# 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 <sup>©</sup> 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

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<sup>™</sup> 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.

<u>Configure Gateways</u> ∍ VCg32-sjc2 <mark></mark>			
Overview Monitor			
Properties			
* Name	vcg32-s	jc2	
Description			1
Gateway Roles	Cont CDE Clou Data Parti	rol Plane d Web Security Plane ner Gateway Ire VPN Gateway	
Contact & Locatio	n		
Cloud Web Securi	ty		
Geneve Endpoint IP	Address	xxx.xx.x.x	
POP name		PoP-1	

- 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.

			Open	New Orches	trator UI	Recently	Viewed	Operator Standard Ac	lmin
Ed	ges								
Sear	ch	v 0 💷	Cols Reset View	v <b>2</b> Refresh	<b>≛</b> CSV				
	Edge	Status 🛧	HA	Links		VM Status	VNF	Edge Tunnels	
1	Test Edge	٥		•• 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.

vmw Orchestrator	Clo	oud Web Security 🗸 🗸			?	Do
Monitor Configure	~	Security Policies				
Policies						
Certificates		+ NEW POLICY VED	IT 🗍 DELETE			
♣ SSL Termination		Name	Status	Modified	Is Published	

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.

Create a new Security Poil	icy	×
SecurityPolicy1		
Diases enter the should information and	click next to continue	
Please enter the above information and o		

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).

vmw Orchestrator	CIC	bud Web Security 💙			0
Monitor Configure					
	~	Security Policies			
Policies					
Security Policies					
Certificates		+ NEW POLICY VEDIT	DELETE		
SSL Termination		Name	Status	Modified	Is Published
		SecurityPolicy1	Unused	Jun 6, 2021, 9:50:05 PM	No

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.

vmw Orchestrator	CIC	oud Web Security 🗸 🗸			0	උ	Ξ
Monitor Configure							
	~	Security Policies > Securit	yPolicy1			PUBL	LISH
Policies		•					
Security Policies		SSL Inspection URL Filter	ing Content Filtering	g Content Insp	ection		
Certificates Authentication SSL Termination		+ ADD RULE 5 EDIT DELET	E CLONE				
		Name	Source	Destination	Action		
		Default SSL Inspection Rule	Any	Any	Inspect		

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

~	Security	Policies > Secu	urityPolicy1					PUBLISH
Policies								
Security Policies	SSL Insp	url F	Filtering	Content Fill	tering	Content Inspe	ection	
Iertificates								
Authentication								
SSI Termination								
SSL Termination	+ ADD RUI	LE SEDIT 🗇 DE	LETE ÖCLO	NE				
SSL Termination	+ ADD RUI	<b>LE 🕆 Ε</b> ρίτ 📋 DE	LETE 🗋 CLO	NE				
SSL Termination		LE SEDIT 🗎 DE	Transfer Type	NE Based On	Source	Destination	Action	Inspections
SSL Termination	+ ADD RUI	Name Word Processing Docs	Transfer Type Download	Based On File Category	Source Users ( 2 ), Groups ( 2 )	Destination Domains ( 2 ), Categories ( 3 )	Action Inspect	Inspections

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

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

Publish policy?		
NOTE: It will take up to a m	nute for policy t	o take effect.
NOTE: It will take up to a m	inute for policy t	to take effect.

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

Monitor Configure						
	~	S $\times$ Your policy is being published $\times$				PUBLISH
Policies						
Security Policies		SSL Inspection	URL Filtering	Content Filtering	Content Inspection	
Certificates						
4 Authentication						

**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.

vmw Orchestrator	Clo	bud Web Security 💙			0	8	$\equiv$
Monitor Configure							
	~	Security Policies > Security	Policy1			PUB	LISH
Policies							
Security Policies		SSL Inspection URL Filterin	g Content Filtering	g Content In	spection		
Certificates							
Authentication							
SSL Termination							
		+ ADD RULE SEDIT 🗇 DELETE	CLONE				
		Name	Source	Destination	Action		
		Default SSL Inspection Rule	Any	Any	Inspect		

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.

SSL Inspection	Create SSL Excep	tion		×
1 Create SSL Exception	Create SSL exception for co domains, IP addresses, web	ertain sources based or osite categories or CIDR	n IP address or destinations based on hostn ? prefixes	ames,
2 Name and Tags	Skip SSL Inspection based	on on O Destination (	Categories	
	Destination Type			
	O Destination IP Range		to	
	O Destination IP CIDR			
	<ul> <li>Destination IP z</li> <li>Host/Domain</li> </ul>	oom.us		

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.

SSL Inspection	Create SSL Exception ×
1 Create SSL Exception	Create SSL exception for certain sources based on IP address or destinations based on hostnames, domains, IP addresses, website categories or CIDR prefixes
2 Name and Tags	Skip SSL Inspection based on Source ODestination Categories
	Destination Type O Destination IP Address
	Destination IP Range to      Destination IP CIDR
	Destination IP zoom.us     Host/Domain

- 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.

