

VMware Cloud Web Security Release Notes

VMware Cloud Web Security

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

<https://docs.vmware.com/>

VMware by Broadcom

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

Copyright © 2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. [Copyright and trademark information](#).

Contents

1	Introduction	4
2	Important Changes to Cloud Web Security	5
3	Overview	6
4	New Features and Resolved Issues	7
	v1.18.1	7
	v1.17.0	8
	v1.16.0	11
	v1.15.2	14
	v1.15.1	15
	v.1.14.1	17
	v1.14.0	17
	v1.12.1	20
	v1.12.0	20
	v1.11.1	22
	v1.11.0	25
	v1.10.1	27
	v1.10.0	28
	v1.9.1	30
	v1.8.0	32
	v1.7.0	34
	v1.6.1	35
	v1.5.2	36
	v1.5.1	36
	v1.5.0	38
5	Known Issues	41

Introduction

1

VMware Cloud Web Security | **06 June 2024**

Check for additions and updates to these release notes.

Important Changes to Cloud Web Security

2

Important VMware Cloud Web Security service is being re-architected to feature the strength of the Symantec Enterprise Cloud. As part of this re-architecting, Cloud Web Security customers should transition by August 31, 2024. If you are currently using this service please promptly contact your VMware sales representative to review alternate service options available to you.

Overview

3

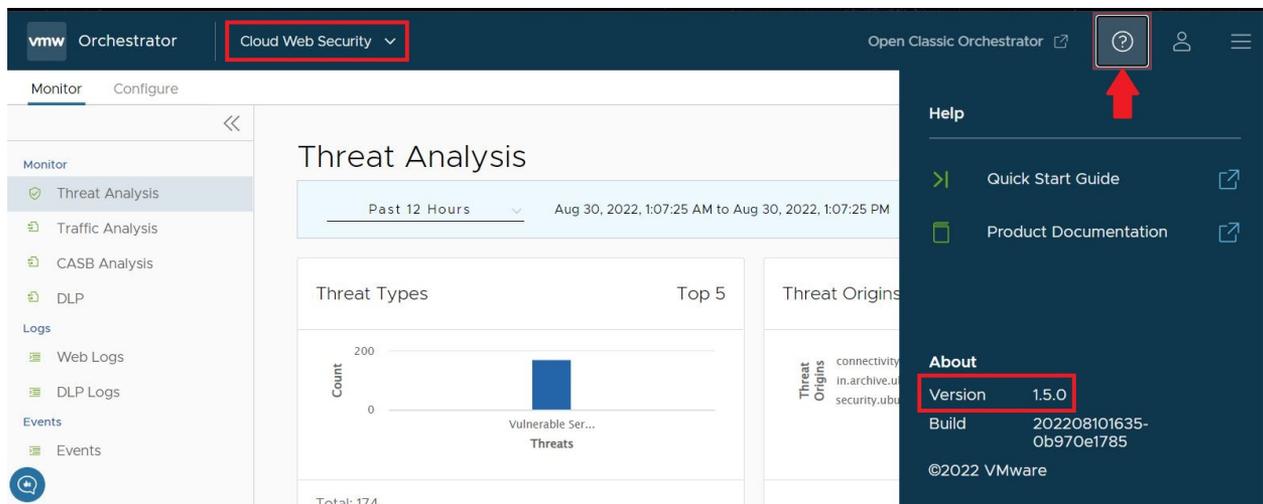
VMware Cloud Web Security™ is part of the VMware SASE™ solution and is a cloud hosted service that protects users and infrastructure accessing SaaS and Internet applications from a changing landscape of internal and external threats, offers visibility and control, and ensures compliance.

The Cloud Web Security Release Notes documents both resolved and known Cloud Web Security issues as well as new features and enhancements. Where previously this material was documented in the VMware SASE Release Notes, it will be exclusively documented here going forward. Cloud Web Security issues include those caused by a defect in the VMware SASE Orchestrator UI and those caused by a defect in the Cloud Web Security service itself.

Cloud Web Security follows a versioning system different from VMware SD-WAN and should be understood as separate from SD-WAN or the SASE Orchestrator.

The Cloud Web Security version for a customer deployment is found on the Orchestrator by first selecting the **Cloud Web Security** screen, and then clicking the (?) icon to open the **Help** menu. The Cloud Web Security version is displayed at the bottom of the **Help** menu.

Figure 3-1. Cloud Web Security Version Location



New Features and Resolved Issues

4

Read the following topics next:

- [v1.18.1](#)
- [v1.17.0](#)
- [v1.16.0](#)
- [v1.15.2](#)
- [v1.15.1](#)
- [v.1.14.1](#)
- [v1.14.0](#)
- [v1.12.1](#)
- [v1.12.0](#)
- [v1.11.1](#)
- [v1.11.0](#)
- [v1.10.1](#)
- [v1.10.0](#)
- [v1.9.1](#)
- [v1.8.0](#)
- [v1.7.0](#)
- [v1.6.1](#)
- [v1.5.2](#)
- [v1.5.1](#)
- [v1.5.0](#)

v1.18.1

Cloud Web Security version **1.18.1** was released on **01 February, 2024**.

This version adds one new enhancement as well as resolving three issues.

The new enhancement added, and issues resolved in Cloud Web Security version 1.18.1:

- **New Enhancement: Custom File Types for Web Application Rules**

Web application rules to block **All File Types** only block pre-defined file types and do not block custom file extensions and MIME types.

This enhancement enables users to add custom file extensions and MIME types to their Web Application Rules to ensure complete coverage.

- **Fixed Issue 133873: The tooltip on "Enable Verbose Debugging" is not explicit about what will happen if a user saves or does not save.**

Currently, the tooltip on "Enable Verbose Debugging" always displays a time 2 hours in the future for when the feature will be turned off, and does not display an explicit expiry time and what the expiration time would be on saving.

- **Fixed Issue 134090: Rules and Objects can become invalid if updated with invalid contents via API.**

When updating Rules, DLP Auditors, and DLP Dictionaries via the Cloud Web Security API, issuing a PATCH API request may not always enforce the same validation used for creation requests, resulting in the possibility of invalid data. This issue is only encountered when using an API and updates work as expected when using the Orchestrator UI.

- **Fixed Issue 134091: The CWS Orchestrator UI does not prevent a user from entering and saving duplicate entries for common fields for rules or settings.**

Duplicate entries for common fields like user, group, tag, and domain can sometimes be saved. The user would only realize there is an issue when they attempt to publish the rule or setting and trigger an error message "schema validation error", except there is no wording for what the real cause of the error is.

The fix includes validation for duplicate entries that prevents a user from saving the rule or setting with a clear error message.

v1.17.0

Cloud Web Security version **1.17.0** was released on **10 January, 2024**.

This version adds one new feature as well as resolving two issues.

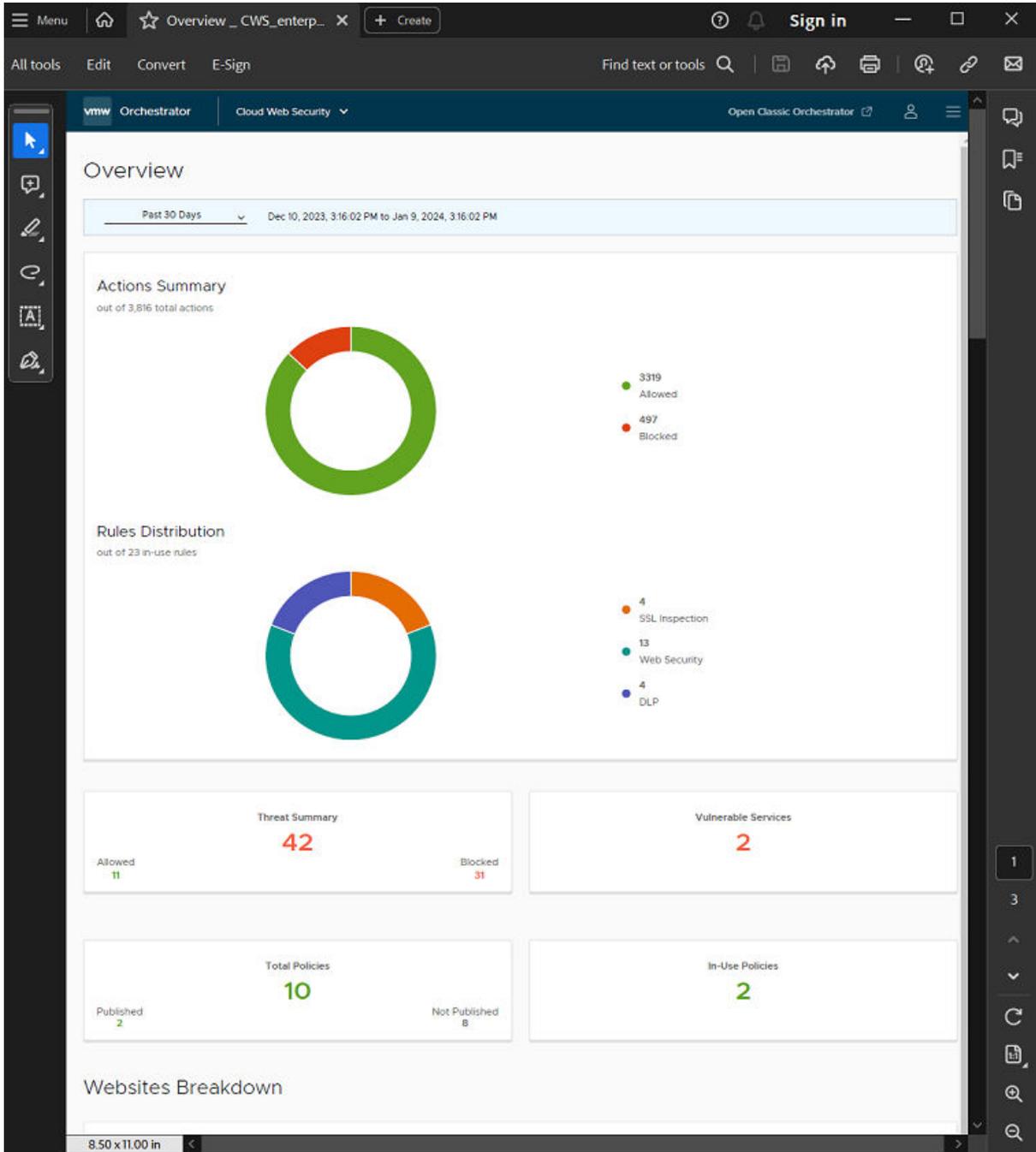
The new feature added, and issues resolved in Cloud Web Security version 1.17.0:

- **New Feature: Printable Overview Page**

Release 1.17.0 improves the **Overview** page to automatically format for printing.

