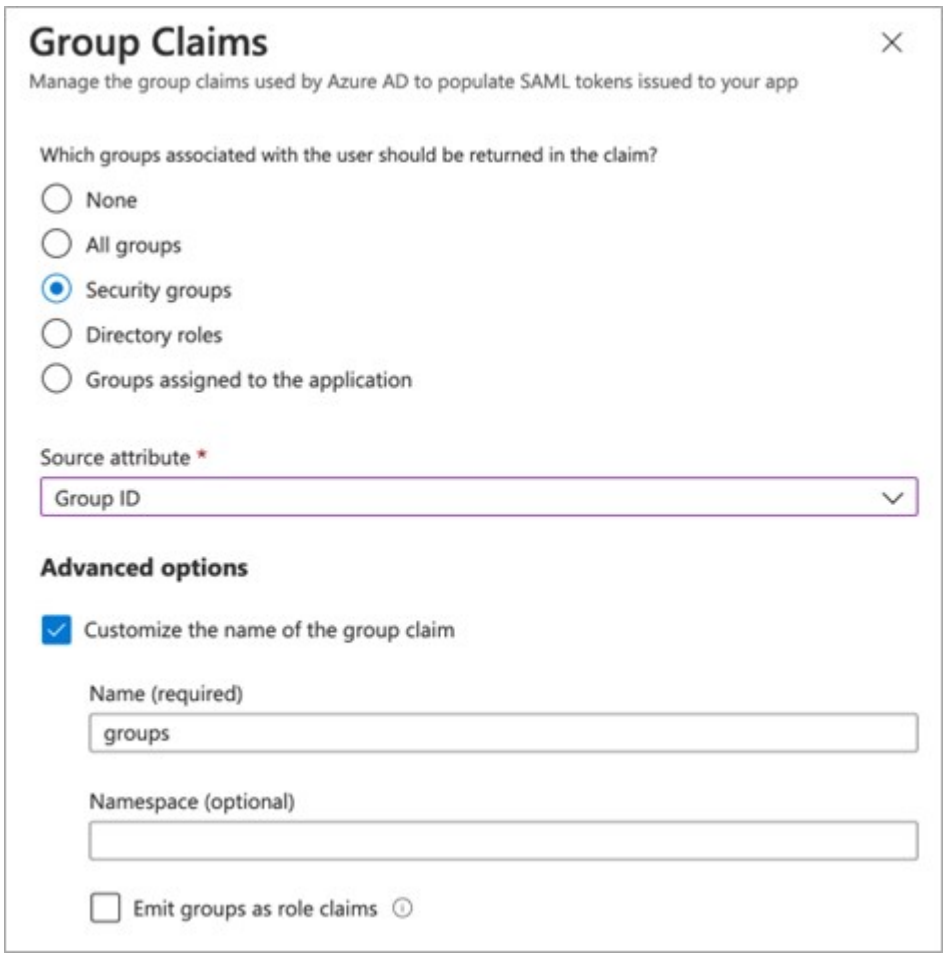
Field Name	Field Value	Field Description
Identifier (Entity ID)	https://safe-cws-sase.vmware.com/safeview-auth-server/saml/metadata	Azure AD allows multiple values. Set it to this value and select th **Default** checkbox for it. This is the Entity ID that Cloud Web Secu will present itself as in the SAML **AuthnRequest** 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 pa to. This is how Cloud Web Security learns that the user authentic 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). T 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 file 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 the user to lo to Azure AD (if they are not already logged in).

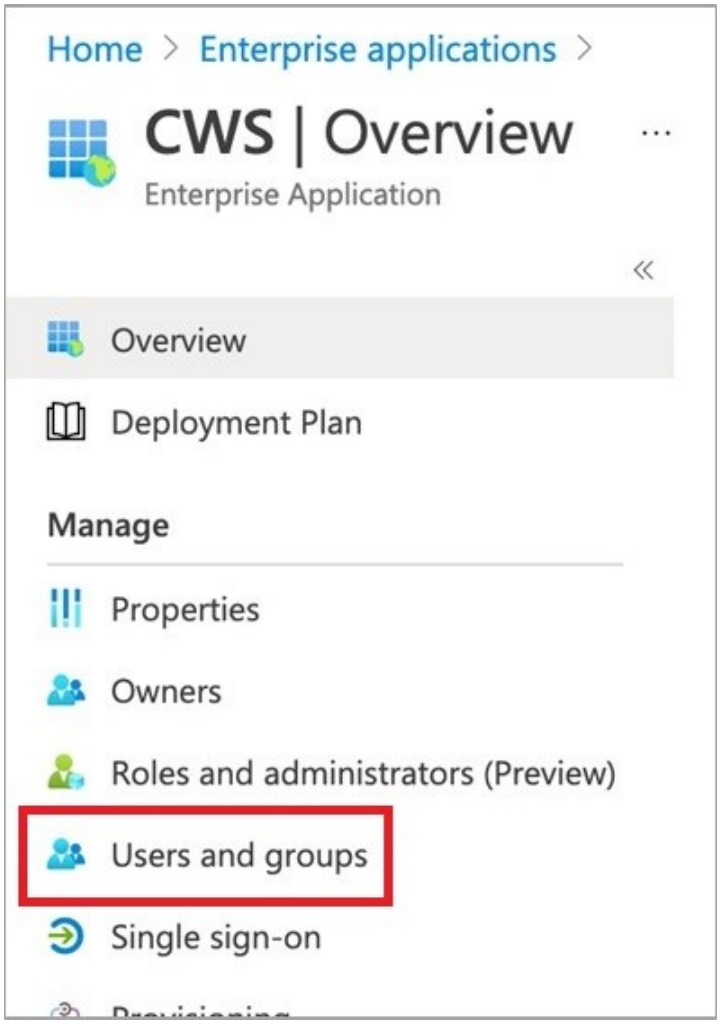
12 Click on the pencil icon in the upper-right corner of **User Attributes & Claims**.

13 Add a **Group Claim** using the following settings:

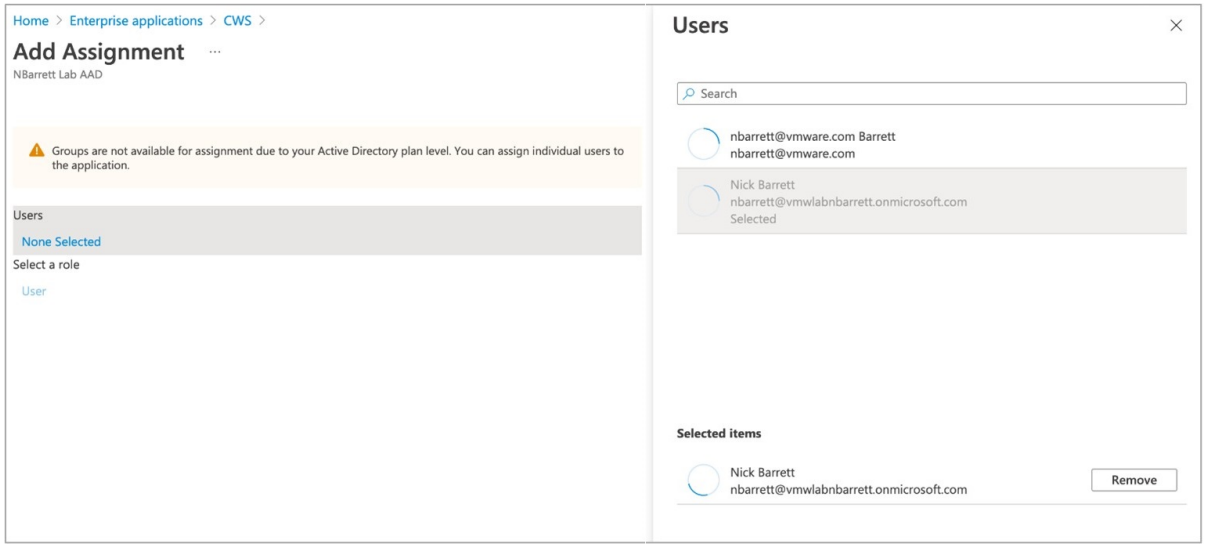


14 The Azure AD SAML configuration is now complete.

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**.



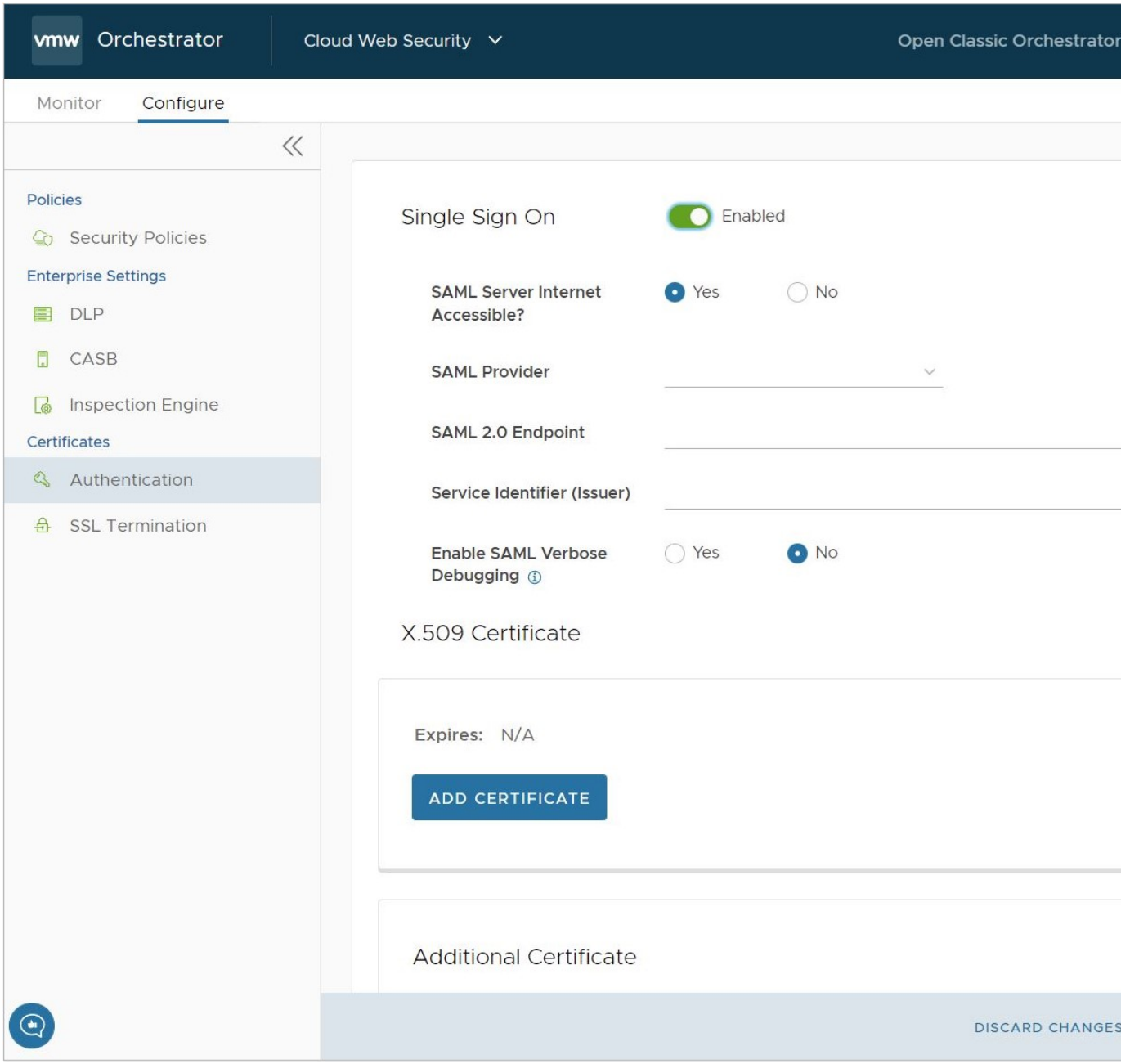
Note

- 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 you have an upgraded Azure Active Directory P1 or P2 tenant. The default AD plan level will only allow assigning individual users to the application.