SSL Inspection	Name and Tag	S		×
1 Create SSL Exception	Create SSL exception domains, IP addresses	for certain sources based on IP addr , website categories or CIDR prefixe:	ess or destinations based on hostnames, 5	
2 Name and Tags				
	Rule			
	Name	Zoom		
	Tags	Eg: tag1, tag2, tag3		
	Reason	Zoom Outbound Traffic		

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.

URL Filtering	Select Source And Destination
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses
2 Select Source And Destination	Source
3 Action	All Users and Groups
4 Name, Reasons and Tags	Destinations O All Categories (84) Custom Selection (12) Q Search
	Abortion       Abused Drugs       Adult and Pornography       Alcohol and Tobacco       Auctions       Bot Nets         Business and Economy       Cheating       Computer and Internet info       Computer and Internet Security         Confirmed SPAM Sources       Content Delivery Networks       Cult and Occult       Dating       Dead Sites         Dynamic Content       Educational Institutions       Entertainment and Arts       Pashion and Beauty       Financial Services         Food and Dining       Gambling       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         Keyloggers and Monitoring       Kids       Legal       Local Information       Malivare Sites       Marijuana       Military         Motor Vehicles       Music       News and Media       Nudity       Online Greeting cards       Open HTTP Proxies         Parked Domains       Pay to Surf       Peer to Peer       Personal Sites and Blogs       Personal Storage         Philosophy and Political Advocacy       Phishing and Other Frauds       Private IP Addresses         Proxy Avoidance an

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.

URL Filtering	Action		×
1 Applied To	Control access and addresses	uploads/downloads from various websites using Web categories, Threat categories, domains,	q
2 Select Source And Destination			
3 Action	Action	BLOCK V	
4 Name, Reasons and Tags			

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.

URL Filtering	Name, Rea	sons and Tags		×
1 Applied To	Control access a addresses	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains addresses		ategories, domains, IP
2 Select Source And Destination				
3 Action	Rule Name	Website Categories 1		
4 Name, Reasons and Tags	Tags	Eg: tag1, tag2, tag3		
	Reason	Spam, Malware, Security		
	Position	Top of List ~		

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

Security	Policies > SecurityPolicy1				
SSL Inst	Dection URL Filtering Conten	t Filtering Content Inspection			
+ ADD RU	LE 17 EDIT 🖹 DELETE 🖺 CLONE				
	Name	Based On	Source	Destination	Action
	TikTock	Domains	Any	Domains (1)	Block
	Threat Categories 1	Threats	Апу	Threats (7)	Block
0 :	Website Categories 1	Categories	Any	Categories ( 12 )	· Block
	Default Domain Rule	Domains	Any	All Domains	Allow
	Default Threat Rule	Threats	Апу	All Threats	Allow
	Default Category Rule	Categories	Any	All Categories	Allow

- 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 dropdown 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.

URL Filtering	Applied To	
1 Applied To	Control user/group access to certain website catego domains,categories and file types	ries or control file uploads/downloads based on
2 Select Source And Destination		Brief Description
3 Action	<ul> <li>Control access to certain website based on</li> <li>Type Threat Categories </li> </ul>	Website Access Control     Select the category or
4 Name, Reasons and Tags	Website Categories Threat Categories Domain	categories you would like to create an exception for

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.

JRL Filtering	Select Source And Destination
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses
2 Select Source And Destination	Source
3 Action	All Users and Groups
4 Name, Reasons and Tags	Destinations         All Categories (11)         Q. Search           © Custom Selection (7)         Custom Selection (7)         Custom Selection (7)
	Vulnerable Service         Uncategorized Site         Flash         Spam         Phishing         Malware         Malvertising           Compromised Host         Command & Control         Botnet         Parked Domains         Malvertising

- 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.

URL Filtering	Action
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses
2 Select Source And Destination	
3 Action	Action BLOCK ALLOW RUGCK
4 Name, Reasons and Tags	

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.

URL Filtering	Name, Reas	sons and Tags
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses	
2 Select Source And Destination		
3 Action	Rule Name	Threat Categories 1
4 Name, Reasons and Tags	Tags	Eg; tag1, tag2, tag3
	Reason	Malware, Spam, Security
	Position	Top of List 🗸

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

Security	/ Policies > SecurityPolicy1				
SSL Inst	Dection URL Filtering Conten	t Filtering Content Inspection			
+ ADD RU	LE 17 EDIT 🖹 DELETE 🖺 CLONE				
	Name	Based On	Source	Destination	Action
	Name	Based On Domains	Source	Destination Domains (1)	Block
	Name TRETOCK Threat Categories 1	Based On Domains Threats	Source Any Any	Destination Domains (1) Threats (7)	Action Block Block
	Name TRETock Threat Categories 1 Website Categories 1	Based On Domains Threats Categories	Source Any Any Any	Destination Domans (1) Threats (7) Categories (12)	Action Block Block Block
	Name TRClock Threat Categories 1 Vebsite Categories 3 Default Domain Rule	Based On Domains Threats Categories Domains	Source Any Any Any Any	Demination Domains (1) Threats (7) Categories (12) All Domains	Action Block Block Block Allow
	Name TRCIOCK Threat Categories 1 Vebsite Categories 1 Default Domain Rule Default Threat Rule	Based On Domains Threats Categories Domains Threats	Source Any Any Any Any Any Any Any Any	Demination Domains (1) Threats (7) Categories (12) All Domains All Threats	Action  Block Block Block Allow Allow

- 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.