Note To get a PDF report of the **Overview**, initiate a *Print* in your browser and select “*Save as PDF*” (or similar, depending on your browser and operating system).

Below is an example report opened in an Adobe Acrobat reader:



Caution The Mozilla Firefox browser may have issues displaying graphs in the printed output. If you run into issues, try printing from another browser (for example, Safari, Microsoft Edge, Google Chrome, or any other Chromium-based browser).

- **Fixed Issue 131353:** Some wizards or forms can be submitted multiple times if the 'Submit' button is clicked while a submission is already in progress, which may lead to unexpected rule data or errors.

On **CASB**, **Web Application**, and **DLP** rule wizards; and on **SaaS Header Exceptions**, and **Corporate Gateway IPs** pages, a form can be submitted multiple times if the **Submit** button is clicked rapidly while a submission is already in progress. The effect is more noticeable with slow network connectivity.

- **Fixed Issue 134198: When attempting to download an SSL Certificate Description, a user may observe instead a new browser tab open with the error "401 Authorization Required".**

The issue can be observed when a user goes to **Cloud Web Security > Configure > SSL Certificate**, and then clicks either of the **Download Certificate** buttons on this page.

v1.16.0

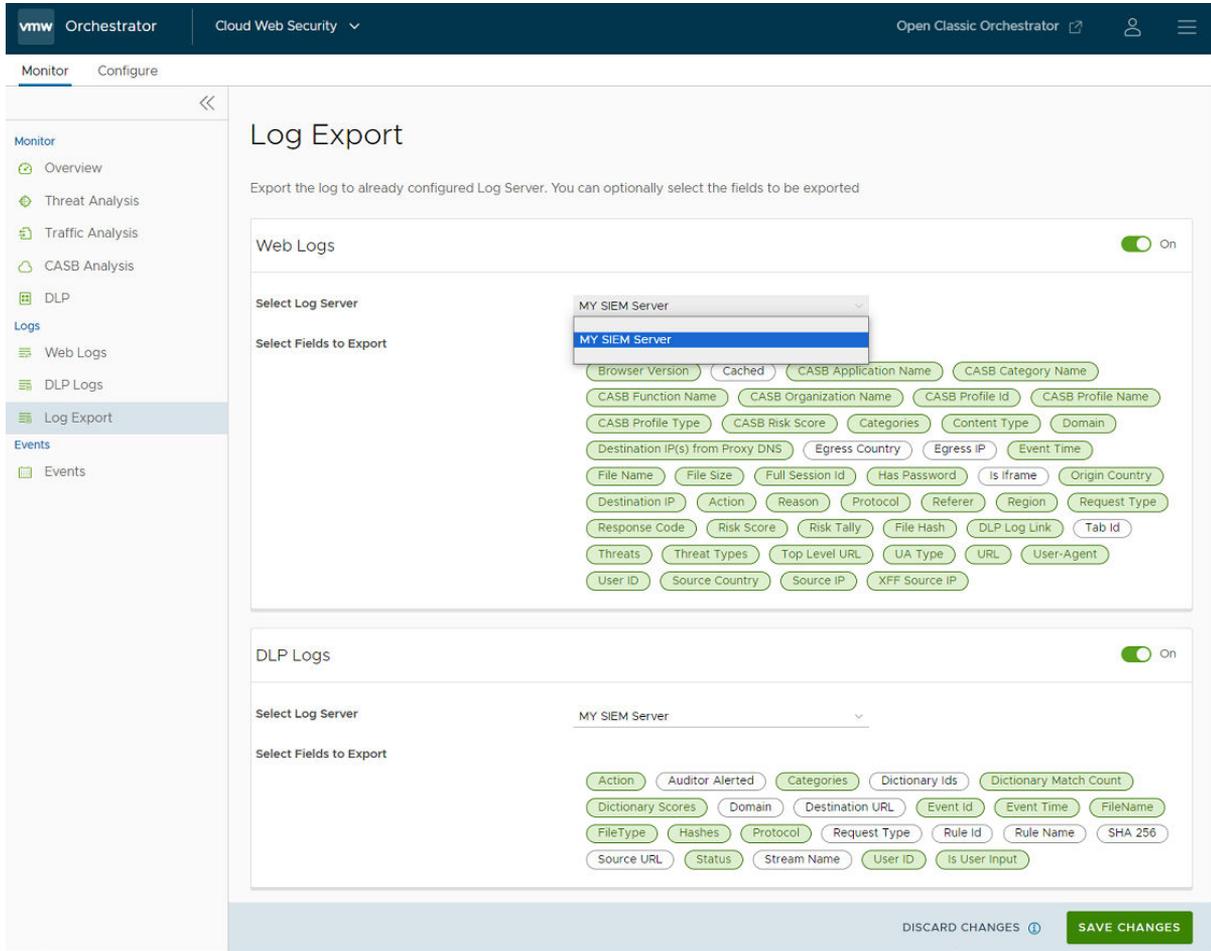
Cloud Web Security version **1.16.0** was released on **14 December, 2023**.

This version adds two new features as well as resolving one issue.

The new features added, and issue resolved in Cloud Web Security version 1.16.0:

- **New Feature: Log Export**

The **Log Export** feature enables a customer to forward near-realtime logs about Cloud Web Security activities to a customer-controlled SIEM (Security information and event management) endpoint for storage and analysis.

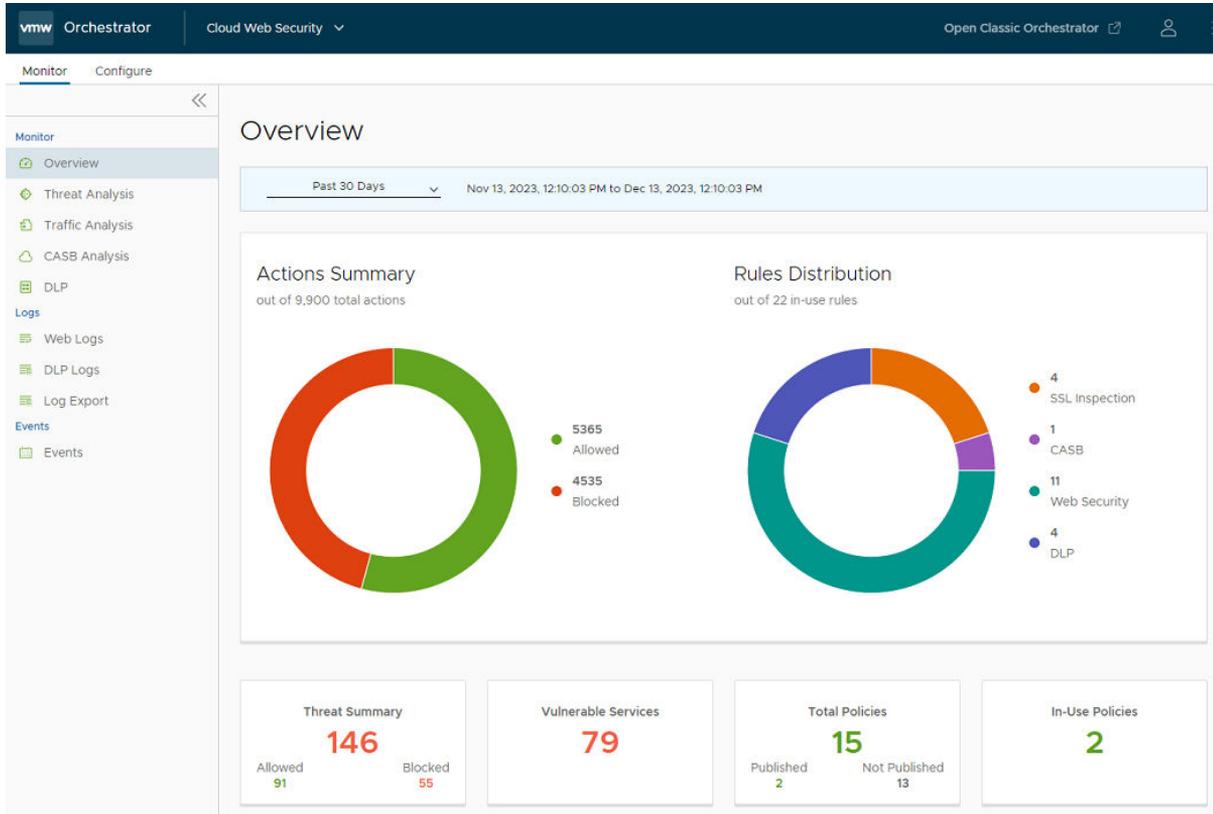


For more information, see the [Log Export](#) section in the Cloud Web Security documentation.