VMware SASE Orchestrator Configuration

1 Log onto the Orchestrator UI and then open the New Orchestrator UI.

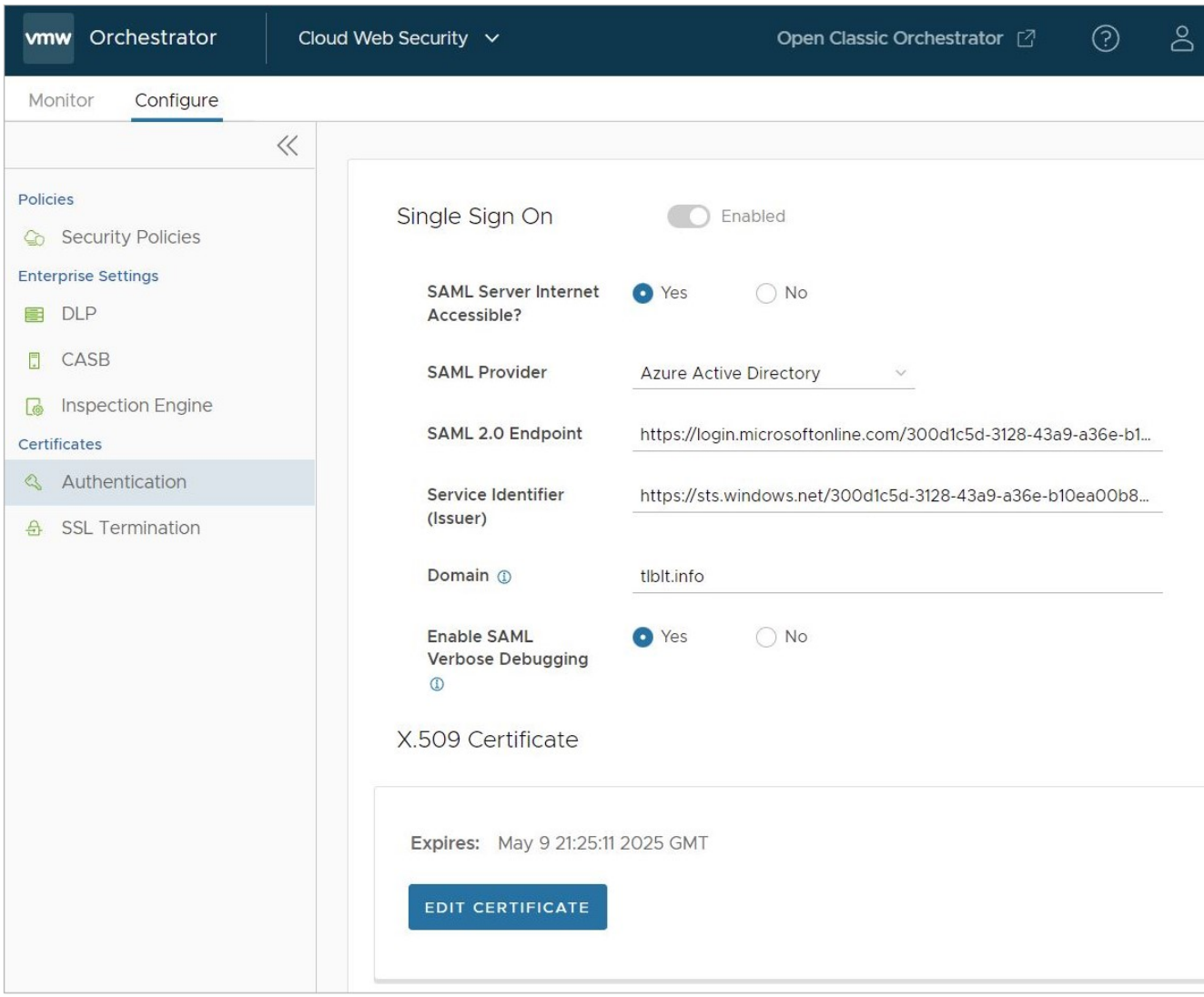
2 Go to **Cloud Web Security > Configure Authentication**. Toggle **Single Sign On** to **Enabled**.



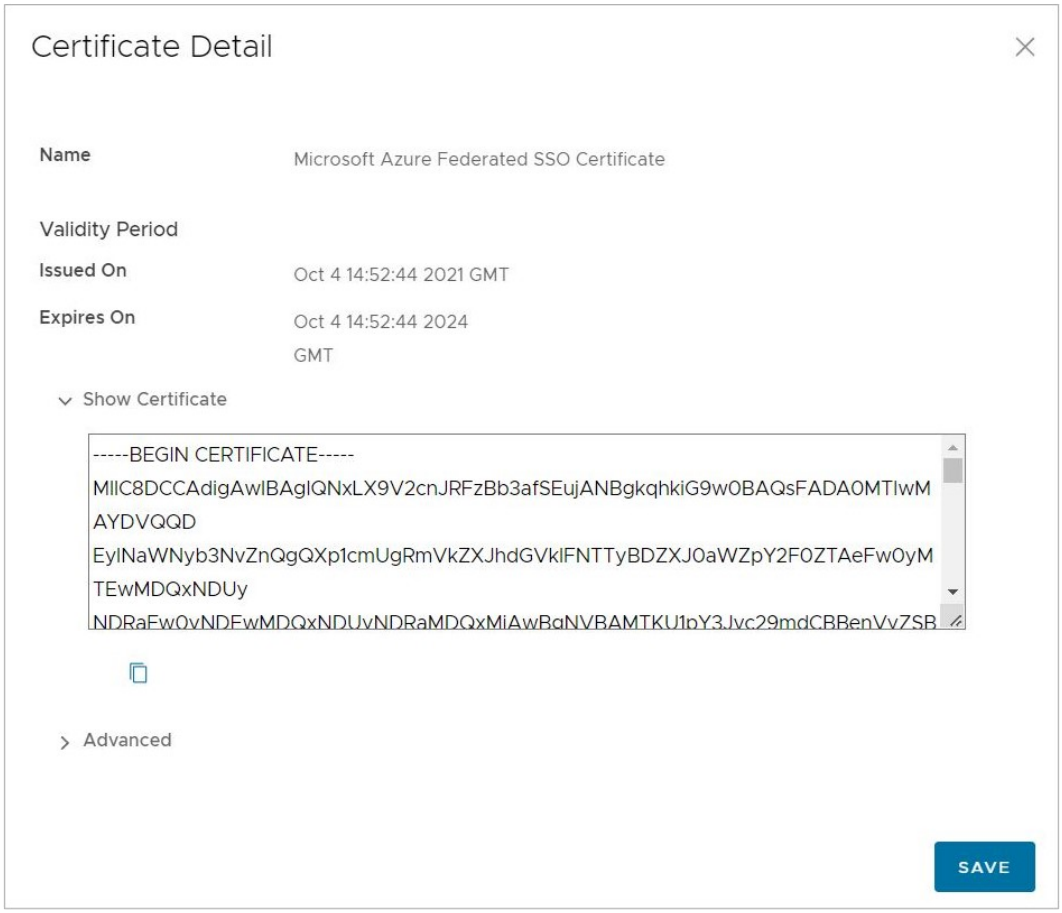
3 Configure the following:

- 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.

- Enable **SAML Verbose Debugging** if desired.
  - This turns on debugging messages for a period of 2 hours, after which the debugging is disabled automatically.
  - The SAML debug messages can be viewed in the Chrome Developer console.



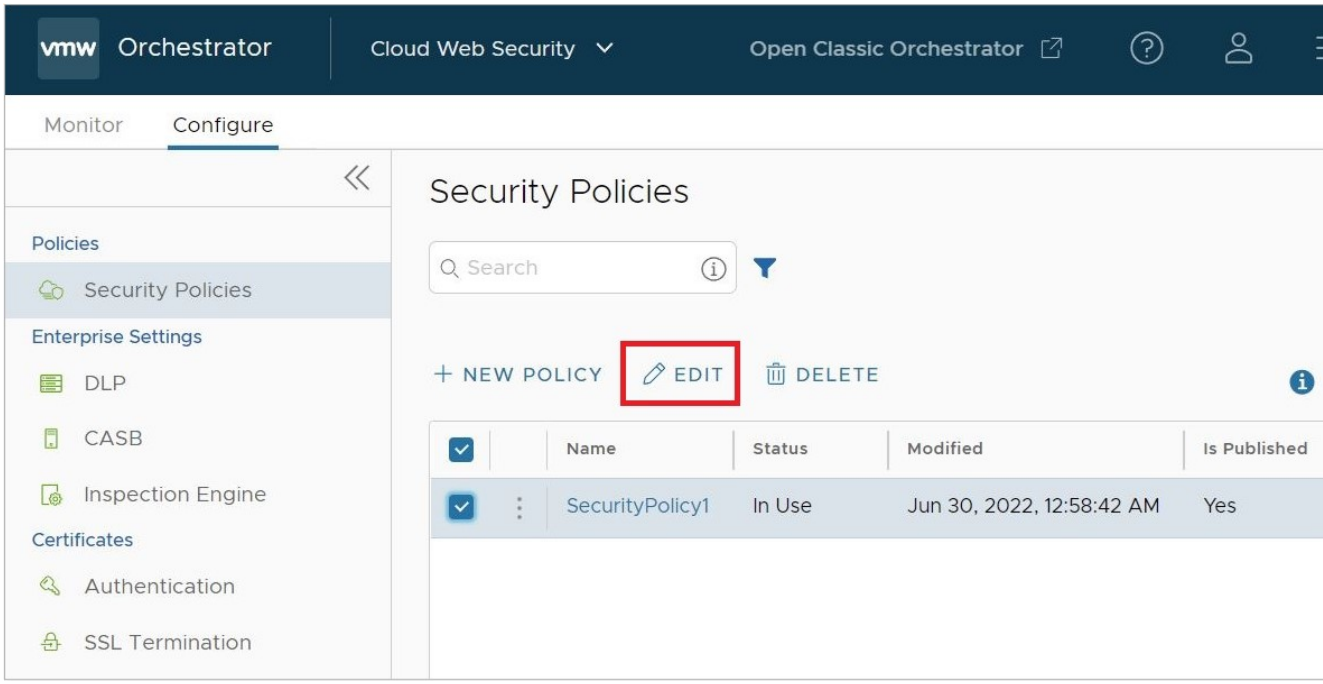
- X.509 Certificate, click on **Add Certificate** and copy the certificate from the notepad application as per step 11 of the Azure AD configuration and paste here, and then click **Save**.



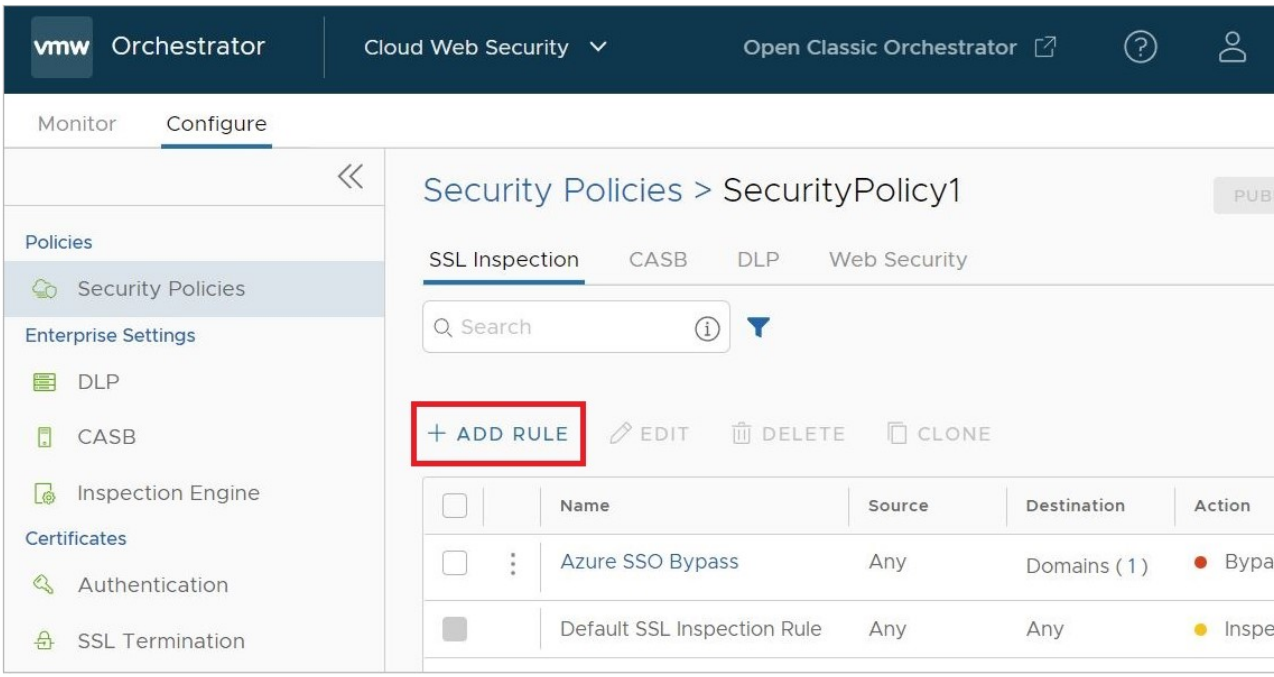
- Finally, click **Save Changes** to complete the configuration changes on the **Configure Authentication** screen.