URL Filtering	Select Source And Destination
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses
2 Select Source And Destination	Source
3 Action	All Users and Groups
4 Name Deasons and Tags	Destinations
4 Hunte, Reasons and rags	Specify Domains tiktok.com

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.

URL Filtering	Action
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses
2 Select Source And Destination	
3 Action	Action BLOCK  ALLOW BLOCK
4 Name, Reasons and Tags	

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.

Security	y Policies > SecurityPolicy1				
SSL Inst	Dection URL Filtering Conten	t Filtering Content Inspection			
+ ADD RU	LE +) FOIT B DELETE CLONE	Basad On	Source	Destination	Action
	TikTock	Domains	Any	Domains (1)	Block
0 :	Threat Categories 1	Threats	Any	Threats (7)	Block
0 :	Website Categories 1	Categories	Any	Categories ( 12 )	Block
	Default Domain Rule	Domains	Any	All Domains	Allow
	Default Threat Rule	Threats	Any	All Threats	Allow
-	Default Category Rule	Categories	Any	All Categories	Allow

- 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	Supported Documents		
Windows Executable	.com, .exe, .dll, .msi, .scr	AutoCAD	CSV	Excel
Linux Executable	.rpm, .deb	Hangul	Ichitaro	MS One Note
Mac Executable	.dmg	MS Project OpenOfficeSpreadsheet	OpenOffice Presentation PDF	OpenOffice Text PowerPoint
Text based script files	.py, .reg, .sh, .vb, .vbe, .bat, .vbs, .cmd, .msh, .pif, .msc	RTF Word Perfect	Visio XPS	Word
JAR	.jar, .ear, .war			
Android Executable	.apk, .dex	Supported Archives		
Audio files	.mp2, .mp3, .wav, .ra	7-ZIP	ARJ	BZIP
		CAB	GZIP	LZH
/ideo files	.mpg, .3gp, .mp4, .webm	RAR	TAR	ZIP
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.

Content Filtering	Applied To	
1 Applied To	Control user/group access to certain website categori domains,categories and file types	ies or control file uploads/downloads based on
2 Select Source And Destination		
3 Action	Transfer Tune	
4 Name, Reasons and Tags	Download Upload	Brief Description
	File Type	> Download
	Select File Category	> Upload
	All Documents Engineering Applications Productivity Word Processors Spreadsheets Presentation Tools All Files	
	Scripts and Executables Archives and Compressed Packages Multimedia Calendar	

5 Click Next.

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

ontent Filtering	Select Source And I	Destination	
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses		
2 Select Source And Destination	Source		
3 Action	All Users and Groups		
4 Name, Reasons and Tags	Destinations All Domain/Categories		
	Specify Domains	Eg: www.google.com,	
		Hacking × Malware Sites ×	
		Proxy Avoidance and Anonymizers x	
		Guestionable $\times$ Shareware and Freeware $\times$	
		Uncategorized x Spyware and Adware x	
	Specify Categories		

- 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.

Content Filtering	Action	
1 Applied To 2 Select Source And Destination	Control access and addresses	uploads/downloads from various websites using Web categories, Threat categories, domains, IP
3 Action	Anting	DI COLY
4 Name, Reasons and Tags	Action	ALLOW BLOCK

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

Content Filtering	Action		
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses		
2 Select Source And Destination			
3 Action	Action	ALLOW ~	
4 Name, Reasons and Tags			
	More Actions		
	Perform Content Inspection		

- 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.

Content Filtering	Name, Re	asons and Tags		
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, do addresses		gories, domains, IP	
2 Select Source And Destination				
3 Action	Rule Name	Executables and Scripts		
4 Name, Reasons and Tags	Tags	Eg: tag1, tag2, tag3		
	Reason	Blocking executables	_	
	Position	Top of List	<u>v</u>	

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 O" 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.

*	Security Policies > SecurityPolicy1			PUBLIS
Policies				
Security Policies	SSL Inspection URL Filtering C	Content Filtering	Content Inspection	
Certificates				
4 Authentication				
SSL Termination				
	+ ADD RULE 5 EDIT 📋 DELETE 📋 CLONE			
	Name Transfer Type Based On	Source Des	ination Action	Inspections

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.

Content Inspection	Applied To
1 Applied To	Control user/group access to certain website categories or control file uploads/downloads based on domains,categories and file types
2 Select Source And Destination	
3 Action	Transfer Type Upload V Download
4 Name, Reasons and Tags	Based on  File Type File Hash  Word Processors  Ichitaro  Word PDF
	Hangul XPS OpenOffice Text 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.