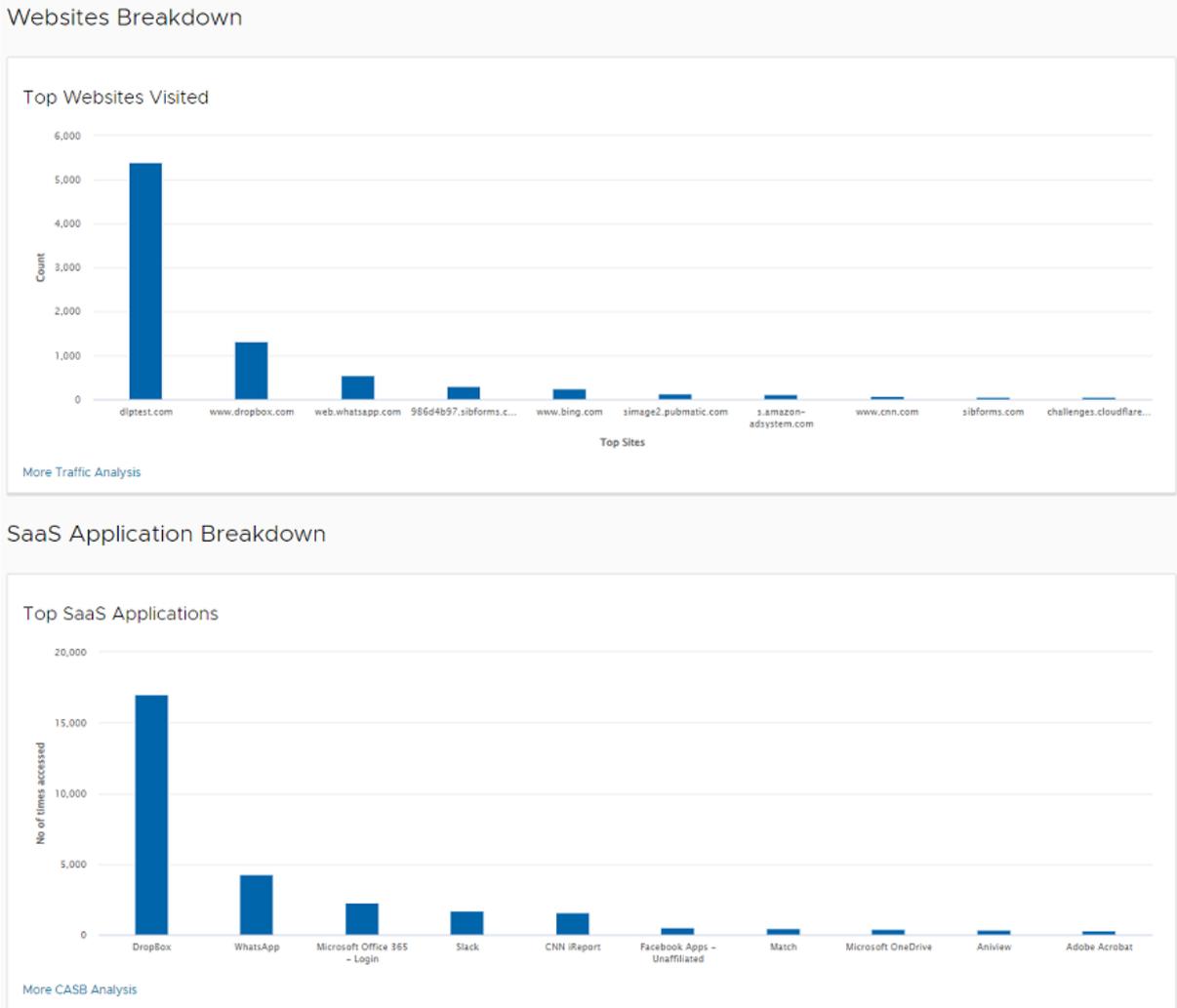
Note The **Log Export** feature is activated on a limited number of Orchestrator's at the time of this release. VMware will continue to roll this feature out over the next three weeks to additional Orchestrators.

■ **New Feature: Monitoring Overview Page**

Cloud Web Security introduces a new **Monitor > Overview** page. This dashboard presents a cleaner, more accessible presentation of critical information on a single page, while also pointing the user to more detailed information for each data category. The top graphs provide a user with the Cloud Web Security **Actions Taken** over the configured time period and the current **Rules Distribution** for that customer.



In addition, a user can scroll further and see at-a-glance graphs for **Top Websites Visited**, **Top SaaS Applications**, **Threat Breakdown**, and **User Breakdown**.



- **Fixed Issue 132528:** A user trying to paste in a list of comma-separated items into a multi-item input field may find that Cloud Web Security treats this effort as a single item and does not respect the comma separators.

Adding comma-separated lists is a common time-saving practice when configuring tags, domains, email addresses, and similar items where a multi-item input field is used. With this issue, the commas are ignored by the UI and the list yields only one item. For example, if pasting in a list of tags for a Web Security rule, the result is just a single tag.

v1.15.2

Cloud Web Security version **1.15.2** was released on **14 November, 2023**.

Issues resolved in Cloud Web Security version 1.15.2:

- **Fixed Issue 114373:** Multi-item input fields in the Cloud Web Security UI does not allow keyboard focus or interaction.

When adding selections to various lists and tags in the CWS UI, multi-item input fields do not allow keyboard focus or manipulation. This is often used for inputting tags, domains, email addresses, or other similar items.

- **Fixed Issue 114379: On the Cloud Web Security UI, some multi-item dropdown fields in the DLP Rule Wizard cannot be focused and are not interactive via the keyboard.**

For example, on the **Select Destinations** screen, navigating within this screen and selecting multiple **Categories** cannot be done using the keyboard.

- **Fixed Issue 128108: URL Filtering rules will sometimes lose their contents and become blank.**

When editing a **URL Filtering** rule, rapidly clicking *Update* on the final step multiple times can result in the rule's contents being corrupted. Once corrupted, the user would need to recreate the rule and its contents.

- **Fixed Issue 128782: Policy action in the Content Inspection wizard reverts to "Mark As Clean" when selected file types are changed.**

The UI should only reset the policy action in **Content Inspection** when a user switches the category type between **File Type** and **File Hash**. But if a user changes the type of files to **Inspect**, the UI also resets the policy action and the user must manually reset the policy action back to its intended value.

- **Fixed Issue 129269: SAML verbose debugging cannot be turned off once it is turned on.**

When a user turns on SAML verbose debugging, it cannot be turned off. In addition, 2 hours after enabling verbose debugging, the state should automatically be set to *disabled/No* but remains *enabled/yes*.

- **Fixed Issue 130111: If a user performs an invalid action on the Cloud Web Security UI, the UI does not return an error message to let the user know their action was invalid.**

For example, if the user tries to add the same corporate Gateway a second time, this action triggers an error by the API, but the UI fails to display the error notification.

v1.15.1

Cloud Web Security version **1.15.1** was released on **01 November, 2023**.

Issues resolved in Cloud Web Security version 1.15.1:

- **Fixed Issue 114363: A user may find it difficult to navigate in the Cloud Web Security UI when using only keyboard navigation.**

When a user relies on keyboard navigation on the UI, it is difficult to focus or scroll on signpost content that pops up.

- **Fixed Issue 123063: CASB application icons do not load on the VMware SASE Orchestrator UI.**

CASB application icons do not load in CASB Rule configuration dialog and on the CASB Applications page of the UI.

- **Fixed Issue 123816: Destination domains are not displayed in the Web Applications rules grid on the Orchestrator UI.**

Destination domains are not displayed in the Web Applications rules grid, and instead the user sees "Any".

- **Fixed Issue 125526: When creating a Web Application rule, if a user selects a request type "Download", they do not see a file types option menu.**

The user only observes file types selection menus for "Uploads" and "Uploads and Downloads" options, these file types options are hidden for the "Download" type.

- **Fixed Issue 126051: The default, non-editable Content Inspection Rule shows "Mark as Clean" as the default behavior.**

Every Cloud Web Security policy begins with a set of non-editable rules that show the default behavior. While this is usually "Allow", in the case of Content Inspection, the default behavior should be "Inspect", not "Mark as Clean".

- **Fixed Issue 126264: Attempts to move or reorder Cloud Web Security rules on the second page or later of the Orchestrator UI does not work as expected.**

With more than 21 policy rules added, an attempt to reorder rules on the second or later page via drag and drop, OR an attempt to move a rule from the second or later page to the first page fails.

In addition, when a user is on the second or higher page of: **SaaS Header**, **CASB**, **DLP**, **Web Application**, or **Web Security** rules, if they attempt to move one or more rules, the rules will temporarily appear correctly reordered, but have the original order after refresh.

A user can workaroud this issue for a single rule they wish to move to the first page by deleting it and re-adding it, specifying "top of list" or "bottom of list" on the final rule creation wizard page; or for reordering a rule list use an API call instead of the Orchestrator UI.

- **Fixed Issue 127646: When selecting CASB controls for Instagram, the "Search" control may be unexpectedly toggled off and can be difficult to restore.**

The only way to restore the Search control for CASB controls is to select "Block" under "Browser Action" to switch all the toggles off. Then, toggle "Block" again to allow all Instagram rules. This will restore the "Search" control when toggling individual controls does not work.

v.1.14.1

Cloud Web Security version **1.14.1** was released on **11 July, 2023**.

Issues resolved in Cloud Web Security version 1.14.1:

- **Fixed Issue 113256: Items for several rule and configuration tables in Cloud Web Security are not selectable or interactive via keyboard navigation.**

On a security policy rules screen (for example, **SSL Inspection**), when using the Tab key to focus the name of an existing rule, the browser's focus skips over the rule name, and the only way to select times is to use a mouse/touchpad.

- **Fixed Issue 114409: Users may find it difficult to navigate between UI screens because there no explicit identification of a "main" section of the page, making it more difficult to jump past the header and navigation.**

Using a screen reader or accessibility tool, the user would be challenged to identify the part of the page with the role "main" because there are no headers or banners that point to it.

- **Fixed Issue 114438: Navigating the Cloud Web Security UI using the side menus is difficult via keyboard or a screen reader. In addition, users cannot open links from the side navigation menu into new tabs or browser windows.**

When using a screen reader or accessibility tool to focus on items in the left navigation, the resulting captions are muddled and had superfluous announcements.

v1.14.0

Cloud Web Security version **1.14.0** was released on **06 June, 2023**.

This version adds a new feature as well as resolving several issues.