4 Add a SSL Bypass rule for the Workspace ONE Access domain.

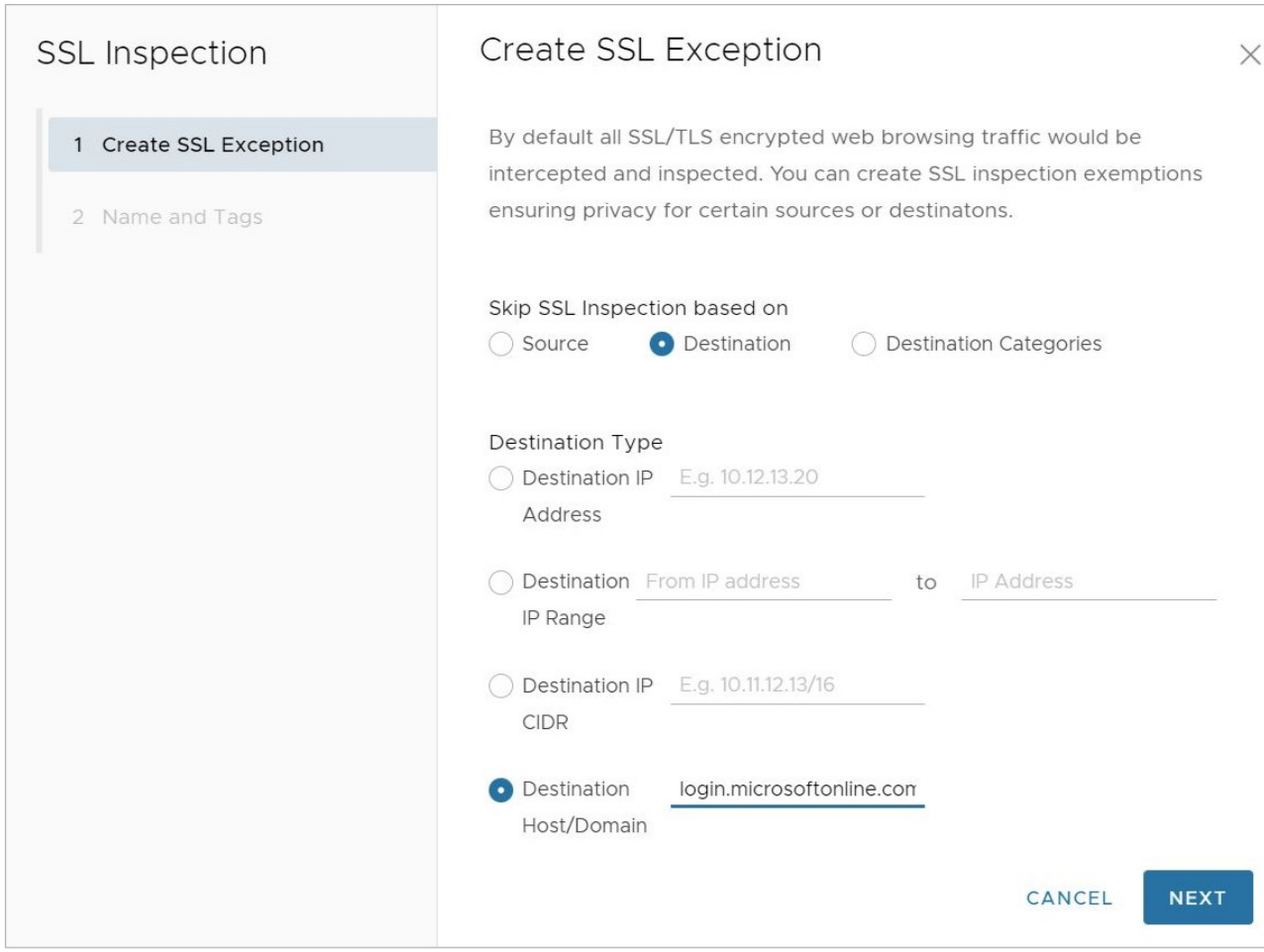
- Under Cloud Web Security, **Configure > Select Policy** for example, "SecurityPolicy1"
- Click on **Policy > Edit**



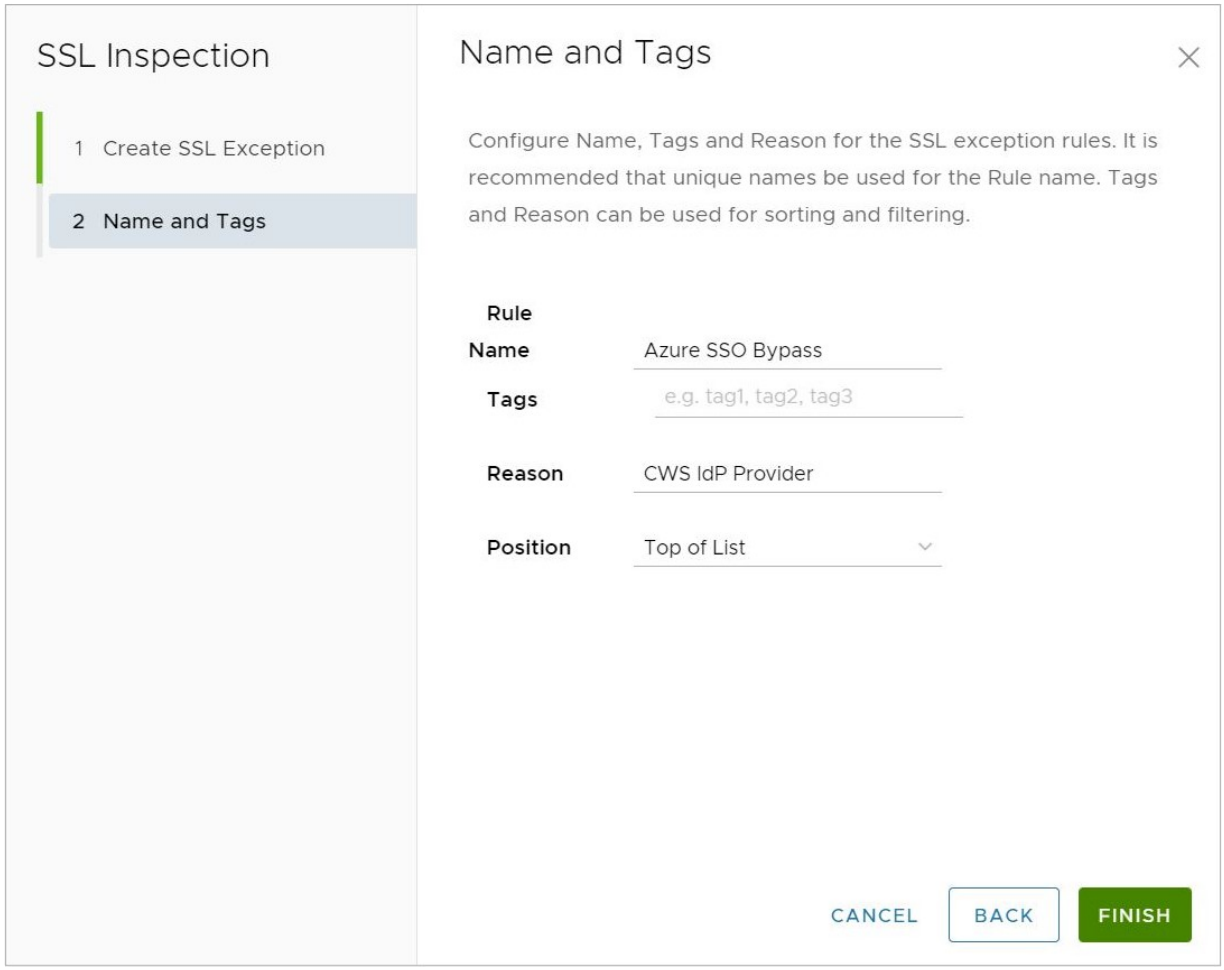
- On the **SSL Inspection** tab
  - Click**Add Rule**



  - For **Skip SSL Inspection based on**: select **Destination**.
  - For **Destination Type**, select **Destination Host/Domain**
  - Then specify the domain **login.microsoftonline.com**.



- On the **Name and Tags** screen, name the new rule and add a reason, if desired. Click **Finish**, and then **Publish** the applicable Security Policy to apply this new rule.

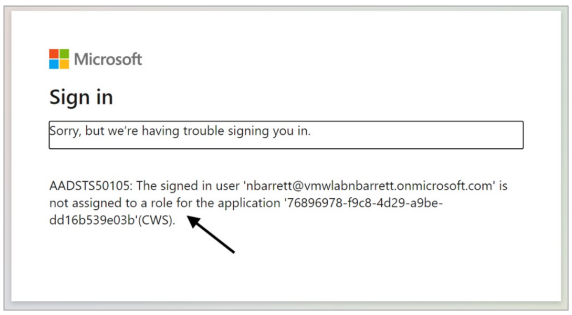
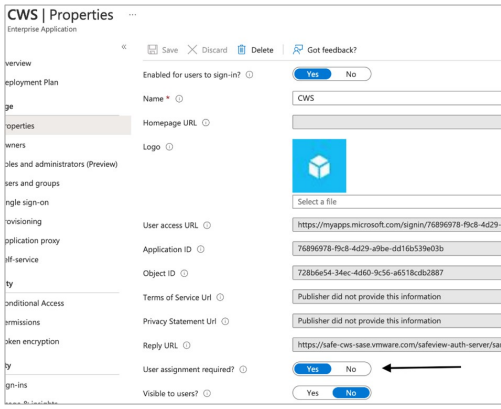


Note The domain **login.microsoftonline.com** is part of the **Microsoft 365** group of domains as found in the document: Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended. If you have already configured an SSL Bypass rule which includes the full **Microsoft 365** domain group, you can skip this step. If you 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: 	■ Ensure that all users are assigned to the CWS ent ■ Requiring user assignment can be disabled in the Azure AD. ■ They can also be in a group that is assigned to the has appropriate licensing. ■ https://docs.microsoft.com/en-us/azure/active-d access-portal 

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 SASE Orchestrator configuration.

Prerequisites

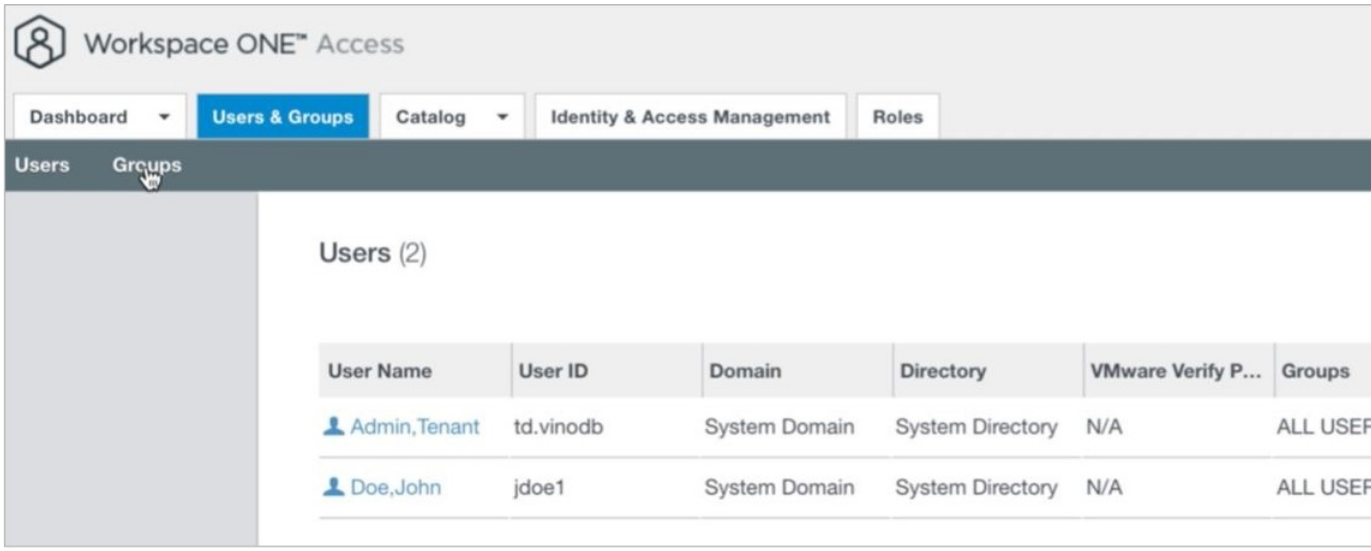
A user needs the following to configure Workspace ONE as an identity provider with VMware Cloud Web Security:

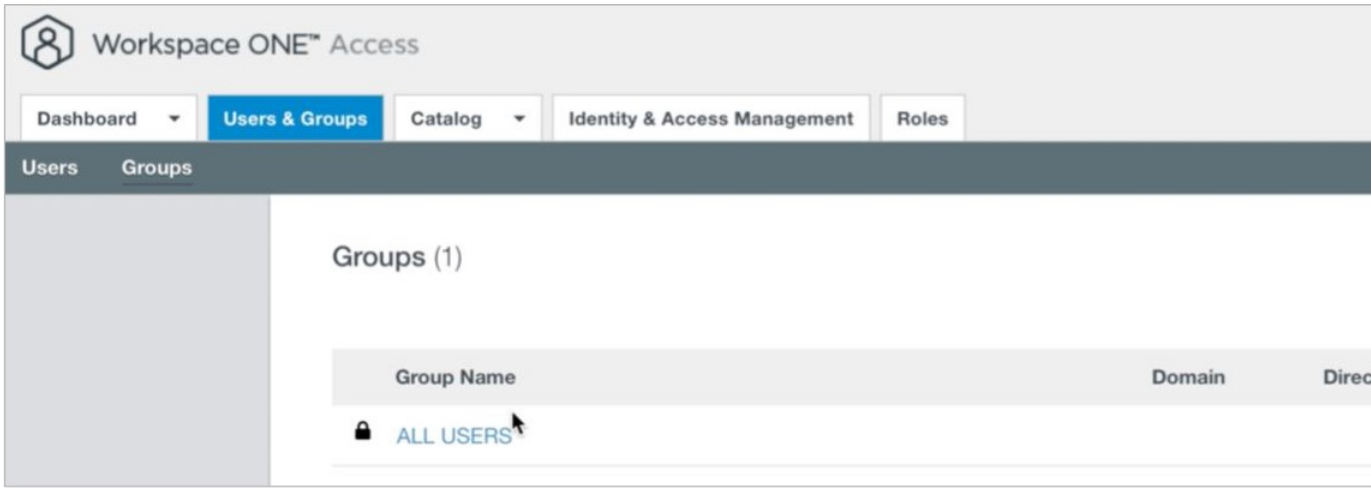
1 A Workspace ONE account.