Content Inspection	Select Source And De	estination	×
1 Applied To	Control access and uploads/dow categories, domains, IP addresse	nloads from various websites using Web cate s	gories, Threat
2 Select Source And Destination	Source		
3 Action	All User Groups		
4 Name, Reasons and Tags	Specify Users	User 1 User 2	
	Specify Groups	Group A Group B	
	Destinations		
	All Domain/Categories		
	Specify Domains	(www.google.c.,.) (dropbox.com)	
		Computer and Internet Info x	
	Specify Categories	Computer and internet Security $\ \ \times$	~
		Hacking	*
		Hate and Racism	
		Health & Medicine	1
		Home and Garden	BACK
		Hunting and Fishing	
		llegal	
		Image and Video Search	
		Individual Stock Advice and Tools	×

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.

Content Inspection	Action	
1 Applied To	Control access and uploads/dow addresses	nloads from various websites using Web categories, Threat categories, domains, IP
2 Select Source And Destination	Policy Action	Mark As Clean 🗸
3 Action	More Options (i)	Mark As Clean Mark As Infected Inspect
4 Name, Reasons and Tags	All Checks	Inspect
	File Hash Check	
	File Full Scan	
	Sandbox Inspection	

 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.

Content Inspection	Action		
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domain addresses		
2 Select Source And Destination	Policy Action	Inspect	-
3 Action	More Options (j)		
4 Name, Reasons and Tags	All Checks 🔽		
	File Hash Check		
	File Full Scan		
	Sandbox Inspection		

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.

Content Inspection	Name, Reasons and Tags	
1 Applied To	Control access and uploads/downloads from various websites using Web categories, Threat categories, domains, IP addresses	
2 Select Source And Destination		
3 Action	Rule Name	Word Processing Docs
4 Name, Reasons and Tags	Tags	Eg: tag1, tag2, tag3
	Reason	To inspect docs dl'd by search
	Position	Top of List
		Top of List Bottom of 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, applecloudkit.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.cdnapple.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, lcdnlocator.apple.com, icloud.com.cn, mdmenrollment.apple.com, ns.itunes.apple.com, cdnapple.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, psyjscdn.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, 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.microsoftonlinep.com, msidentity.com, outlook.office.com, msftidentity.com, security.microsoft.com, login-us.microsoftonline.com, autologon.microsoftazureadsso.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, 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, wsuklwestprod.blob.core.windows.net, usseulnorthprod.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, wseulwestprod.blob.core.windows.net, usv20.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, ussuklwestprod.blob.core.windows.net, automatedirstrprdweu.blob.core.windows.net, winatpgw-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, usseulwestprod.blob.core.windows.net, winatp-gw-uks.microsoft.com, ussusleastprod.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, winatpgw-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, storeimages.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.smicrosoft.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, axmapp.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, wsuklsouthprod.blob.core.windows.net, wseulwestprod.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, usseulwestprod.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, ussuklwestprod.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, wsuslwestprod.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, usseulnorthprod.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, wseulnorthprod.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, usv20.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, wsuklwestprod.blob.core.windows.net, google-analytics.com, gsa.apple.com, axmadm-enroll.apple.com, passwordreset.microsoftonline.com, eum-appdynamics.com, smp-device-content.apple.com, apps.apple.com, windowsupdate.microsoft.com, gotomeeting.com, ppg.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, ussusleastprod.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.microsoftonlinep.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.slackmsgs.com, gototraining.com, join.me, winatp-gw-cus3.microsoft.com, appleid.cdn-apple.com, ussuklsouthprod.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.smicrosoft.com, stats.adobe.com, apple-livephotoskit.com, zoom.us, appdynamics.com, login.windows.net, autologon.microsoftazuread-sso.com, wsusleastprod.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.

nfigure Rule		?
Rule Name	Security Policy 1	
atch		
Source	Any Object Group Define	
Destination	Any Object Group Define	
	<ul> <li>Anv</li> <li>Internet</li> <li>Edge</li> <li>Non SD-WAN Destination via Gateway</li> <li>Non SD-WAN Destination via Edge</li> </ul>	
	IP Address Ex: 10.0.2.0	
	CIDR prefix V 24	_
	Protocol	_
	Ports Ex: 2224-2226	
Application	Any Define	
tion		
Priority	High Normal Low	
Network Service	Direct Multi-Path Internet Backhaul	
	O Backhaul Hubs O	
	Non SD-WAN Destination via Gateway     O     Non SD-WAN Destination via Edge / Cloud Seci	rity Service 🛈
	SecurityPolicy1	
Link Steering	Select SecurityPolicy1 Transport or oup Interface WAN Link	0
	Inner Packet DSCP Tag Outer Packet DSCP Tag <b>0 - CS0/DF</b>	_1
NAT	Disabled Enabled	
Service Class	Real Time Transactional Bulk	
	_	

- 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.