The new feature added, and issue resolved in Cloud Web Security version 1.14.0:

- **New Feature: Time-Based Policies for a URL Filtering Rule with the Schedule feature.**

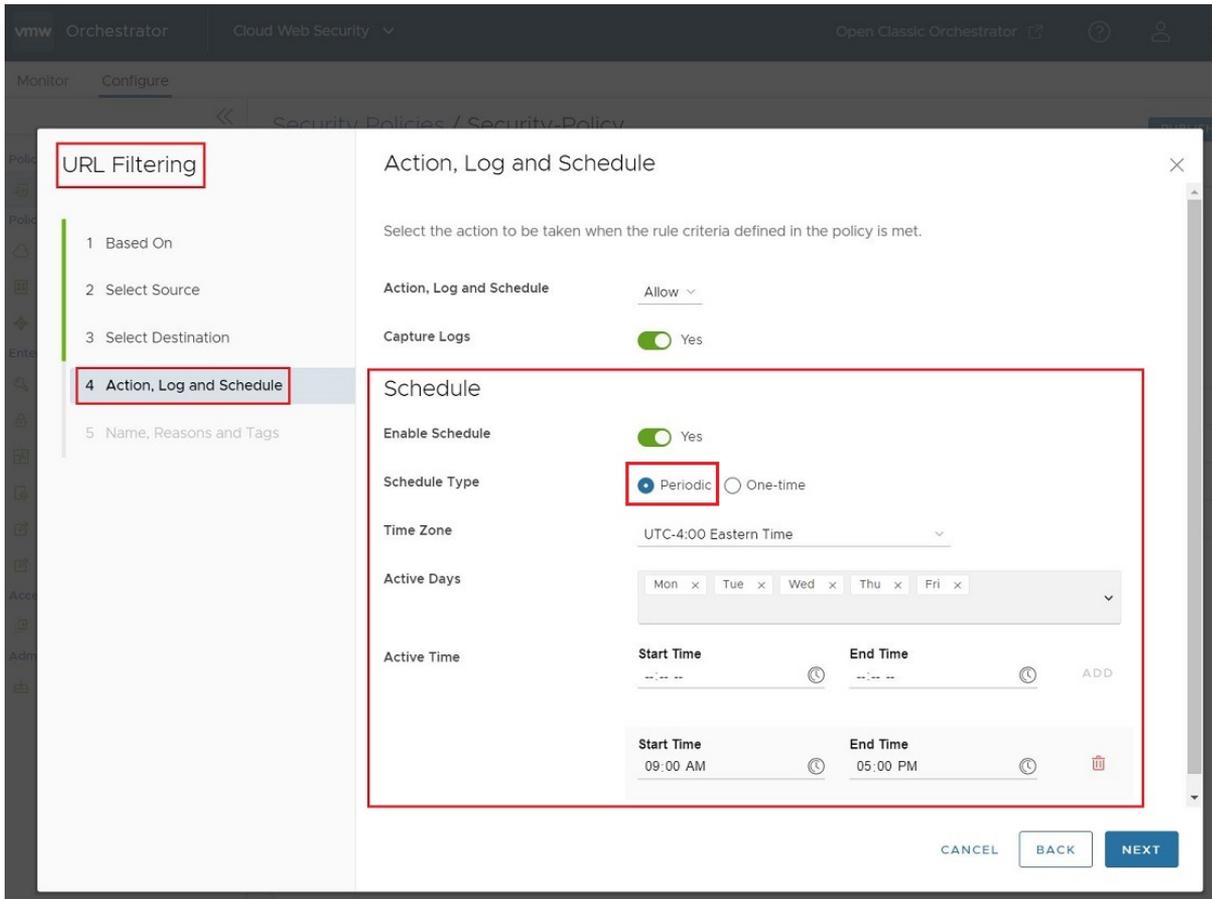
Cloud Web Security now provides you with the ability to apply some **URL Filtering** rules only within specified time periods using the **Schedule** feature. This feature is added to the **Action, Log and Schedule** section when configuring a Web Security Rule with a **URL Filtering** type.

Note The **Schedule** feature is available for **URL Filtering** rules where the **Based On** type is either **Website Categories** or **Domain > Static Domain List**.

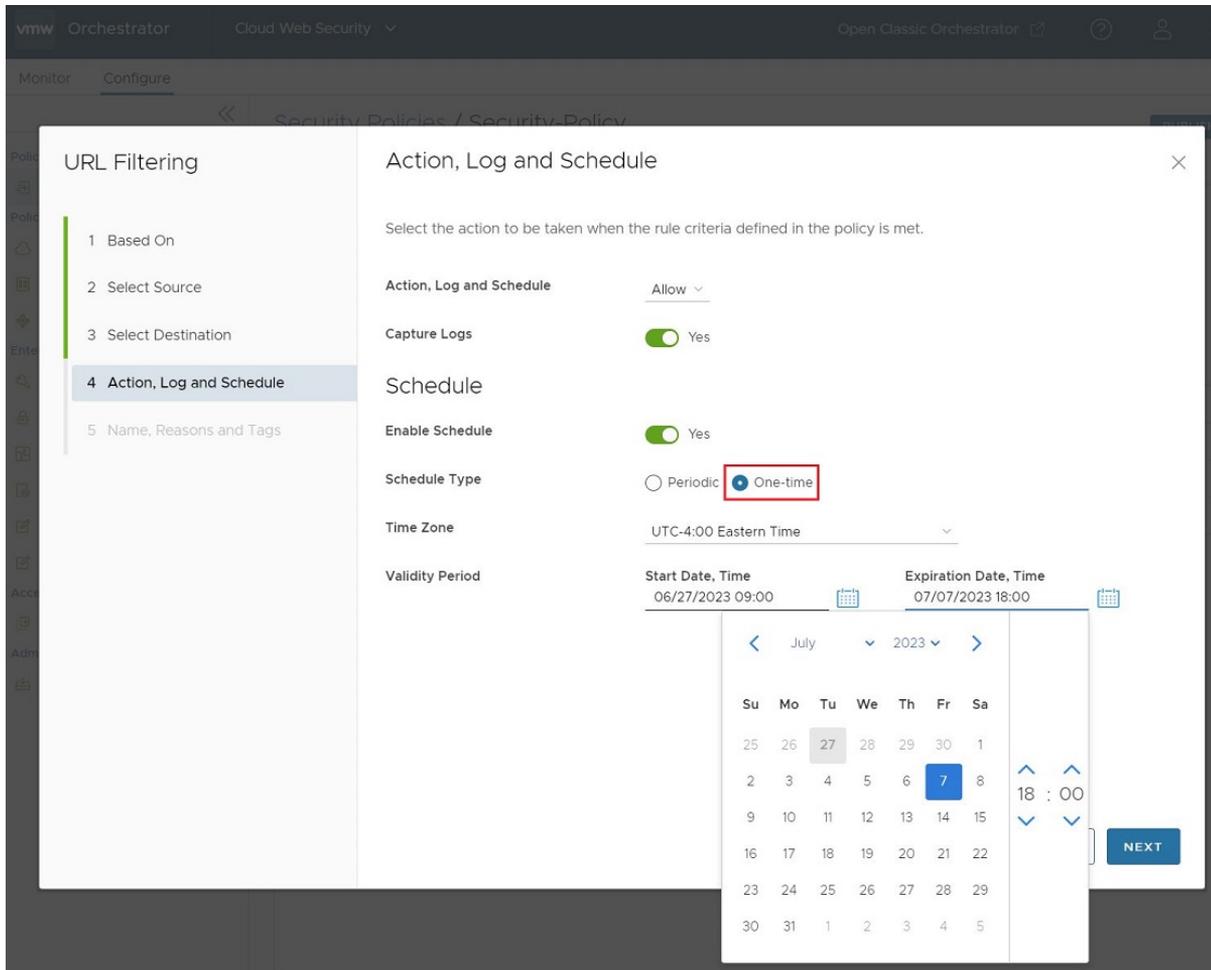
Schedule is not available for **Based On** type **Threat Categories** or **Domain > Dynamic Domain List**, and in those instances the toggle button to activate this feature is inaccessible.

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

The **Periodic** option allows you to configure a weekly, rotating schedule for when your URL Filtering Rule is active. This periodic schedule is based on a global time zone, days of the week, and one or more starting and ending time periods.



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



For more information, see the [Configure Security Policy > Configure Web Security Rules > URL Filtering](#) documentation in the Cloud Web Security Guide

- Fixed Issue 105290: When attempting to publish a Security Rule when two SSL Inspection rules shared the same source or destination domain, IP, CIDRs, or IP Ranges, a non-specific "schema validation error" appears.**

This issue would also occur if two destination domains were duplicated within the same rule. The error is vague and provides no help to the user in terms of troubleshooting the configuration issue that prevents rule validation. A user could only look inside the SSL Inspection rules for duplicate domains, IPs, CIDRs, or IP Ranges (including the contents of Quick Exception Rules), and remove them from all but one rule. Now, an error will describe which sources or destinations are conflicting, or if there are duplicates within a rule itself.

- Fixed Issue 116525: When editing or creating URL Filtering, SaaS Header exceptions, and Geo-Filtering rules that already contain custom Source > Users or Groups, selecting "All Users and Groups" in the Source tab does not clear out the prior custom list of Users and Groups from the underlying rule, and this may result in validation errors when the Security Policy is published.**

Cloud Web Security was not clearing away the manually configured Users and/or Groups and the only way to correct this was to uncheck "All Users and Groups", and then manually remove all Users and Groups, and then re-check "All Users and Groups".

v1.12.1

Cloud Web Security version **1.12.1** was released on **22 May, 2023**.

Issues resolved in Cloud Web Security version 1.12.1:

- **Fixed Issue 63489: Cloud Web Security does not alert a user that they are configuring an SSL Rule with an invalid IP address, IP CIDR, or Domain field prior to saving the rule.**

An SSL Rule with an invalid rule is rejected when the user attempts to save it. The issue is that the user should not have to get that far into the process to discover an SSL Rule IP address, IP CIDR or Domain is invalid. The Orchestrator should alert the user during the SSL Rule editing step using the SSL Rule wizard.