2 A customer enterprise on a production VMware SASE Orchestrator with Cloud Web Security Enabled. 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.

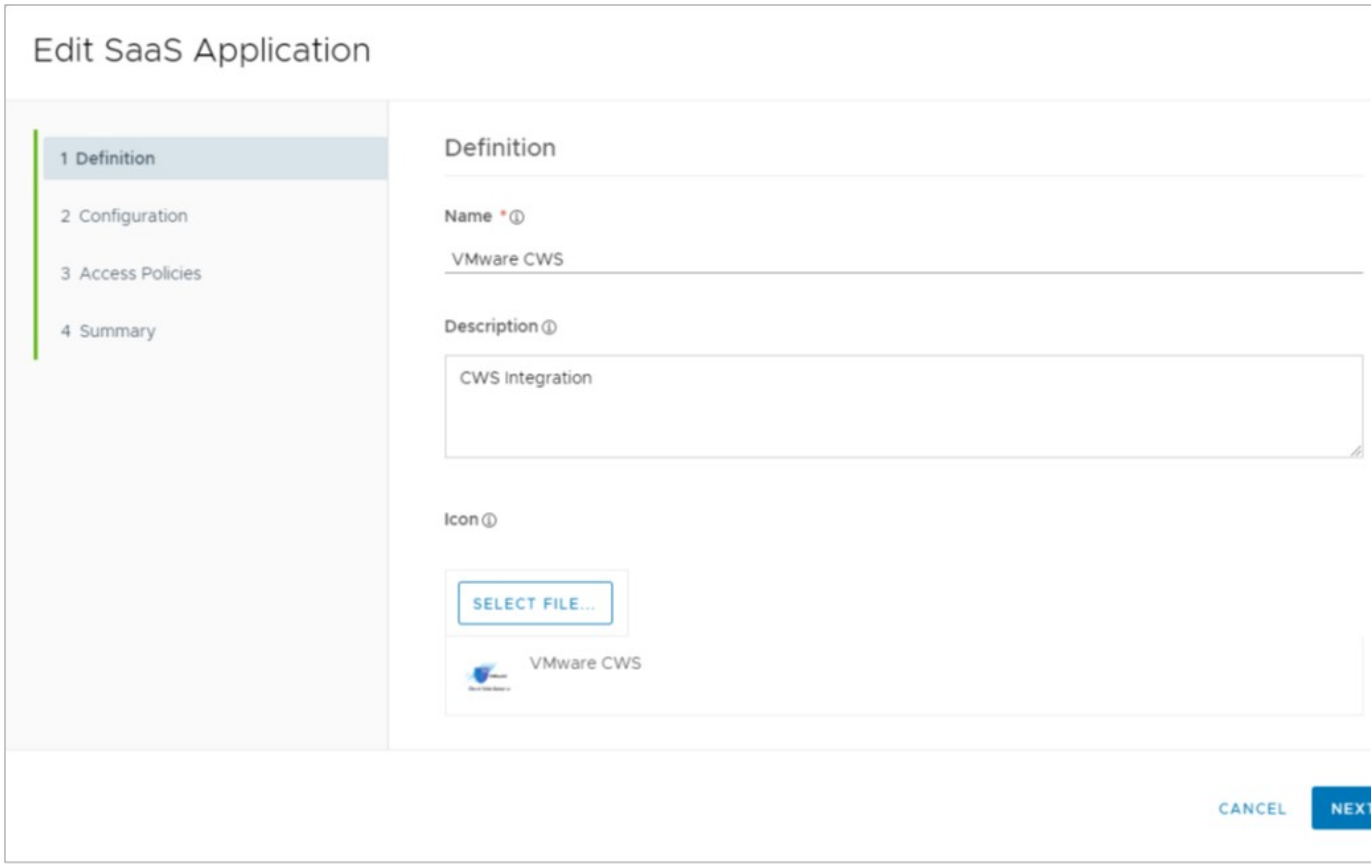




2 Go to **Catalog > Web Apps** .

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

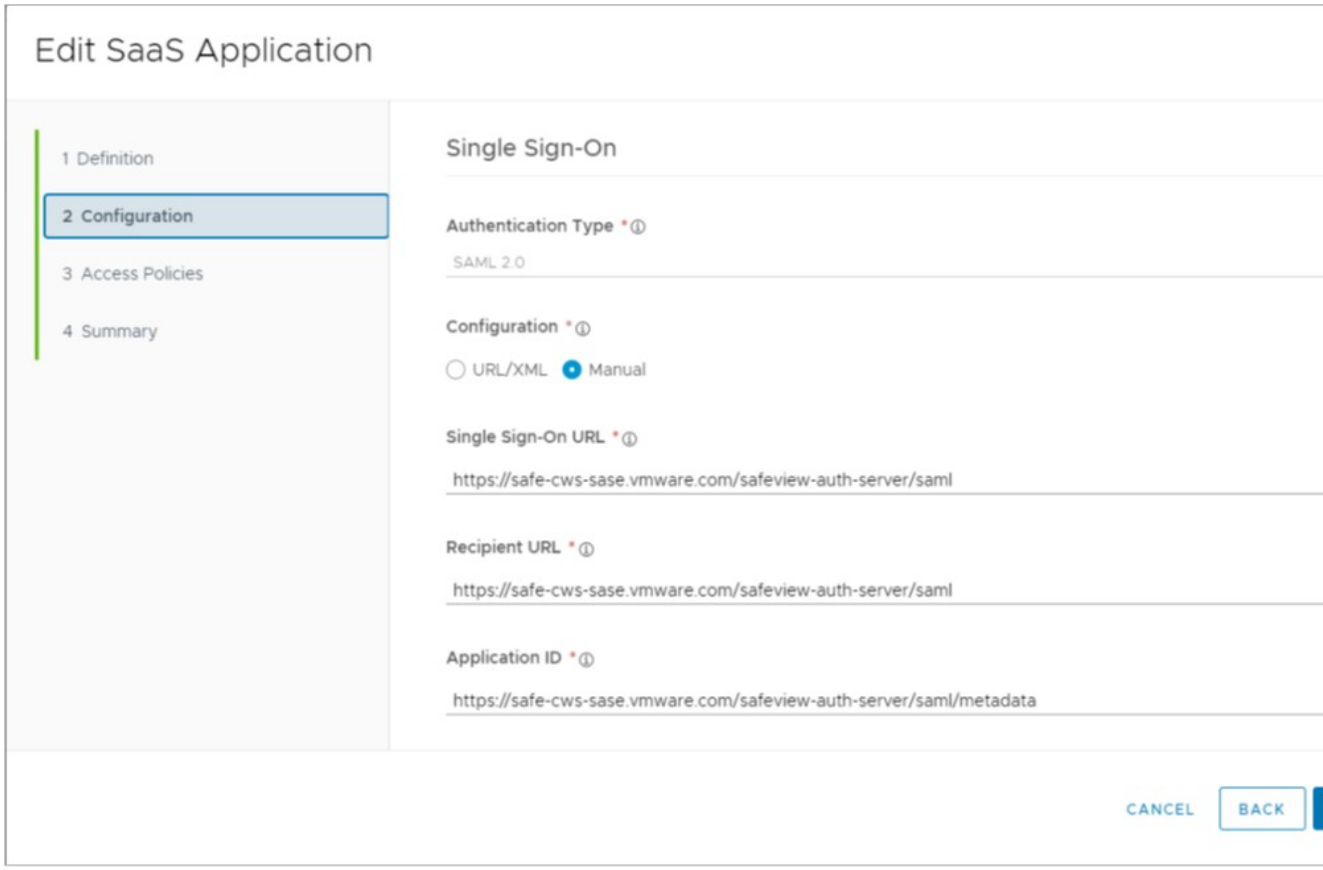
4 Name the Application as VMware CWS and click **Next**.

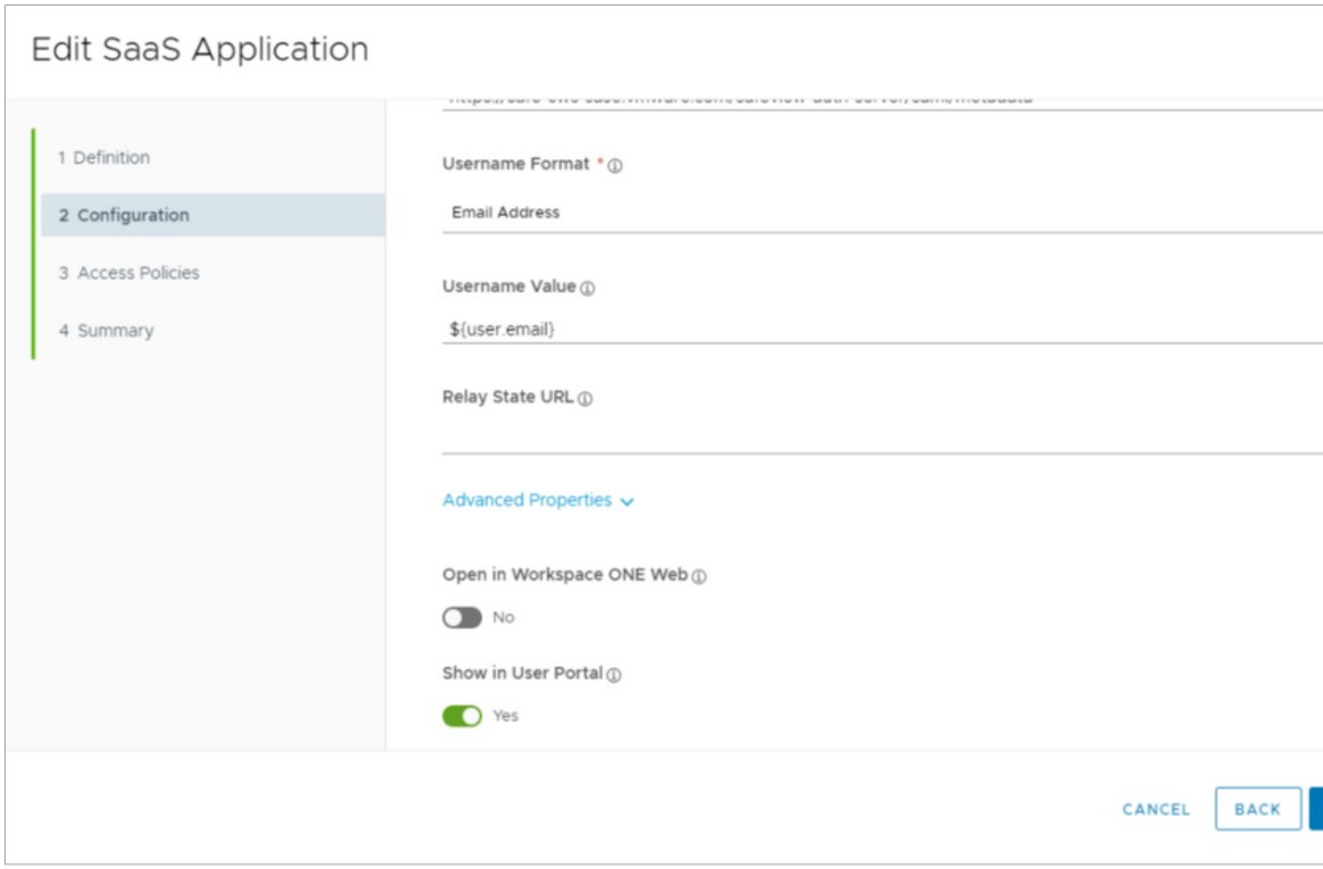


5 On the **Configuration** section:

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-authserver/saml
- Recipient URL: https://safe-cws-sase.vmware.com/safeview-auth-server/saml
- Application ID: https://safe-cws-sase.vmware.com/safeview-authserver/saml/metadata
- Username Format: Email Address (name@domain.com)
- Username Value: ${user.email}

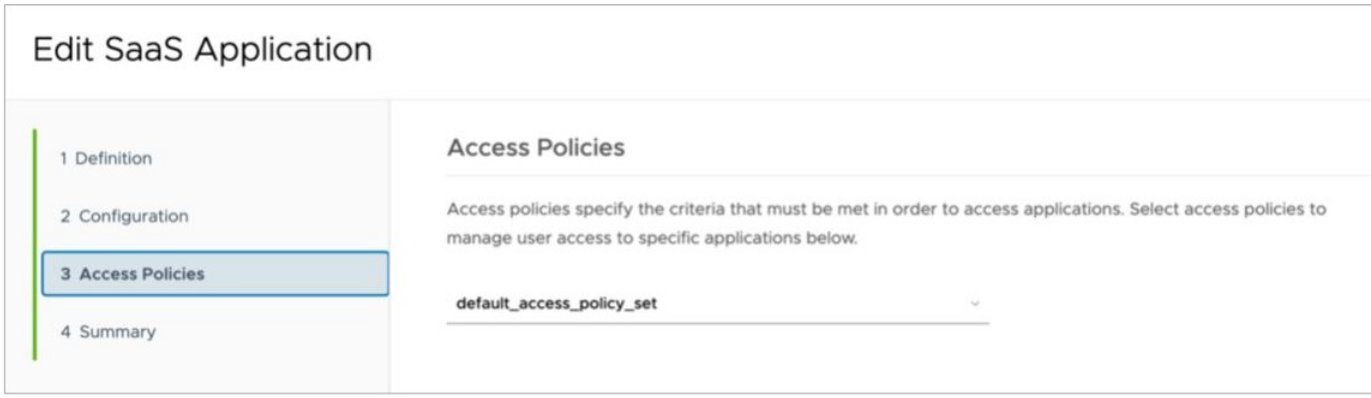

Edit SaaS Application
1 Definition
2 Configuration
3 Access Policies
4 Summary
Single Sign-On
Authentication Type *
SAML 2.0
Configuration *
URL/XML
Manual
Single Sign-On URL *
https://safe-cws-sase.vmware.com/safeview-auth-server/saml
Recipient URL *
https://safe-cws-sase.vmware.com/safeview-auth-server/saml
Application ID *
https://safe-cws-sase.vmware.com/safeview-auth-server/saml/metadata
CANCEL
BACK