Monitor	Configuration Profiles -	Configuration Profiles -							Save Changes	•	
Configure	Quick Start P	Quick Start Profile									-
🚔 Edges	Profile Overview	Device 0 B	usiness Policy	Firent							
📥 Profiles	TRAINE OTESTICH		Ganteso Foncy	C. a contraction							
Object Groups											
Segments	Configure Segn	nents									0
Overlay Flow Control											_
Network Services	Select Segment:	Global Segmer	nt [Regular]			*					
<ul> <li>Alerts &amp; Notifications</li> <li>Customer</li> </ul>	Business Policy	(							New Rule	Actions •	0
Test & Troubleshoot			Match			Action					
Administration	- Rule		Source	Destination	Application	Network Service	Link	Priority	Service Class		
Administration	□ = 1 Security	Policy 1	Any	Internet	Any	Internet Backhaul SecurityPolicy1	auto 🗌	Normal	Transactio	onal	
Used By 1 Edge	□ = 2 Box		Any	Any	Box(File Sharing)	Multi-Path	aino	High	📕 Bulk		

#### 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.

vmw Orchestrator Ci	oud Wel	b Security 🗸							0 2	1
Monitor Configure										
**	We	eb Logs								
Monitor										
Traffic Analysis		User ID	URL	Categories	Threat Types	Request Type	Action	Risk Level	Date	Î
Logs		SSL_Exception	config.teams.microsoft.com	Categories (1)		SSL Exception	SSL Inspection	G	2021-06-02T12:51:41.195Z	
I Web Logs		SSL_Exception	208.91.0.101	Categories (1)	Parked Domains, Uncategorized Site	SSL Exception	SSL Inspection	R	2021-06-02T12:43:41.840Z	
		SSL_Exception	config.teams.microsoft.com	Categories (1)		SSL Exception	SSL Inspection	G	2021-06-02T11:51:40.123Z	
		SSL_Exception	teams.microsoft.com	Categories (1)		SSL Exception	SSL Inspection	G	2021-06-02T11:34:49.673Z	
		SSL_Exception	208.91.0.101	Categories (1)	Parked Domains, Uncategorized Site	SSL Exception	SSL Inspection	R	2021-06-02T11:13:42.307Z	
		COLUMNS C REFR	confin tasme microcoft com	Catagorian (3)		CCI Excantion	\$\$L Inspection	6	0 items K K	•

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.

<ul> <li>SSL_Exception</li> </ul>	208.91.0.101	Categories (1)	Parked Domains, Uncategorized Site	SSL Exception	SSL Inspection	R	2021-06-02T09:43:41.286Z
COLUMNS C REFRESH	*****	• 1 • •				-	0 items  < <
			Log Entry Details	SSL_Exception			
Summary							
User ID	SSL_Exception			Date	2021-06-02T09:43:41.286Z		
Domain	208.91.0.101			URL	208.91.0.101		
Threat Types	Parked Domains, Uncategorized Site			Categories	Dead Sites		
Action	SSL Inspection			Web Risk Score	R		
Browser Type	Unavailable			User-Agent	None		
DNS Response	208.91.0.101			Request Type	SSL Exception		
Protocol	https			Source IP	10.48.49.153		
Policy Headers	3437016787			Rule Matched	Bypass all		

# Single Sign-On Guides (SAML)

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.

Create your own applie	cation
What's the name of your app?	
CWS	~
What are you looking to do with your appl	ication?
O Configure Application Proxy for secure	e remote access to an on-premises application
O Register an application to integrate wi	ith Azure AD (App you're developing)
Integrate any other application you do	on'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.

	Microsoft Azure	
Ho	me > Enterprise applications >	
	CWS   Overview	
		~
11	Overview	
	Deployment Plan	
Ma	nage	
11	Properties	
224	Owners	
2.	Roles and administrators (Preview)	
24	Users and groups	
Э	Single sign-on	

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 <b>Default</b> checkbox for it. This is the Entity ID that Cloud Web Sec will present itself as in the SAML <b>AuthnRequest</b> 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 poto. 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 withBEGIN CERTIFICATE and end withENI CERTIFICATE
Section (4) - Azure AD Identifier	This is the SAML <b>entityID</b> 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:

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?	
O None	
All groups	
Security groups	
O Directory roles	
Groups assigned to the application	
Source attribute * Group ID	~
Advanced entions	
Customize the name of the group claim	
Name (required)	
groups	
Namespace (optional)	
Emit groups as role claims ①	

- 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**.

Home > Enterprise applications > CWS > Add Assignment NBarrett Lab AAD	Users ×
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.	nbarrett@vmware.com         Nick Barrett         nbarrett@vmwlabnbarrett.onmicrosoft.com         Selected
	Selected items Nick Barrett nbarrett@vmwlabnbarrett.onmicrosoft.com Remove

#### 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.

vmw Orchestrator	Cloud Web Security 💙		Open Classic Orchestrator
Monitor Configure			
	«		
Policies	Single Sign On	C Enabled	
Enterprise Settings	SAML Server Internet Accessible?	• Yes 🔿 No	
CASB	SAML Provider		×
Certificates	SAML 2.0 Endpoint		
🔇 Authentication	Service Identifier (Issuer)		
-	Enable SAML Verbose Debugging ③ X.509 Certificate	🔿 Yes 💿 No	
	Expires: N/A		
	Additional Certificate		
			DISCARD CHANGES

- 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.