- **Fixed Issue 98213: User attempts to filter the Data Loss Prevention (DLP) Dictionary or the DLP Auditor pages using localized text (non-English) do not succeed.**

Filters on DLP Dictionary and DLP Auditors were not localized for non-English languages. With this fix, the string filters have been upgraded to checkbox filters which not only fix localization language issues, but also make it easier for users to filter these two sections.

v1.12.0

Cloud Web Security version **1.12.0** was released on **05 May, 2023**.

This version adds a new feature as well as resolving several issues.

The new feature added, and issue resolved in Cloud Web Security version 1.12.0:

- **New Feature: URL Filtering Using Dynamic Domain Lists**

Previously when a user was configuring a Web Security Rule which included a URL Filtering Rule, the customer had only one option when they wanted to filter by domains: a **Static Domain List** they had to manually configure and maintain on the Orchestrator UI. In the case of a large number of domains or where that list changed frequently, this option was not ideal. Beginning with Release v1.12.0, the customer now has an additional option when filtering for domains: a **Dynamic Domain List**.

URL Filtering

- Based On
- Select Source
- Select Destination**
- Action
- Name, Reasons and Tags

Select Destination

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

Domain

Static Domain List

Dynamic Domain List

List Name Malware Domain List
unique name to identify the file

Source URL <https://raw.githubusercontent.com/opensns/public-...> VALIDATE URL

Valid domains: 10,000
Valid IP ranges: 0
Invalid domains: 0

Update Frequency

- Every 5 minutes
- Every 5 minutes**
- Every 30 minutes
- Hourly
- Daily

CANCEL BACK NEXT

For this option Cloud Web Security references a text list of FQDN formatted domains which is stored remotely at a location of the customer's choosing. The location must be publicly accessible to the service. The advantage of this option is that you can make a domain list with a large number of domains and that can be edited and updated easily. Cloud Web Security can be configured to check the Dynamic Domain List at intervals from every 30 seconds up to every 24 hours.

Note While a **Static Domain List** allows domains in a variety of formats (IP Address, IP Address Ranges, FQDNs, or CIDR notations), the **Dynamic Domain List** has a limitation that it can only be created with FQDN formatted domains.

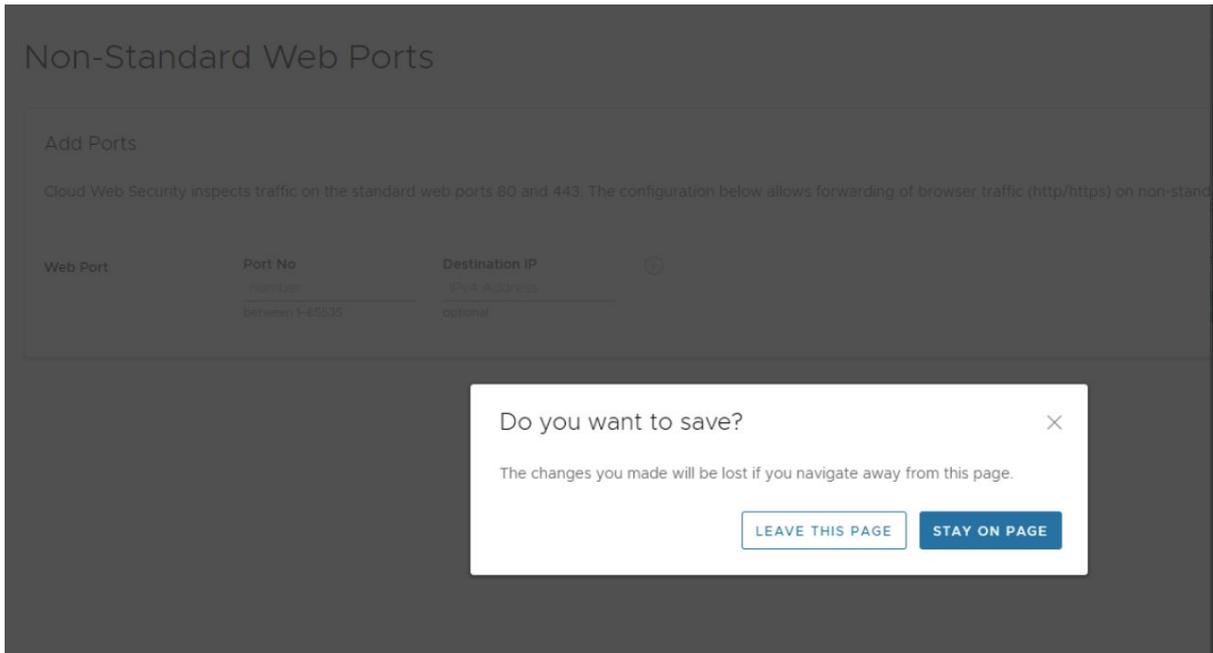
For more information, see the documentation for [Configuring Web Security Rules > URL Filtering](#) in the **VMware Cloud Web Security Configuration Guide**.

- **Fixed Issue 115178: A Cloud Web Security customer with a Standard License cannot access the SaaS Header Restrictions feature.**

The **SaaS Header Restrictions** feature should be useable by all Cloud Web Security customers but when a user under a Standard License clicks on the **SaaS Header Restrictions** link, they are led to the **Content Inspection** page instead of the intended page. This issue does not occur for users under an Advanced License.

- **Fixed Issue 112990: If a user is on the Non-Standard Web Ports page and then navigates away without changing anything, they are still prompted with a "Do you want to save?" screen.**

Even though nothing has changed, the Orchestrator UI still prompts the customer as to whether they want to save changes which can result in unnecessary confusion for the user.



v1.11.1

Cloud Web Security version 1.11.1 was released on **11 April, 2023**.

This version adds a new feature as well as resolving several issues.

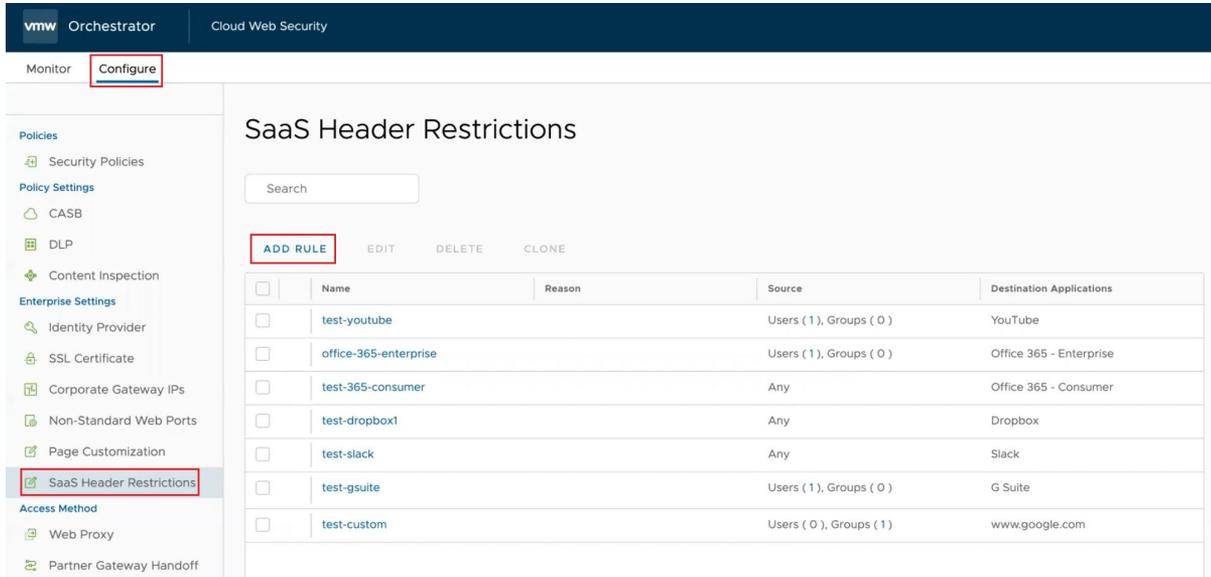
The new feature added, and issue resolved in Cloud Web Security version 1.11.1:

- **New Feature: SaaS Header Restriction**

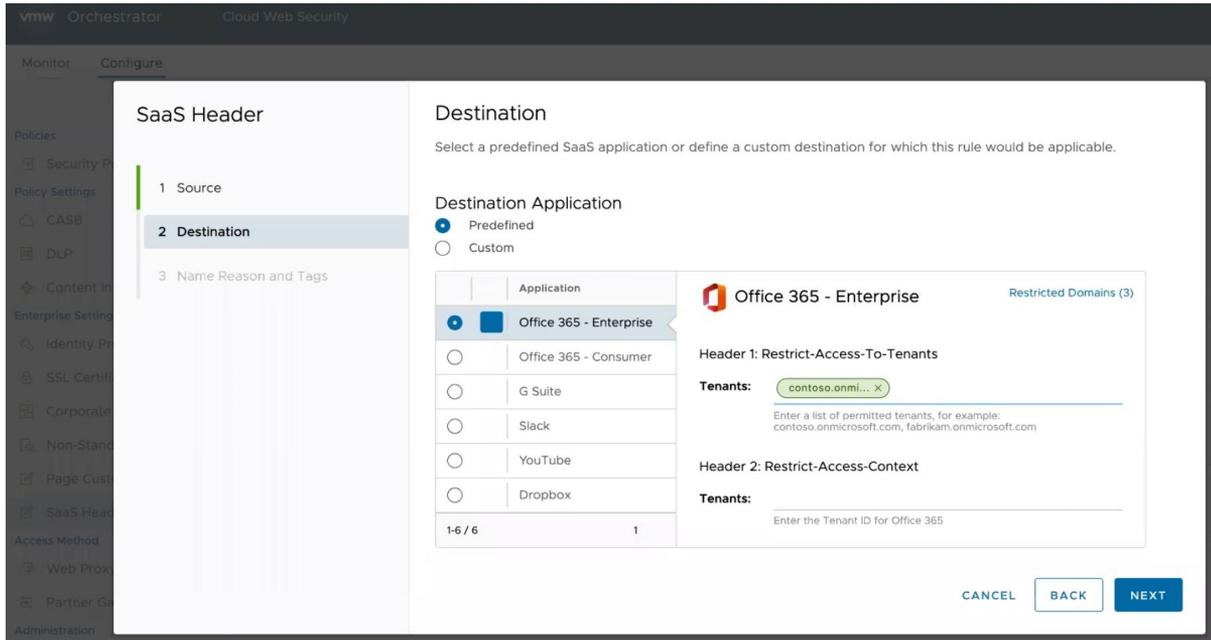
Traditionally, companies restrict domain names or IP addresses when they want to manage access. This approach fails in a world where software as a service (SaaS) applications are hosted in a public cloud and running on shared domain names. For example if a business uses Office 365, they would be working with domain names like outlook.office.com and login.microsoftonline.com. In the Microsoft example, blocking these addresses would keep users from accessing Outlook on the web entirely, instead of merely restricting them to approved identities and resources.