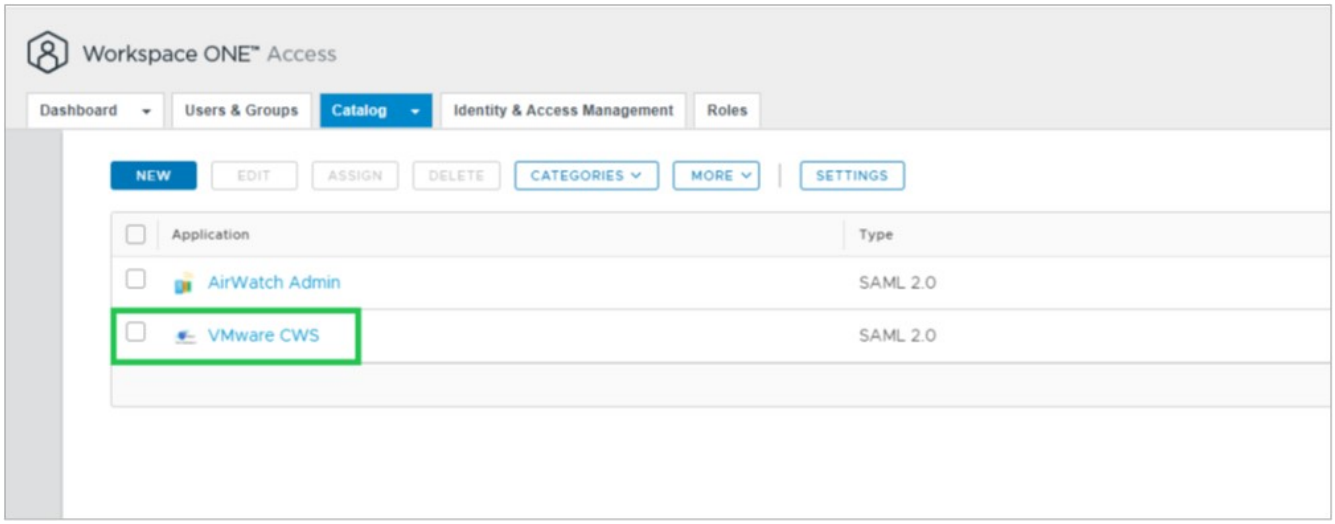
b Click on **Advanced Properties** and Add a **Customer Attribute Marking** as below. This configuration is to send groups attribute in SAML assertion. Note: the Name must be "groups" and the Value is ${groupNames}.

c Click **Next**.

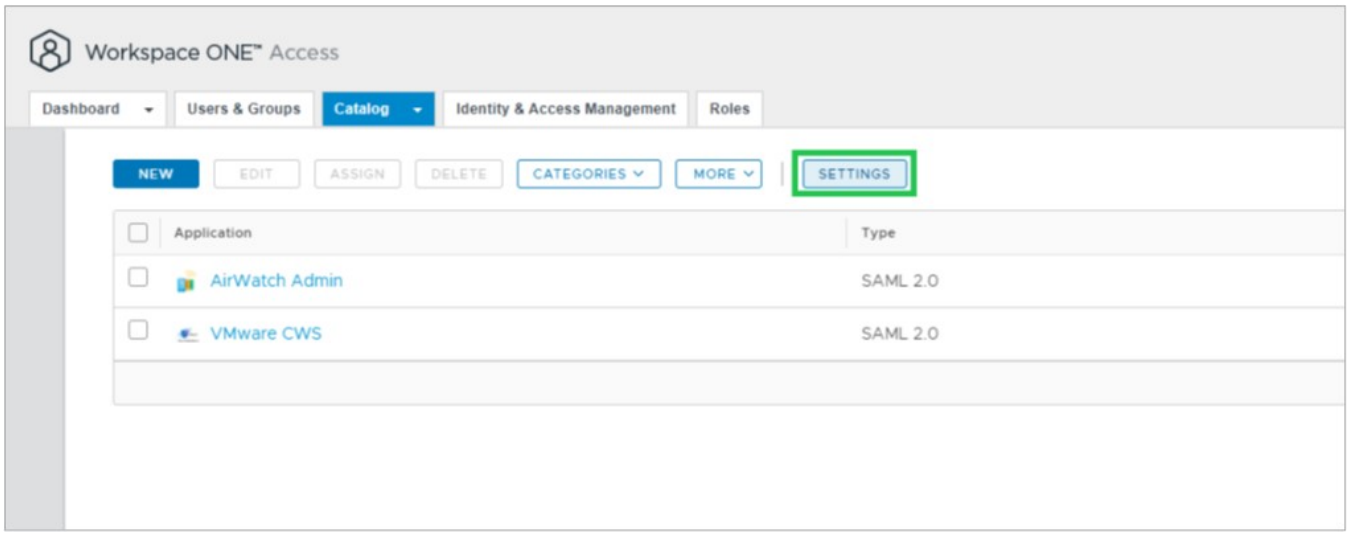
6 On the **Access Policies** page, “default_access_policy_set” is automatically selected.



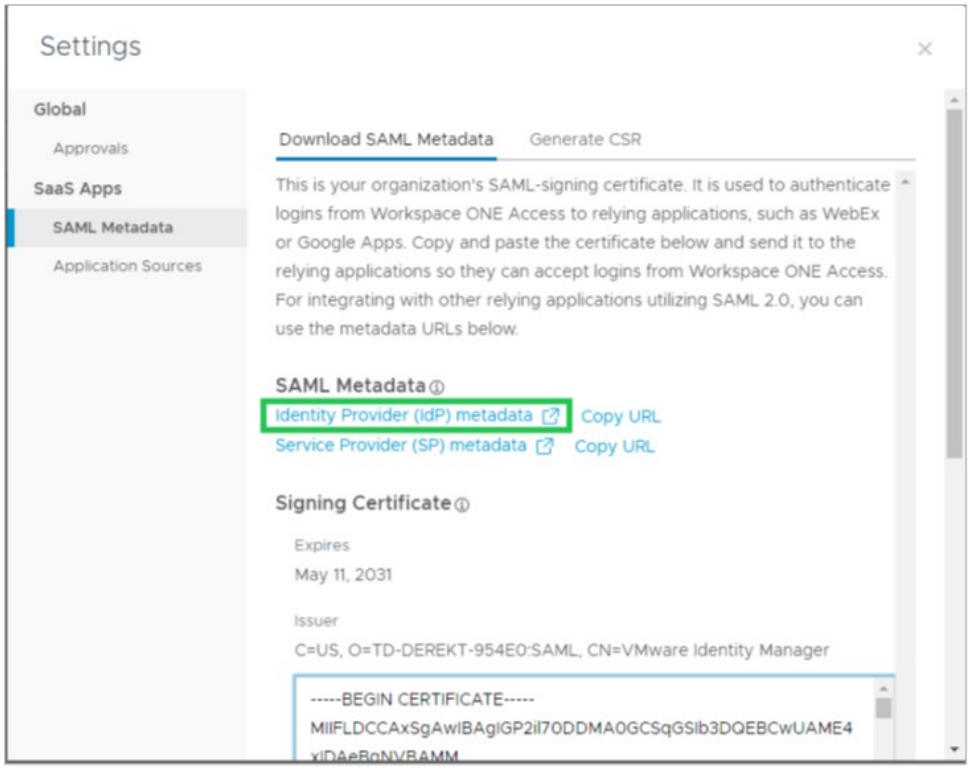
7 Click **Next** and Click **Save and Assign**.



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



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



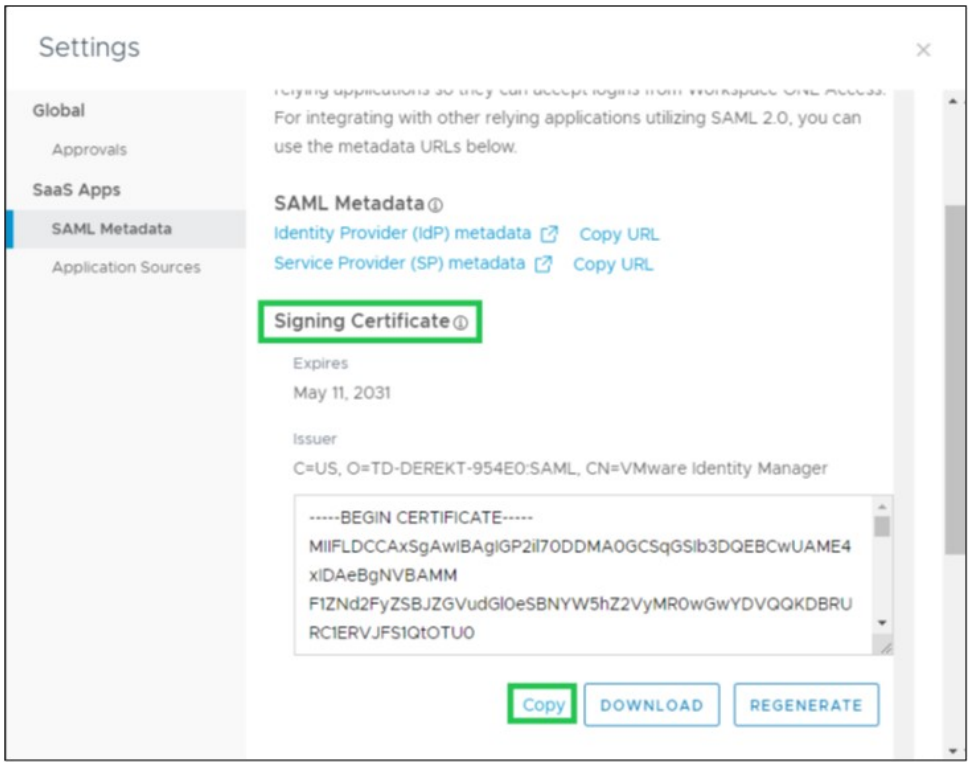
10 Click on **Identity Provider (IdP) metadata**. This action opens a new window in your browser with XML data. Copy the "entityID" and "Location" URL into a notepad.

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

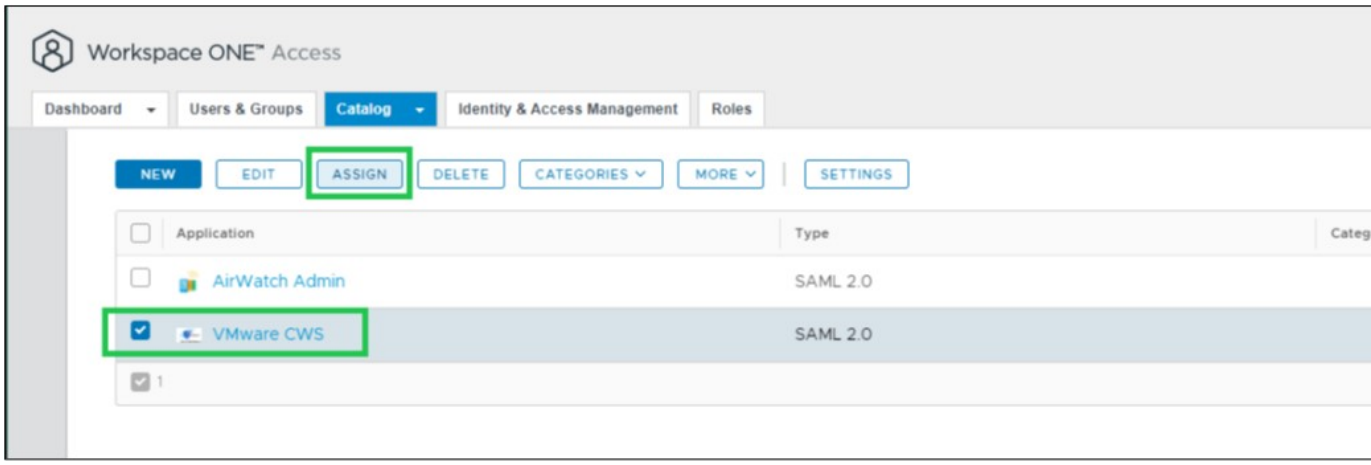
- Location: https://<ws1access_server>/SAAS/auth/federation/sso