vmw Orchestrator	Cloud Web Security 🗸	Open Classic Orchestrator 🛛 🕐 🛆
Monitor Configure		
	«	
Policies	Single Sign On	Enabled
Enterprise Settings	SAML Server Internet Accessible?	• Yes O No
CASB	SAML Provider	Azure Active Directory
Certificates	SAML 2.0 Endpoint	https://login.microsoftonline.com/300d1c5d-3128-43a9-a36e-b1
Authentication	Service Identifier	https://sts.windows.net/300d1c5d-3128-43a9-a36e-b10ea00b8
A SSL Termination	Domain ()	tlblt.info
	Enable SAML Verbose Debugging ①	• Yes No
	X.509 Certificate	
	Expires: May 9 21:25:11 EDIT CERTIFICATE	2025 GMT

 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.

Certificate Detail		$\times$
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	
✓ Show Certificate		
BEGIN CERTIFIC MIIC8DCCAdigAwle AYDVQQD EyINaWNyb3NvZno TEwMDQxNDUy NDRaEw0vNDEwM	AgIQNxLX9V2cnJRFzBb3afSEujANBgkqhkiG9w0BAQsFADAOMTIwM QgQXp1cmUgRmVkZXJhdGVklFNTTyBDZXJ0aWZpY2F0ZTAeFw0yM DQxNDUvNDRaMDQxMiAwBqNVBAMTKU1pY3Jvc29mdCBBenVvZSB	
	SAV	'E

- 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

vmw Orchestrator	Cloud Web Security 🗸	Open Classic Orchestrator 🛛 🤇	
Monitor Configure			
	≪ Security Policies		
Policies			
Security Policies	Q Search (		
Enterprise Settings			
E DLP	+ NEW POLICY 🖉 EDI	T 🔟 DELETE	0
CASB	Name	Status Modified	Is Published
Inspection Engine	SecurityPolicy1	In Use Jun 30, 2022, 12:58:42 AI	M Yes
Certificates			
🔇 Authentication			
윰 SSL Termination			

#### • On the SSL Inspection tab

ClickAdd Rule

vmw Orchestrator	Cloud Web Security 🗸	Open Classic Orchestra	ator 🖄 ?	Do
Monitor Configure				
	« Security Policies >	> SecurityPolicy1		PUB
Policies	SSL Inspection CASB	DLP Web Security		
Security Policies				
Enterprise Settings	Q Search (	D T		
E DLP				
CASB	+ ADD RULE Ø EDIT	🗓 DELETE 🗍 CLON	E	
Inspection Engine	Name	Source	Destination	Action
Certificates		2000 Apv		- Dupo
🔇 Authentication	Azure SSO By	ass Any	Domains (1)	• Вура
윤 SSL Termination	Default SSL Ins	pection Rule Any	Any	<ul> <li>Inspective</li> </ul>

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

SSL Inspection	Create SSL Exception	×
<ol> <li>Create SSL Exception</li> <li>Name and Tags</li> </ol>	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	
	Destination Type Destination IP E.g. 10.12.13.20 Address Destination From IP address to IP Address	
	IP Range O Destination IP E.g. 10.11.12.13/16 CIDR	
	Destination login.microsoftonline.com     Host/Domain	
	CANCEL	т

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.

r			
SSL Inspection	Name an	d Tags	×
1 Create SSL Exception	Configure Na recommende	me, Tags and Reason for the SSL exceptio d that unique names be used for the Rule r	n rules. It is name. Tags
2 Name and Tags	and Reason o	an 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 🗸	
		CANCEL	FINISH

**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.



# 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.

8 Workspace	e ONE <sup>™</sup> Access					
Dashboard -	Users & Groups Catalog	- Identity &	Access Management	Roles		
Users Groups						
	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 USER
8 Workspace	Ce ONE™ Access Users & Groups Catalog	- Identity ∂	& Access Management	Roles		
Users Groups						
	Groups (1)					
	Group Na	me			Domain	Direc
	ALL USE	RS				

- 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**.

Edit SaaS Application	
1 Definition 2 Configuration 3 Access Policies	Definition Name *
4 Summary	CWS Integration
	SELECT FILE VMware CWS
	CANCEL

- 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	Single Sign-On
2 Configuration	Authentication Type *① SAML 2.0
4 Summary	Configuration * O URL/XML  Manual
	Single Sign-On URL * https://safe-cws-sase.vmware.com/safeview-auth-server/saml
	Recipient URL * ① https://safe-cws-sase.vmware.com/safeview-auth-server/saml
	Application ID * ①
	https://sale-cws-sase.vinware.com/saleview-auti-server/salit/metadata
	CANCEL BACK

Edit SaaS Application	
1 Definition 2 Configuration 3 Access Policies 4 Summary	Username Format • ① Email Address Username Value ① \${user.email} Relay State URL ① Advanced Properties ~ Open in Workspace ONE Web ① Open in Workspace ONE Web ① Open in User Portal ① No Show in User Portal ①
	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}.