The solution to this problem is to restrict tenant access, and Cloud Web Security accomplishes this through the use of the **SaaS Header Restriction** feature. This feature allows administrators to enforce tenant restriction policies within SaaS services like Office 365 and G Suite. For example, you may wish to allow access to the Office 365 corporate account for all employees but forbid them from accessing personal accounts. These restrictions are allowed via insertion of HTTP headers which specify allowed tenants.

This feature is added to the **Cloud Web Security > Configure** page under **Enterprise Settings**:



A customer can configure the SaaS Header rule selecting from one of six predefined applications: Office 365 - Enterprise, Office 365 - Consumer, G Suite, Slack, YouTube, and Dropbox. Each of these predefined applications include a varying level of detail like restricted domains and headers. Depending on the application, the customer may need to provide additional inputs to complete the rule.



The customer can also create a custom application assuming the application supports tenant restriction through headers.

- **Fixed Issue 79906:** In some languages, the left-hand navigation contains items with erroneously capitalized words.

For example, the menu term **Security Policies** is translated and displayed as **Directivas De Seguridad** when it should display as **Directivas de seguridad**. In effect, if an English menu item is a single word and the translated item is multiple words, the Orchestrator is capitalizing each additional word when it is correct to leave the additional words uncapitalized.

- **Fixed Issue 91672: When a user makes a change on either the Configure > Content Inspection or the Configure > Corporate Gateways pages, the unsaved changes footer prompt may obscure other content on the page.**

The UI does not account for the unsaved changes footers height and scroll on a smaller web browser and this footer obscures other content on those respective pages.

- **Fixed Issue 102793: The DLP tab appears to the left of Web Security, implying that DLP processing happens prior to Web Security rules.**

The customer can get the mistaken impression that DLP processing precedes Web Security rule processing, which is not the case. In the fixed version, the DLP tab now appears at the end, representing its actual place in the processing flow.

- **Fixed Issue 104122: In SSL Inspection, parts of the "Quick Exception" button are not clickable depending on the language and screen size.**

When the SSL Inspection's **Quick Exception** button is translated into some non-English languages, a user can click on the outer edges of the button and get no result. In the fixed version, the **Quick Exception** button is now fully clickable regardless of where the mouse cursor is placed.

- **Fixed Issue 109624: The VMware Cloud Web Security UI side menu's organization is not optimized for new features and some menu terms are vague.**

Beginning with version 11.1.1 the Cloud Web Security UI now has the following changes to the side navigation menu:

- New section: **Policy Settings**
- **CASB** and **DLP** moved to **Policy Settings**
- **Inspection Engine** renamed **Content Inspection** and moved to **Policy Settings**
- Removed section **Certificates**
- **Authentication** renamed **Identity Provider** and moved to **Enterprise Settings**
- **SSL Termination** renamed **SSL Certificate** and moved to **Enterprise Settings**
- **Corporate Gateways** renamed **Corporate Gateway IPs**
- **Fixed Issue 109687: When configuring a Non-Standard Web Port rule, a user does not have the option to specify a destination IP address and thus cannot create more than one entry using the same port.**

A user may want to configure two different **Non-Standard Web Port** rules where the port value is the same, but the destination IP addresses are different. With Release 11.1.1, a user can do that.

v1.11.0

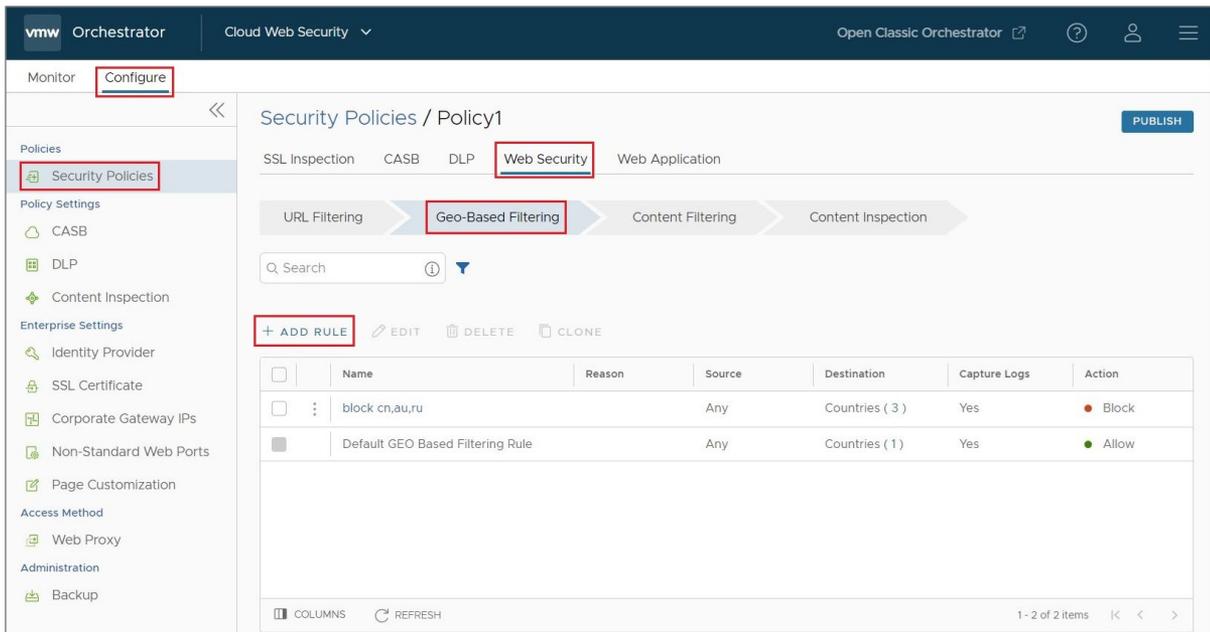
Cloud Web Security version 1.11.0 was released on **08 March, 2023**.

This version adds a new feature as well as resolving one issue.

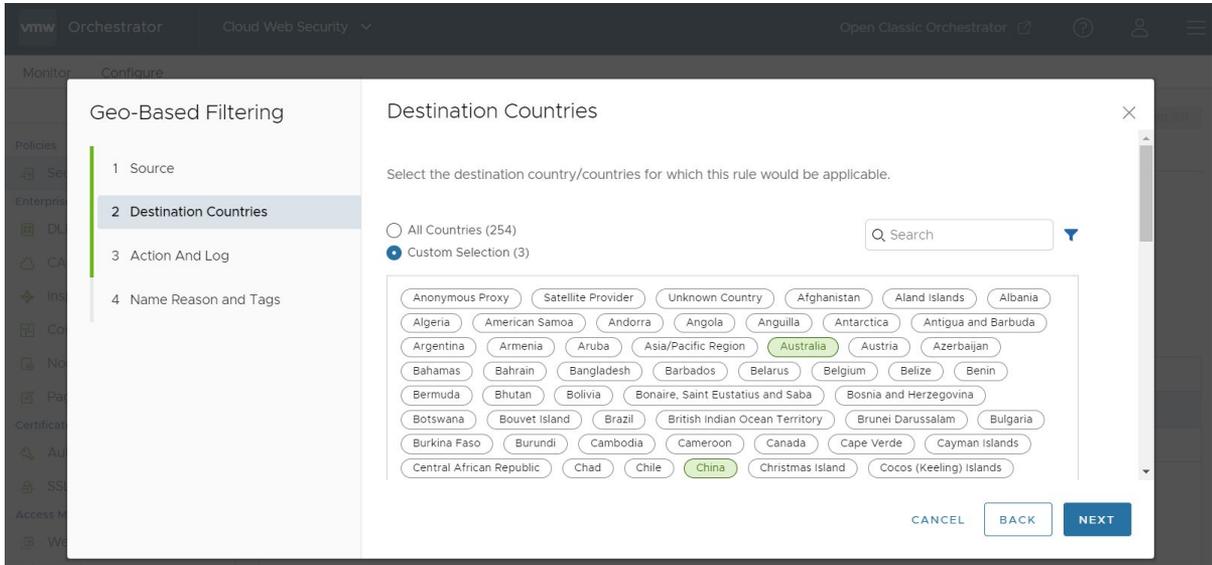
The new feature added, and issue resolved in Cloud Web Security version 1.11.0:

- **New Feature: Geographic Region Based Web Security Rules**

Customers now have the ability to block or allow internet traffic based on the geographic region of the content or the user. This feature is added to the **Configure > Security Policies > Web Security** section by clicking on the **Geo-Based Filtering** tab.