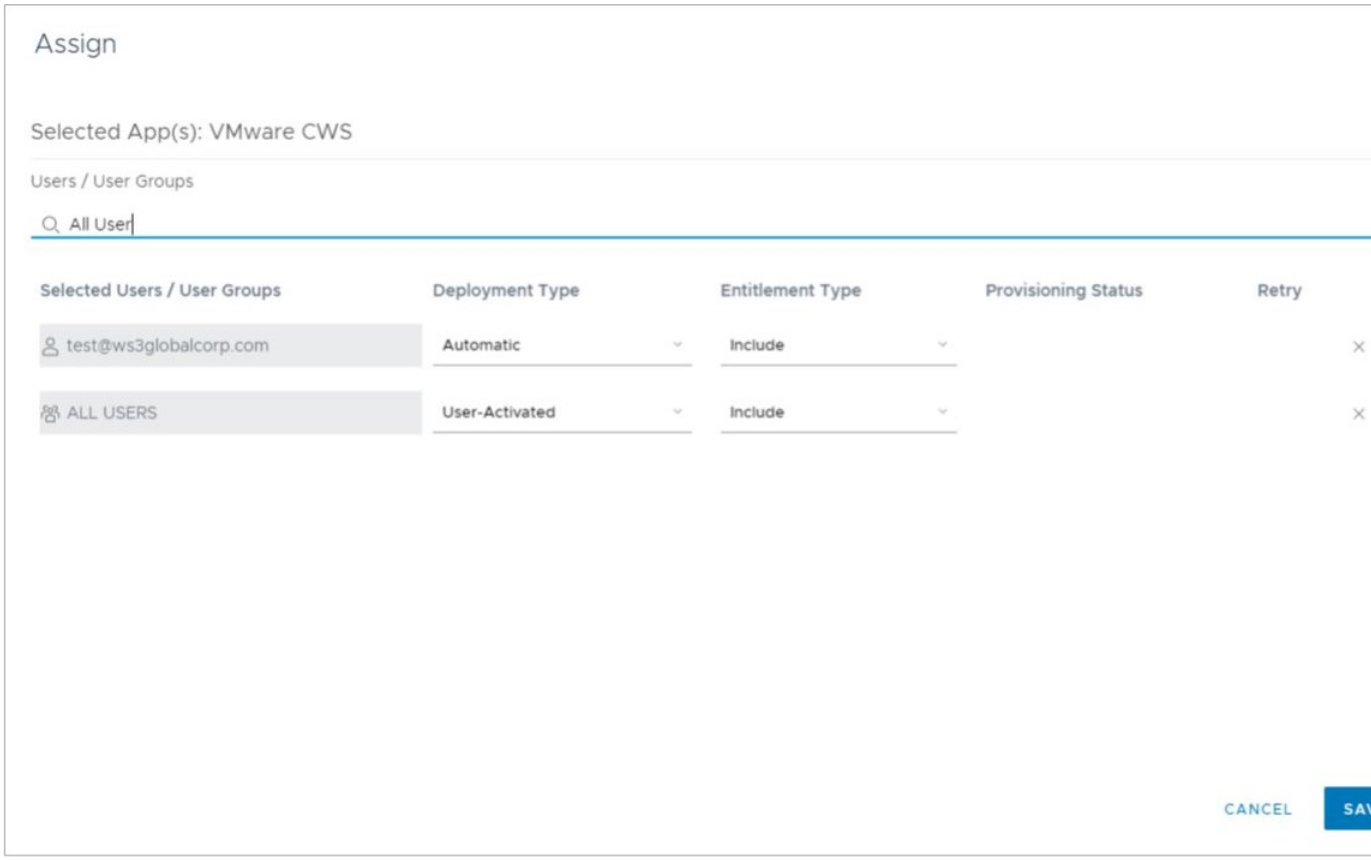
  where <ws1access-server> is the Workspace ONE Access server in your environment.

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



12 Assign User Groups to the VMware CWS web application.

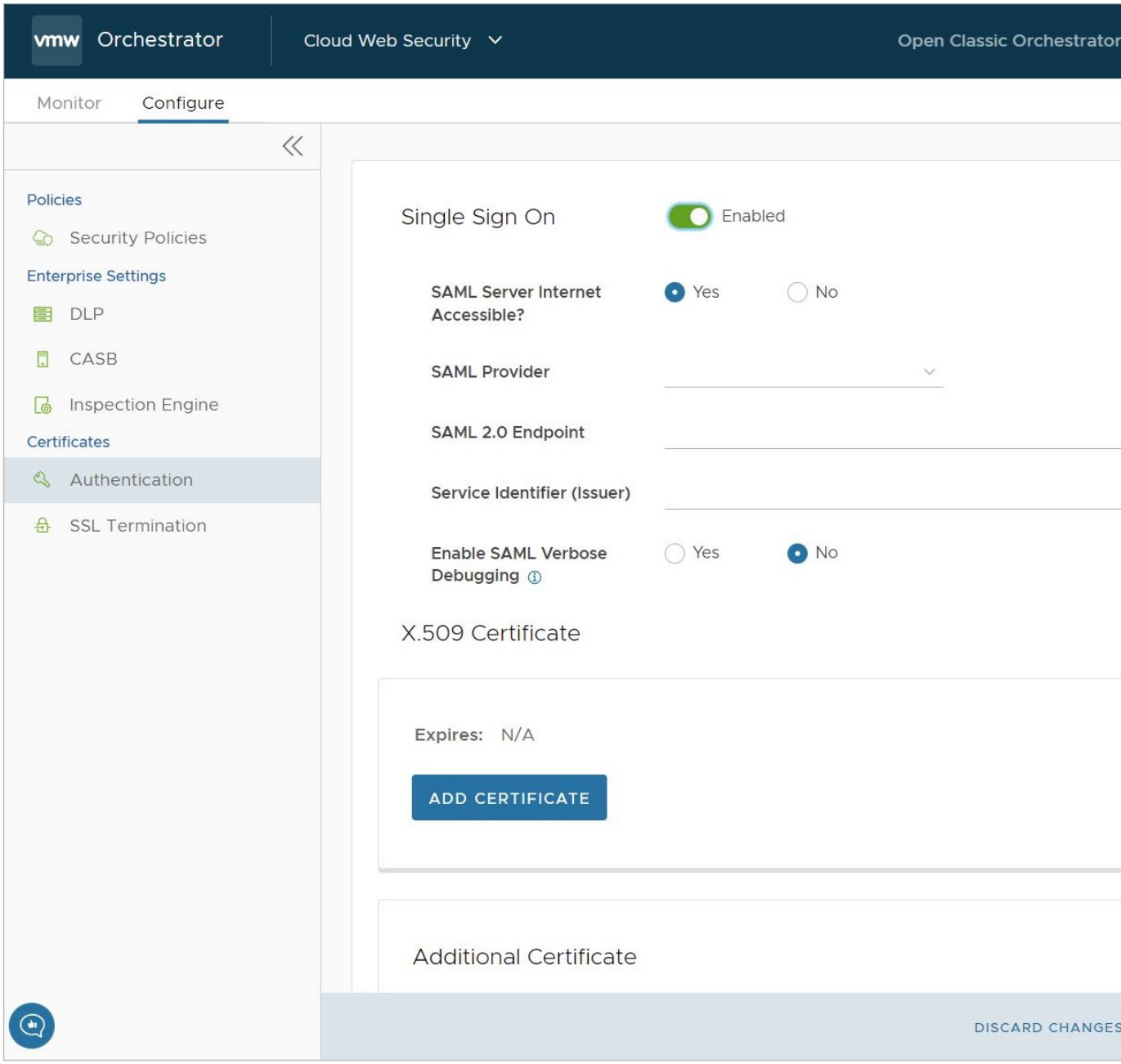




VMware SASE Orchestrator Configuration

1 Log onto the Orchestrator UI and then open the New Orchestrator UI.

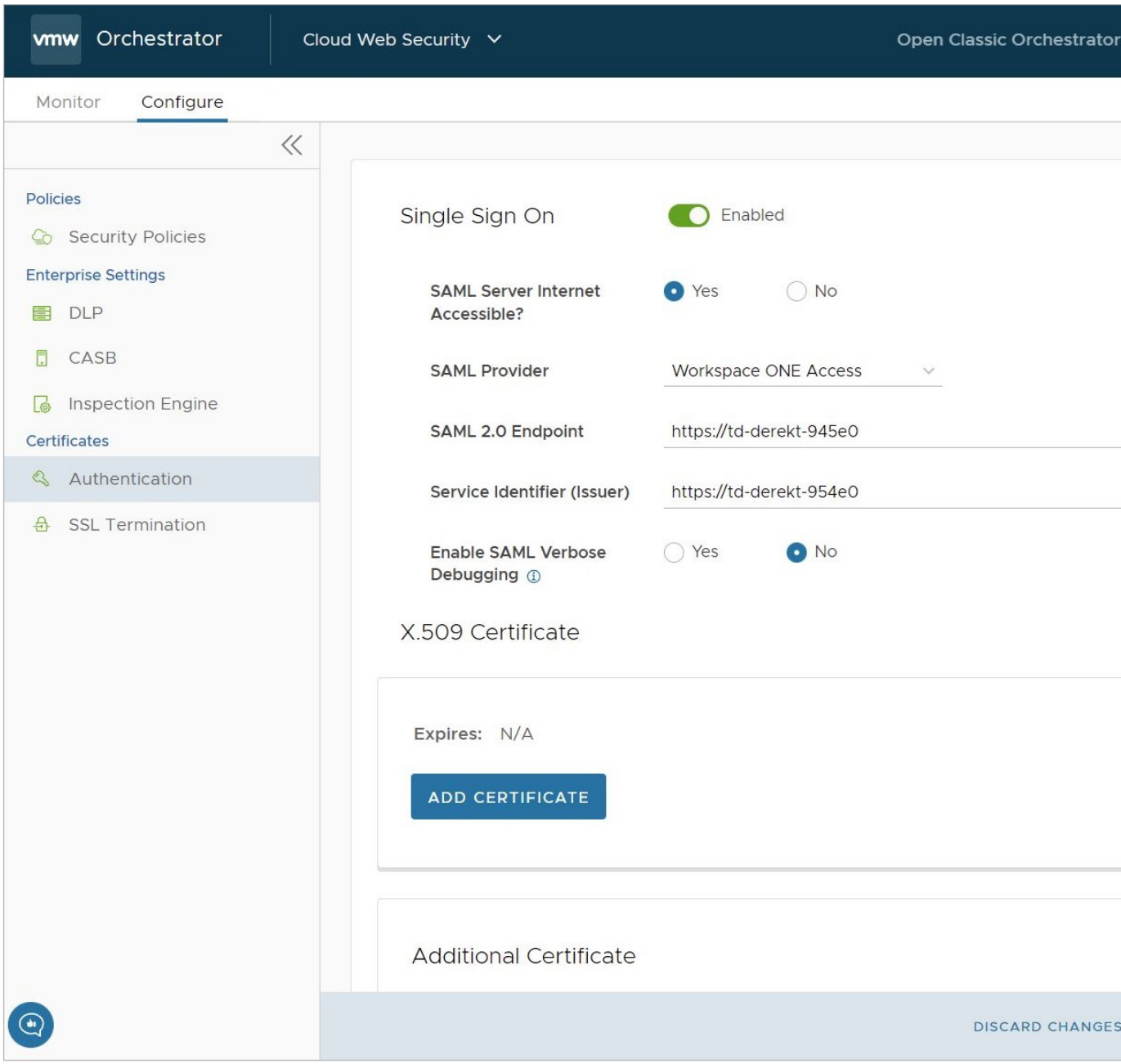
2 Go to **Cloud Web Security > Configure Authentication**. Enable Single Sign On.



3 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.