Custom Attribute Ma	apping (j		
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	1	
1 Definition	Access Policies	
2 Configuration	Access policies specify the criteria that must manage user access to specific applications t	be met in order to access applications. Select access policies to below.
3 Access Policies	default_access_policy_set	~

7 Click Next and Click Save and Assign.

NEW EDIT	ASSIGN DELETE CATEGORIES -	MORE Y SETTINGS	
Application		Туре	
🗌 👔 AirWatch Admi	n	SAML 2.0	
🗌 💉 VMware CWS		SAML 2.0	

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

NEW	DIT ASSIGN DELETE CATEGORIES	V MORE V SETTINGS
Application		Туре
🗌 🍙 AirW	atch Admin	SAML 2.0
🗆 🔬 VMw	are CWS	SAML 2.0

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.

This XML file does not appear to have any style information associated with it. The document tree is shown below.	
<pre>w<md:entitydescriptor cacheduration="P0Y0M30DT0H0M0.0005" ent<br="" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><script></script> <script></script></md:entitydescriptor></pre>	ityID="https://td-dere
<pre>vstrip://wstri //wstrip:/</pre>	0:protocol">
<pre>w<ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></ds:keyinfo></pre>	
<pre><ds:x509certificate>MIIFLDCCAxSgAwIBAgIGP2i170DDMA0GCSqGSIb3DQEBCwUAME4xIDAeBgNVBAMMF1ZNd2FyZSBJZGV </ds:x509certificate></pre>	/udG10eSBNYW5hZ2VyMR0wG
▼ <md:keydescriptor use="encryption"></md:keydescriptor>	
<pre>w<ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></ds:keyinfo></pre>	
▼ <ds:x509data></ds:x509data>	
<ds:x509certificate>MIIFMjCCAxqgAwIBAgIGP2l0hehlMA0GCSqGSIb3DQEBCwUAMFExIDAeBgNVBAMMF1ZNd2FyZSBJZGV </ds:x509certificate>	/udG10eSBNYW5hZ2VyMSAwH
<pre><md:artifactresolutionservice binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" location="https://t &lt;md:NameIDFormat&gt;urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified&lt;/md:NameIDFormat&gt;&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;erekt-954e0.vidmpreview&lt;br&gt;d-derekt-954e0.vidmprev&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;md:NameIDFormat&gt;urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress&lt;/md:NameIDFormat&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;md:NameIDFormat&gt;urn:oasis:names:tc:SAML:2.0:nameid-format:persistent&lt;/md:NameIDFormat&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;md:NameIDFormat&gt;urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName&lt;/md:NameIDFormat&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;md:SingleSignOnService Binding=" urn:oasis:names:tc:saml:2.0:bindings:http-redirect"="" urn:oasis:names:tc:saml:2.0:bindings:http-redirect_location="https://t&lt;/td&gt;&lt;td&gt;d-derekt-954e0.vidmprev&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/r&gt;&lt;/td&gt;&lt;td&gt;Text-SS4corvionpreview.&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;md:AdditionalMetadataLocation namespace=" urn:oasis:names:tc:saml:2.0:metadata"="">https://td-derekt-954e0.vi </md:artifactresolutionservice></pre>	dmpreview.com/SAAS/API

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.

lobal	толушу аррисация зо шку сан ассерстоуна поти чтоткарасе отче мессаз.	
Approvals	For integrating with other relying applications utilizing SAML 2.0, you can use the metadata URI's below	
Approvais	use the filetaata ones below.	
aaS Apps	SAML Metadata ①	
SAML Metadata	Identity Provider (IdP) metadata 📝 Copy URL	
Application Sources	Service Provider (SP) metadata 📝 Copy URL	
	C=US, O=TD-DEREKT-954E0:SAML, CN=VMware Identity Manager	
	xiDAeBaNVBAMM	
	F1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMR0wGwYDVQQKDBRU	
	PCIERV IESIOTOTI IO	
	RELEVUS SIGLETOD	

12 Assign User Groups to the VMware CWS web application.

Dashb	ard 👻 Users & Groups Catalog 👻 Identity & Access Mana	gement Roles	
	NEW EDIT ASSIGN DELETE CATEGORIES	S 🗸 MORE 🖌   SETTINGS	
	Application	Туре	Ca
	🗌 🝺 AirWatch Admin	SAML 2.0	
	🗹 👱 VMware CWS	SAML 2.0	

elected App(s): VMware CWS							
ers / User Groups Q. All User							
elected Users / User Groups	Deployment Type		Entitlement Type		Provisioning Status	Retry	
8_ test@ws3globalcorp.com	Automatic	~	Include	~			
중 ALL USERS	User-Activated	~	Include	~			

# 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.

vmw Orchestrator	Cloud Web Security 🗸	Open Classic Orchestrator
Monitor Configure		
	«	
Policies	Single Sign On	Enabled
Enterprise Settings	SAML Server Internet Accessible?	• Yes O No
CASB	SAML Provider	~
Certificates	SAML 2.0 Endpoint	
& Authentication	Service Identifier (Issuer)	
음 SSL Termination	Enable SAML Verbose Debugging () X.509 Certificate	O Yes O No
	Expires: N/A	
	Additional Certificate	
		DISCARD CHANGES