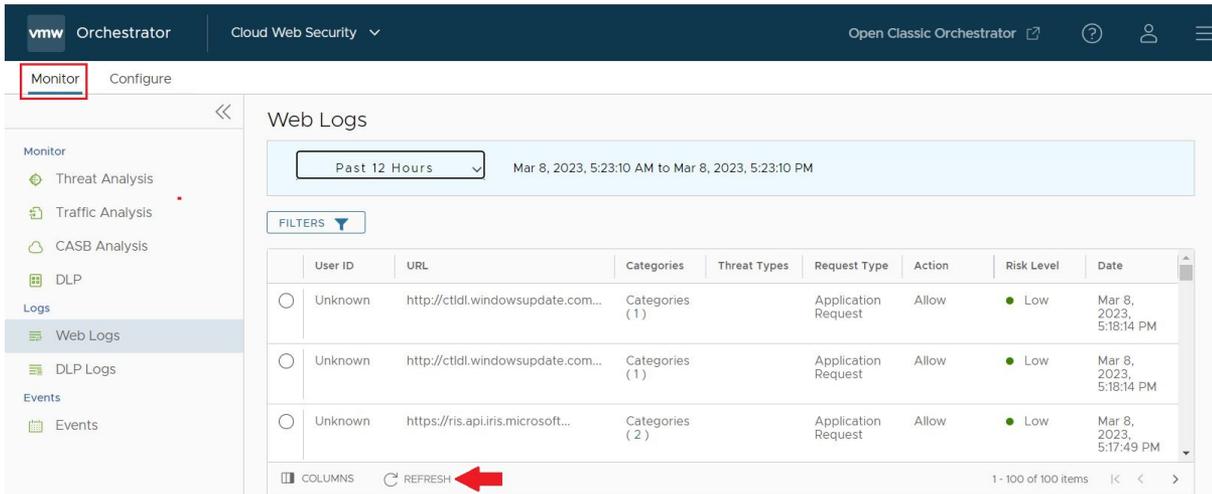


When configuring a **Geo-Based Filtering** rule the user can specify which users and groups it applies to and can then chose from a list of 251 countries with added options for Unknown Countries, Anonymous Proxy, and Satellite Provider traffic to ensure users cannot bypass the rules.



- Fixed Issue 108990: The Refresh button does not work for a Cloud Web Security user when on the Cloud Web Security > Monitor pages of the Orchestrator.**

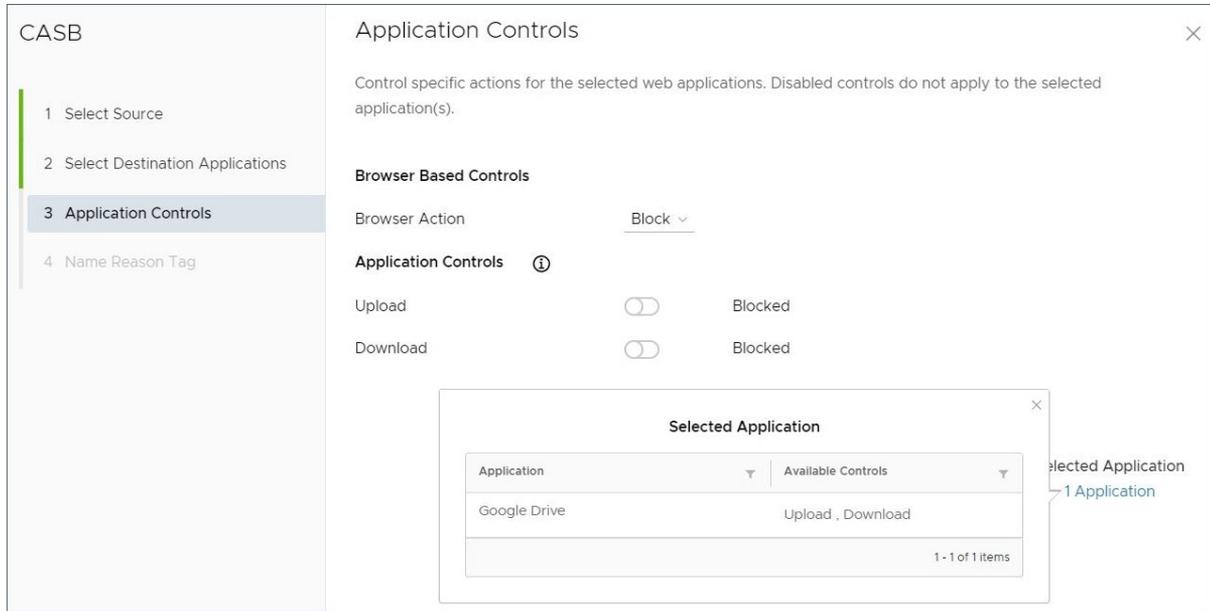
If the user wishes to refresh and update the information on a **Monitor** page (for example, Web Logs or DLP Logs), the Orchestrator includes a **Refresh** button at the bottom of the page.



However, if the user clicks on **Refresh**, the data does not update due to an underlying change in an Orchestrator component.

- Fixed Issue 10900: If a CASB user has a rule for Google Drive, under Application Controls they have the option to configure "Create".**

Symptom: CASB only supports **Upload** and **Download** control options for Google Drive and thus the control for **Create** is removed for version 1.11.0 and later.



- **Fixed Issue 110901: A user has the option to select and configure Telegram as a Destination Application for a CASB rule.**

CASB no longer supports the Telegram application and the option to configure a CASB rule for it is removed with this release.

Should a customer have an existing CASB rule that includes Telegram as a **Destination Application** they should remove that application if their Cloud Web Security version is upgraded to 1.11.0 or later as the rule will no longer enforce that application.

In a later release, Cloud Web Security will automatically remove the Telegram application from all CASB rules and log this action as an Event.

v1.10.1

Cloud Web Security version 1.10.1 was released on **07 February, 2023**.

This version adds a new feature as well as resolving several issues.

The new feature added, and issues resolved in Cloud Web Security version 1.10.1:

- **New Feature: Customizable Block Pages using Page Customization.**

VMware Cloud Web Security displays a VMware branded block page by default to all users when a security policy blocks a user from accessing a website or cloud application.

The **Customizable Block Page** feature allows users to create and customize their own branded block page to display to the user when their traffic (Web or Data Loss Prevention traffic) is blocked. Using the **Configure > Page Customization** section of the Orchestrator, a Cloud Web Security administrator can customize:

- A Block page that VMware cloud uses to respond to an HTTP request or file upload that violates a configured security policy.

- A Block page that VMware cloud returns when a user is trying to upload a file that violates a configured DLP rule.

For more information on how to configure a custom block page, see [Page Customization](#).

- **Fixed Issue 96370: While creating a Data Loss Prevention (DLP) rule, user sees incorrect information in the UI for the “Maximum File Size” tooltip.**

While creating a Data Loss Prevention (DLP) rule, a user would see incorrect information for the “Maximum File Size” tooltip. The tooltip states that “If the uploaded file size is more than the specified value, the file is dropped, and auditor is informed” which is incorrect. The issue is resolved by rewording the tooltip to “If the uploaded file size is more than the specified value, the file is not inspected by DLP and is allowed through”.

- **Fixed Issue 99511: The Cloud Web Security web logs include only “Threat Type” without thread details.**

Cloud Web Security web logs include only the **Threat Type** and the risk details are not shown. To enhance a user’s ability to monitor Web traffic, the risk details for vulnerabilities should also be shown in addition to the **Threat Type** identified.

- **Fixed Issue 106671: Some customers may get an error when they publish a Non-Browser Web Application rule.**

While inspecting browser traffic on Non-Browser Web Applications, older customers may observe an error when they publish a Non-Browser Web Application security policy rule. The issue is the result of the default value not being configured for the supported browser. This issue is not observed for new customers.

Workaround: Support can create a ticket on the Cloud Web Security team requesting to add the default supported browser for the customer manually.

v1.10.0

Cloud Web Security version 1.10.0 was released on **24 January, 2023**.

This version adds one new feature:

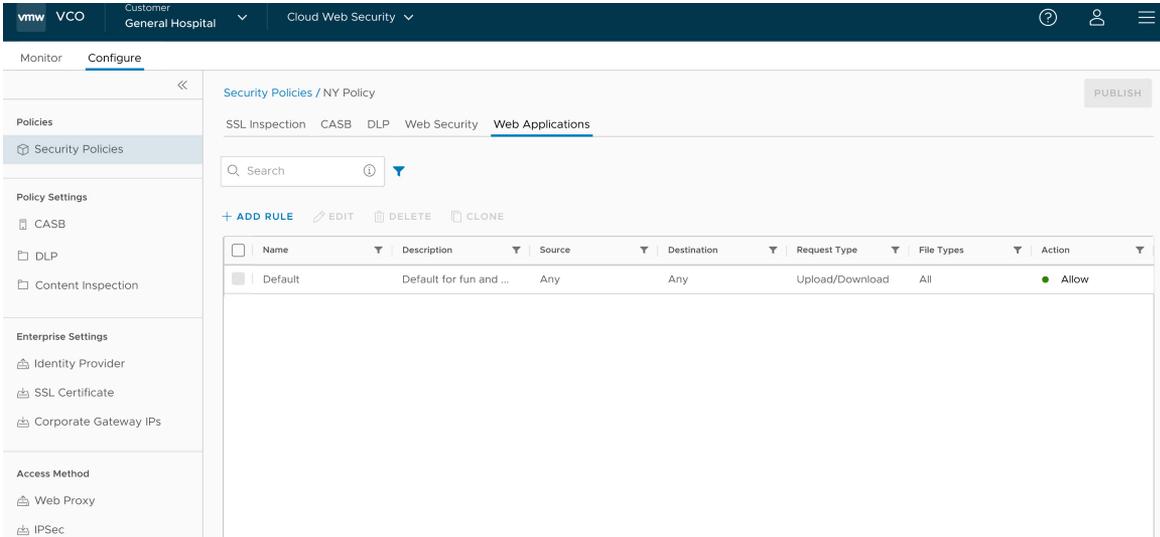
- **New Feature: Configure Rules for Non-Browser Web Application Traffic**

Previously, a user could configure a CWS Security Policy rule to inspect browser-based web applications like Chrome, Edge, Firefox, Safari, and so on, but the rule would not apply for Non-Browser Web Applications like Slack or Dropbox.