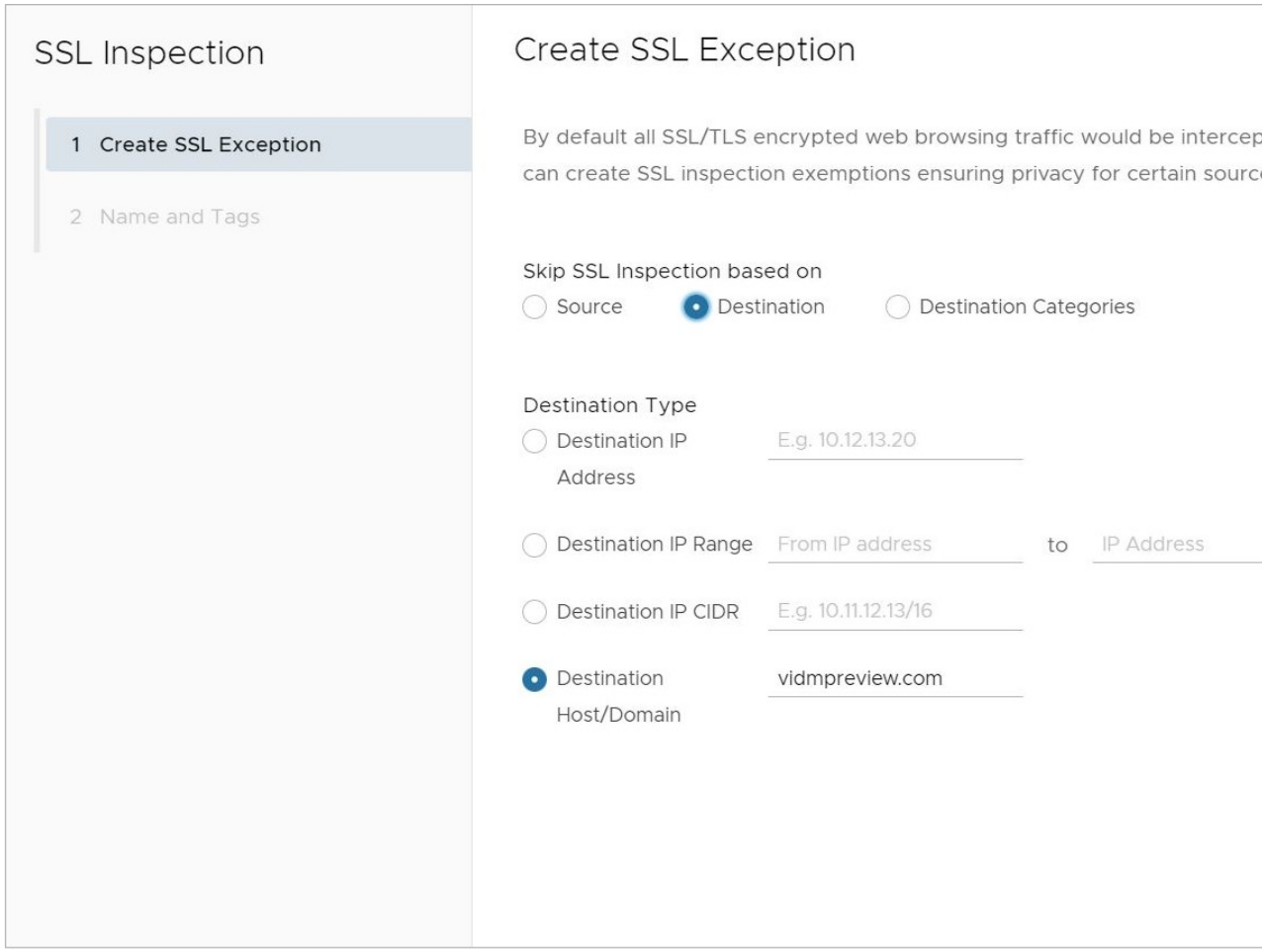
- Click **Save Changes**



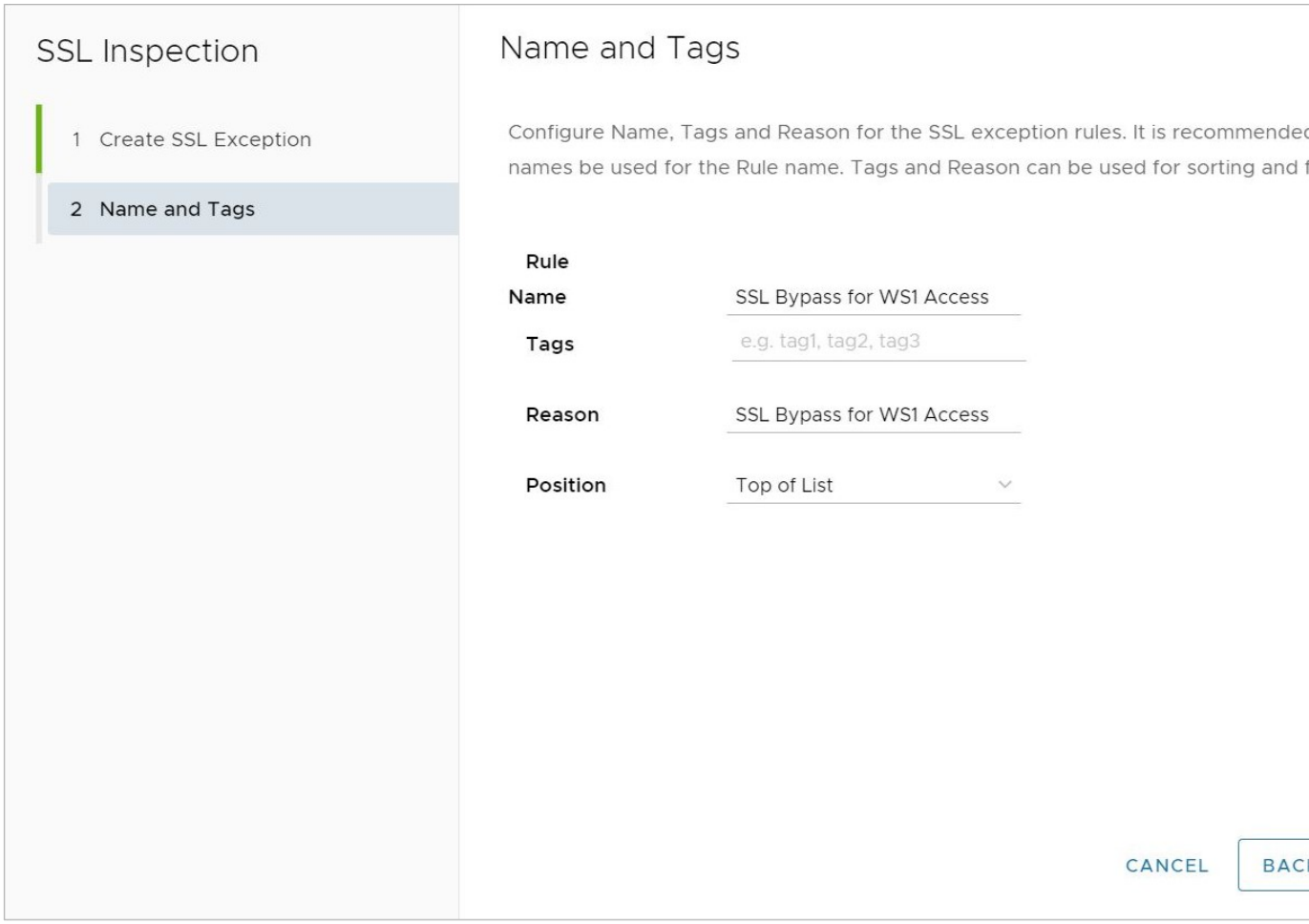
4 Add an SSL Bypass rule for the Workspace ONE Access domain.

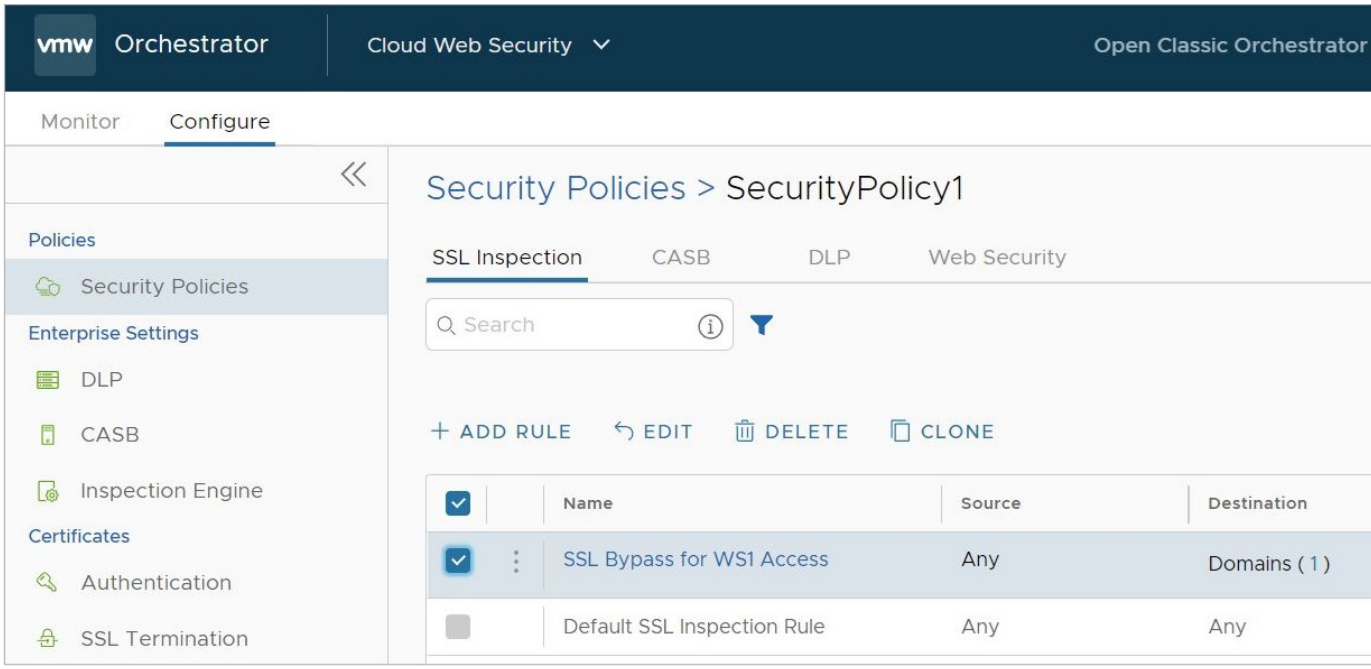
- Under Cloud Web Security, **Configure > Select Policy** for example, "SecurityPolicy1"
- Click on **Policy > Edit**
- Under **SSL Inspection**
  - **Add Rule**
  - For **Skip SSL Inspection based on**: select **Destination** checkbox
  - For **Destination Type**, select **Destination Host/Domain**

- Then specify the domain of the Workspace ONE Access server: **vidmpreview.com**, and click **Next**.



- On the **Name and Tags** screen, name the new rule and add a reason, if desired. Click **Finish**, and then republish the Security Policy to apply this new rule.


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
names be used for the Rule name. Tags and Reason can be used for sorting and f
Rule Name
SSL Bypass for WS1 Access
Tags
e.g. tag1, tag2, tag3
Reason
SSL Bypass for WS1 Access
Position
Top of List
CANCEL
BACK