- 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

vmw Orchestrator c	loud Web Security 🗸		Open Classic Orchestrator
Monitor Configure			
*			
Policies	Single Sign On	Enabled	
Enterprise Settings	SAML Server Internet Accessible?	• Yes 🔿 No	
CASB	SAML Provider	Workspace ONE Access	~
lnspection Engine	SAML 2.0 Endpoint	https://td-derekt-945e0	
🔇 Authentication	Service Identifier (Issuer)	https://td-derekt-954e0	
윤 SSL Termination	Enable SAML Verbose Debugging ① X.509 Certificate	🔵 Yes 💿 No	
	Expires: N/A ADD CERTIFICATE		
	Additional Certificate		
			DISCARD 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	Name and T	Fags			
1 Create SSL Exception	Configure Name, names be used fo	Tags and Reason for the or the Rule name. Tags an	SSL exception d Reason can k	rules. It is recon be used for sort	nmended
2 Name and Tags					
	Rule				
	Name	SSL Bypass for WS1 A	Access		
	Tags	e.g. tag1, tag2, tag3			
	Reason	SSL Bypass for WS1 A	Access		
	Position	Top of List	~		
				CANCEL	BAC

vmw Orchestrator ci	oud Web Security 🗸 🗸	Open Classic Orchestrator
Monitor Configure		
~	Security Policies > SecurityPo	licy1
Policies	SSL Inspection CASB DLP	Web Security
Security Policies	Q Search	
CASB	+ ADD RULE う EDIT 前 DELETE 〔	] CLONE
☐ Inspection Engine	Name	Source Destination
Certificates	SSL Bypass for WS1 Access	Any Domains (1)
음 SSL Termination	Default SSL Inspection Rule	Any Any

**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	Cle	oud Web Security 🗸 🗸			Open Classi	c Orchestrate
Monitor Configure						
	$\ll$	Security Policies	> SecurityPo	licy1		
Policies		SSL Inspection CA	SB DLP	Web Security		
Security Policies						
Enterprise Settings		URL Filtering	Content Filtering	Conte	nt Inspection	
CASB		Q Search	() <b>T</b>			
Certificates		+ add rule 5 edi	T 🗍 DELETE 🌔	] CLONE		
A SSI Termination		Name Name	Ba	ased On	Source	Destination
E SSE Fernindion		Block All Twi	tter Do	omains	Any	Domains ( 1
		Default Dom	ain Rule Do	omains	Any	All Domain:
		Default Three	at Rule Th	nreats	Any	All Threats
		Default Cate	gory Rule Ca	ategories	Any	All Categor

URL Filtering	Based On	
<ol> <li>Based On</li> <li>Select Source And Destination</li> <li>Action</li> <li>Name, Reasons and Tags</li> </ol>	Manage access to various websites using Web categories, Addresses, IP ranges FQDNs, CIDR notations). Control access to certain website based on Type Domain $\checkmark$	Threat categories or Domains Brief Descriptio 1. URL Filtering Website Categories set p entire category of the web 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	Select Source And Destination			
1 Based On	Apply this exception to all user select the Destination domains	s and groups (Source) or limit the exception to a particula based on IP,IP Ranges, FQDNs, CIDR notations.		
2 Select Source And Destination	Source			
3 Action	All Users and Groups			
	Specify User(s)	e.g. User1, User2		
4 Name, Reasons and Tags	Specify Group(s)	ws1a-users@w 🛞 all users 🛞		
	Destinations	(twitter.com (X))		
	Specify Domains			
		CANC		

#### Check the Web Logs under Cloud Web Security > Monitor > Web Logs
vmw Orchestrator	a	oud Web Security 🗸 🗸						
Monitor Configure								
	~	Web Logs						
Monitor								
O Threat Analysis								
Traffic Analysis		User ID	URL		Categories	Threat Types	Request Type	A
Logs		test@ws3globalcorp.c	om https://www.twitte	er.com/	Categories (1)		Page Request	В
🕮 Web Logs		Unknown	https://unagi.amai	zon.com/1/eve	Categories (1)		File Upload	A
		test@ws3globalcorp.c	om https://s.amazon-a	adsystem.com/	Categories (1)		Page Request	A
		test@ws3globalcorp.c	om https://s.amazon-i	adsystem.com/	Categories (1)		Page Request	A
		test@ws3globalcorp.c	om https://www.amaz	ton.com/	Categories (1)		Page Request	A
		O Unknown	https://safebrows	ing.googleapi	Categories (1)		Page Request	A
		C REFRES	н					
				Log	Entry Details	test@ws3g	lobalcorp.	.com
		Summary						
		User ID	test@ws3globalcorp.com	m		Date	Jun	1 30, 20
		Domain	www.twitter.com			URL	http	ps://ww
		Web Risk Score	• Low			Catego	ries Soc	cial Net
		Action	Block					
		Browser Type	Chrome			User-Ag	jent Moz	zilla/5.0 pleWeb
$\bigcirc$		Browser Version	91				Chr	rome/9