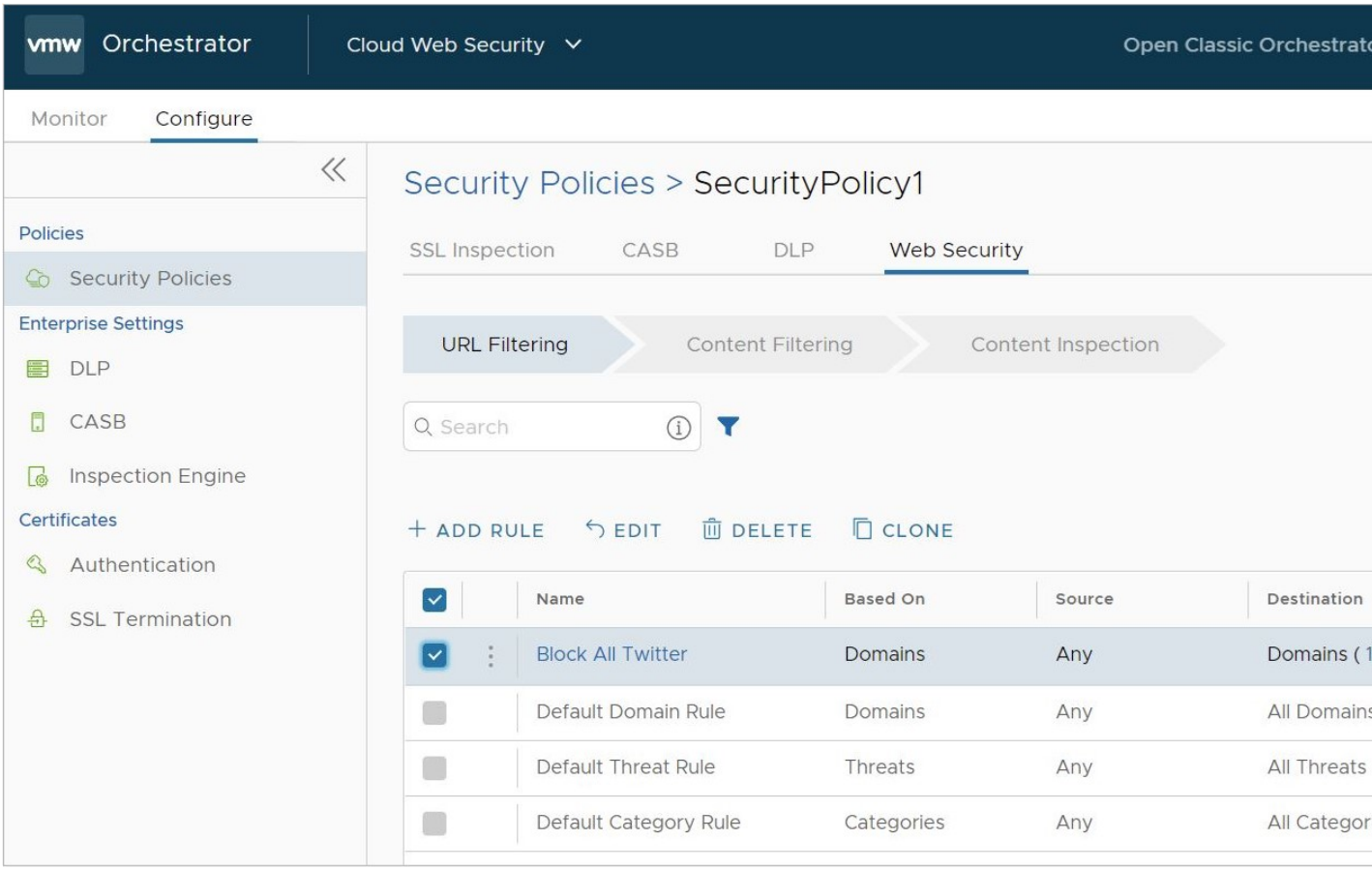


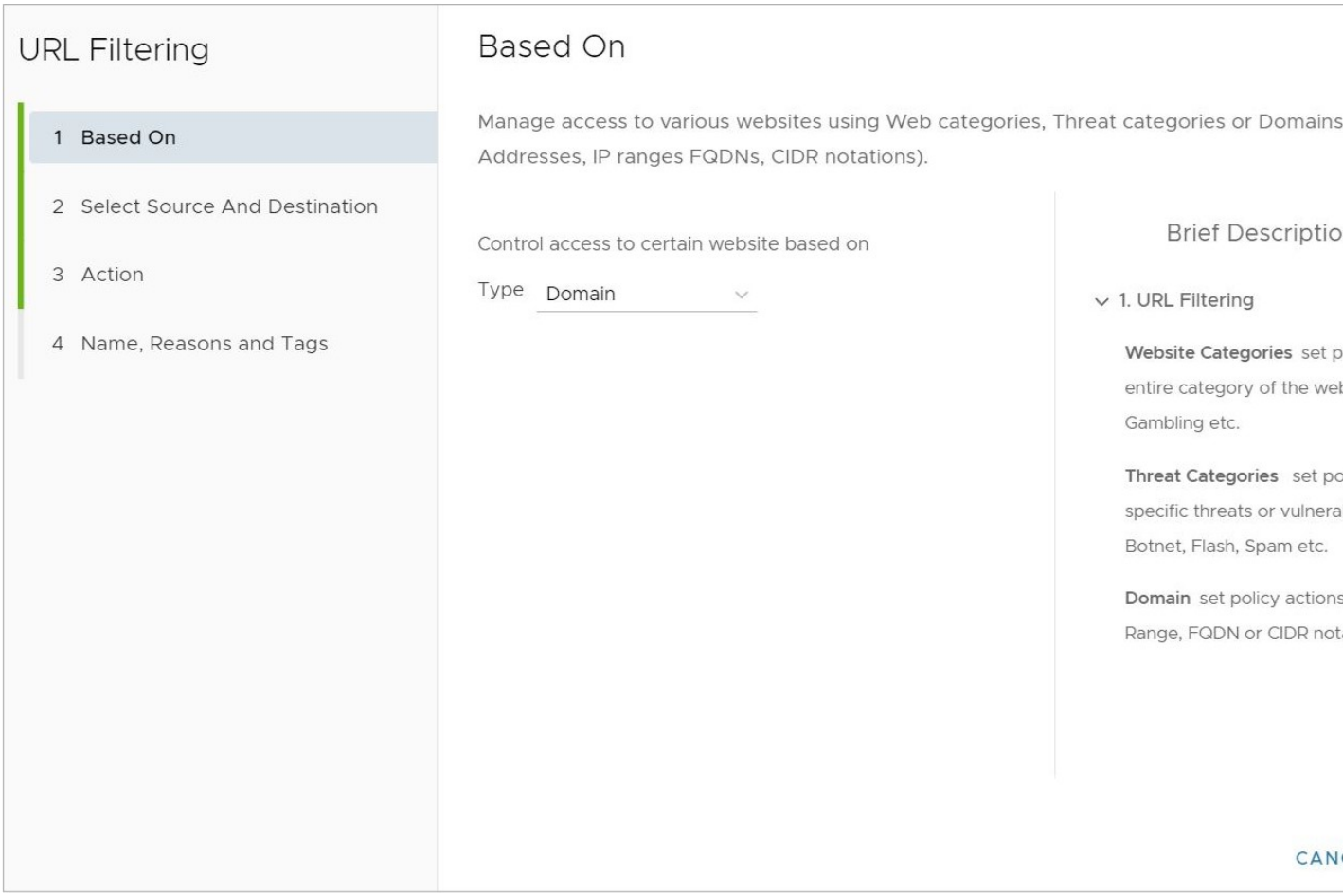
Note The domain **vidmpreview.com** is part of the **Workspace ONE** pair of domains as found in the document: Domains and CIDRs Where an SSL Inspection Bypass Rule Is Recommended. If you have already configured an SSL Bypass rule which includes both **Workspace ONE** domains, you can skip this step. 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 customer enterprise.

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

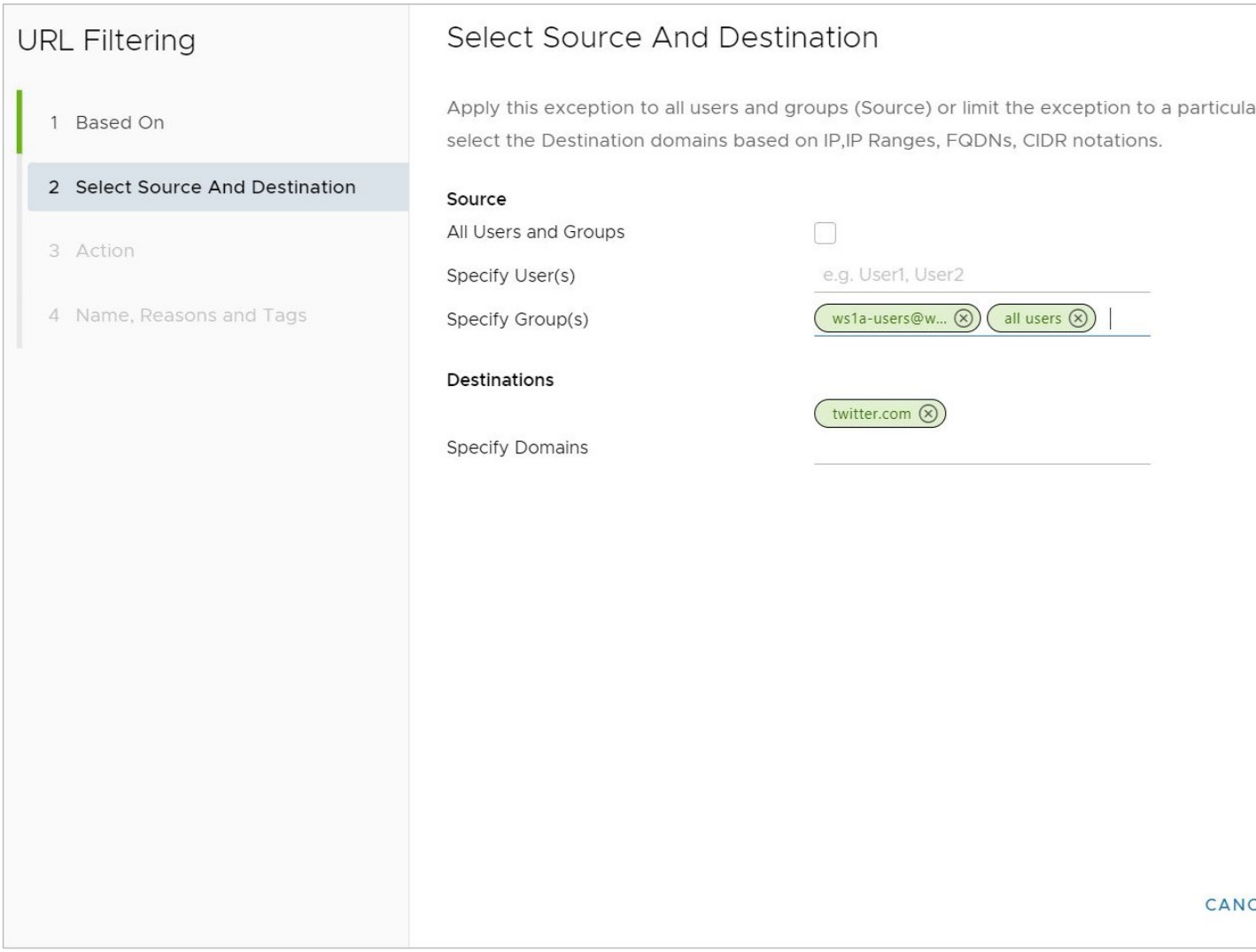
Verifying your configuration may be done using one or more group based web policy rules on Cloud Web Security. For example, using URL Filtering and blocking Twitter.com.


vmw Orchestrator
Cloud Web Security
Open Classic Orchestrato
Monitor
Configure
Policies
Security Policies
Enterprise Settings
DLP
CASB
Inspection Engine
Certificates
Authentication
SSL Termination
Security Policies > SecurityPolicy1
SSL Inspection
CASB
DLP
Web Security
URL Filtering
Content Filtering
Content Inspection
Search
+ ADD RULE
EDIT
DELETE
CLONE
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

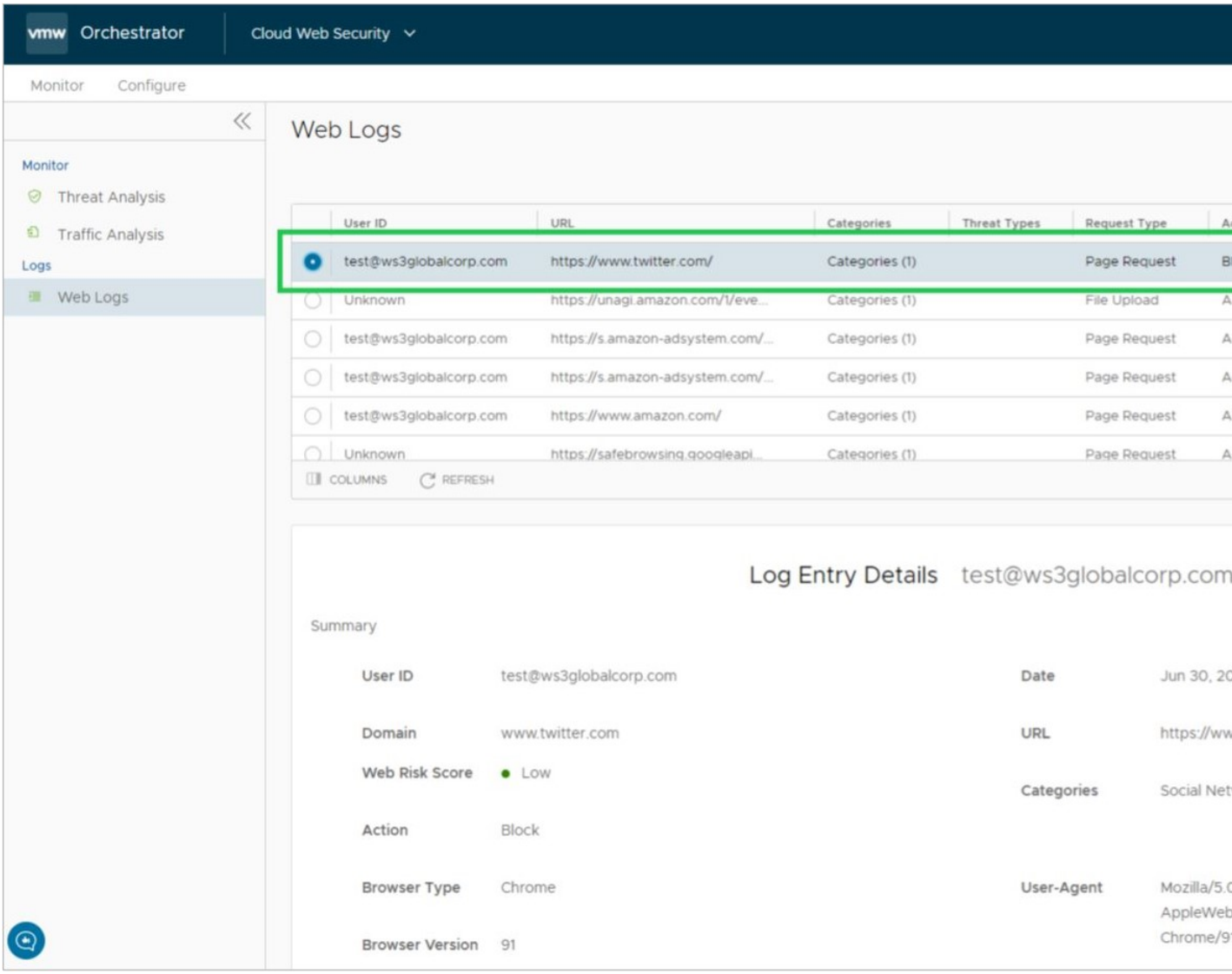


Add the Groups to be considered for the URL Filter rule.

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.



Check the Web Logs under **Cloud Web Security > Monitor > Web Logs**


vmw Orchestrator
Cloud Web Security
Monitor
Configure
Monitor
Threat Analysis
Traffic Analysis
Logs
Web Logs
Web Logs
User ID
URL
Categories
Threat Types
Request Type
test@ws3globalcorp.com
https://www.twitter.com/
Categories (1)
Page Request
Unknown
https://unagi.amazon.com/1/eve...
Categories (1)
File Upload
test@ws3globalcorp.com
https://s.amazon-adsystem.com/...
Categories (1)
Page Request
test@ws3globalcorp.com
https://s.amazon-adsystem.com/...
Categories (1)
Page Request
test@ws3globalcorp.com
https://www.amazon.com/
Categories (1)
Page Request
Unknown
https://safebrowsing.googleapi...
Categories (1)
Page Request
COLUMNS
REFRESH
Log Entry Details
test@ws3globalcorp.com
Summary
User ID
test@ws3globalcorp.com
Date
Jun 30, 20
Domain
www.twitter.com
URL
https://ww
Web Risk Score
Low
Categories
Social Net
Action
Block
Browser Type
Chrome
User-Agent
Mozilla/5.0
AppleWeb
Chrome/9
Browser Version
91