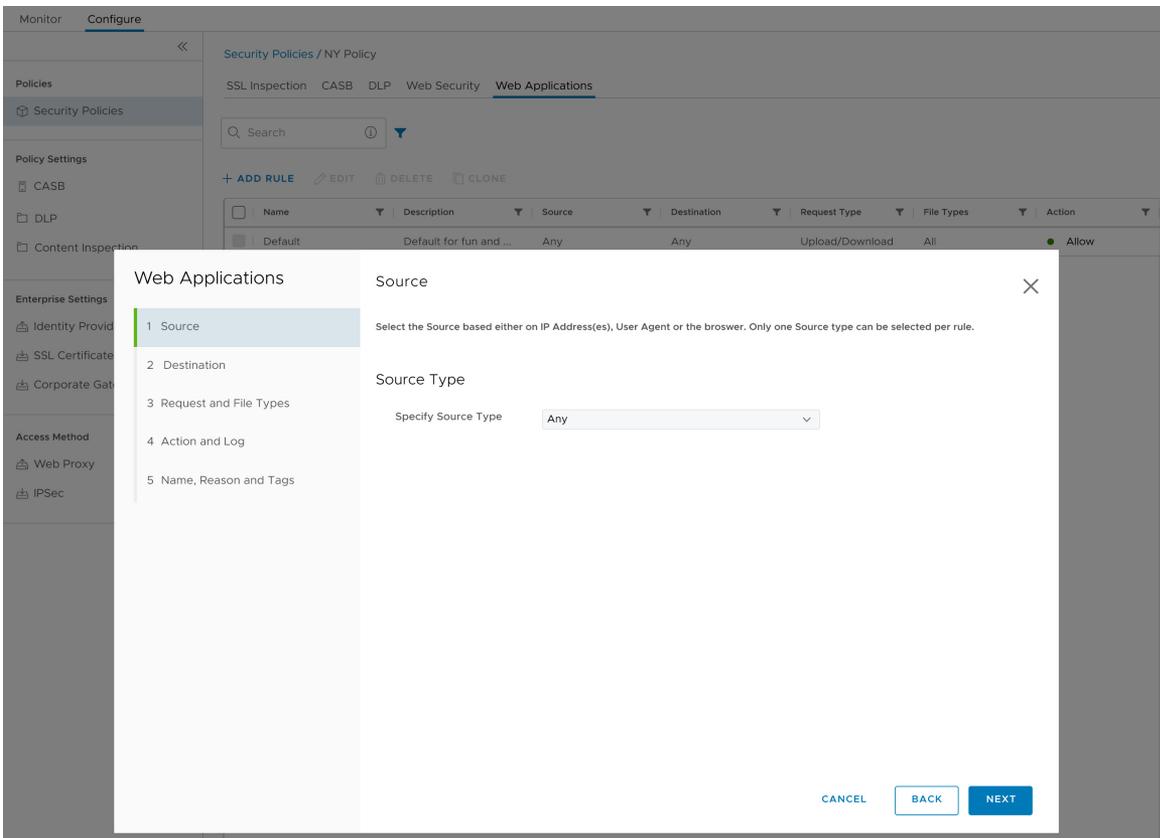
Beginning with Release 1.10.0, a user has the option to configure rules to inspect browser traffic on **Non-Browser Web Applications**.

A user can view, add, and remove rules for Non-Browser Web Applications traffic. To configure rules for a Non-Browser Web Application:

- Navigate to **Cloud Web Security > Configure > Security Policy** and then select an existing policy and click the **Web Applications** tab.



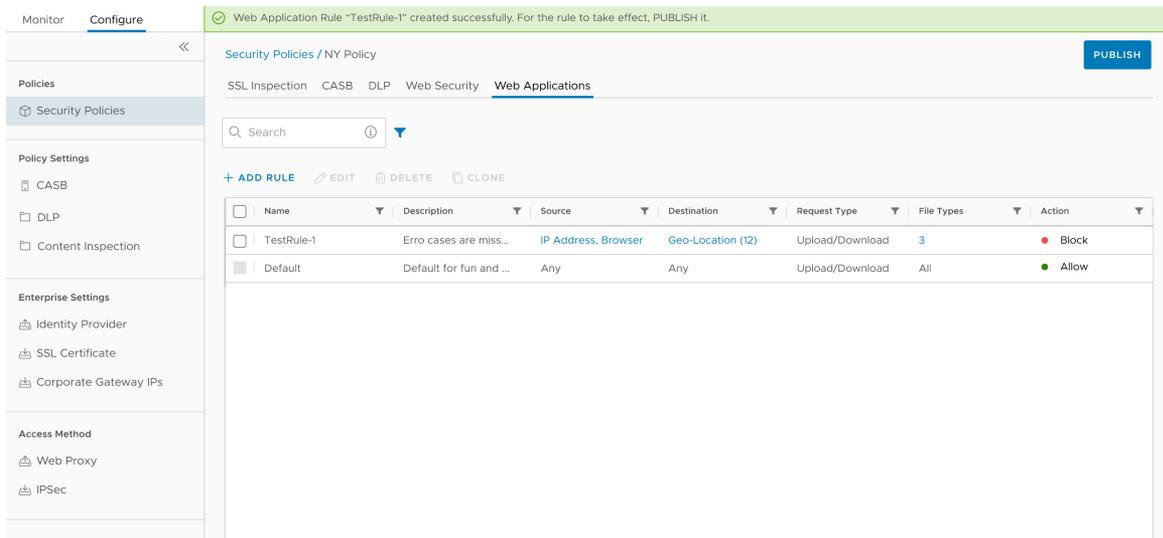
- b Click **+ ADD RULE** and enter all the required details such as Source type, Destination type, Request and File types, Action and Log details to create a new Non-Browser Web Application rule.



Field	Description
Source	Select the Source based on IP Addresses/IP Ranges, User Agent, or Browser. Note Only one Source type can be selected per rule.

Destination	Select the Destination based on Domain, IP Addresses/IP Ranges, URL, Category, Thread, or Geo-Location. Note Only one Destination type can be selected per rule.
Request And File Type	Select the Request Type (Uploads, Downloads, or Both) and the File Type for the rule to apply. You can also select the HTTP method (POST, PUT) for the Upload request type. Optionally, you can also enter the minimum file size for the action to apply.
Action And Log	Select the action (Allow or Deny) to be taken if the rule criteria is met. Optionally, you can collect the logs for this rule by turning ON the Capture Logs toggle button.
Name, Reason and Tags	Configure Name, Tag, Reason, and Position for the Geo-based rules. Ensure you specify a unique name for the rule. Optionally, you can add reasons and tags for the rules, that can be used for sorting and filtering. Note The Position field designates the rule's position on the list of Web Application rules.

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



- d For the new Security Policy rule to take effect, select the rule and click the **Publish** button on the upper right-hand corner of the screen.
- e After publishing the Security Policy, the user is ready to [Apply the Security Policy](#).

v1.9.1

Cloud Web Security version 1.9.1 was released on **17 January, 2023**.

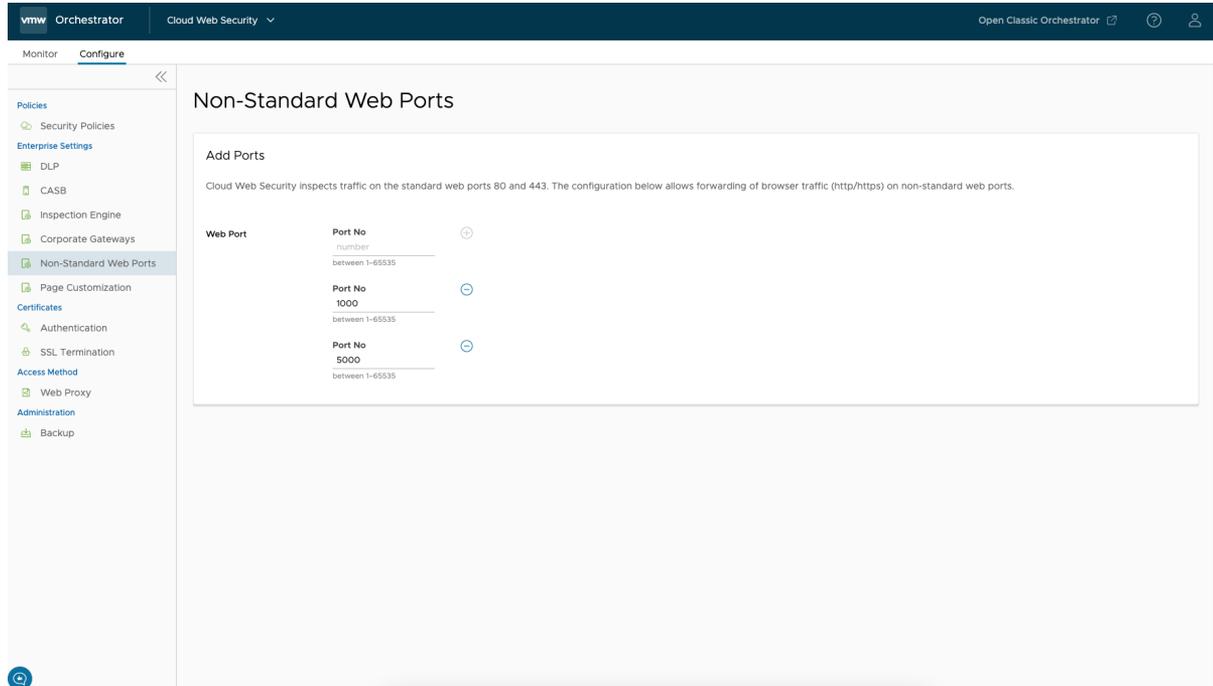
This version adds a new feature as well as resolving several issues.

The new feature added, and issues resolved in Cloud Web Security version 1.9.1:

- **New Feature: Configure Port Rules for Non-Standard Web Ports**

In previous versions, VMware Cloud Web Security could inspect traffic on standard Web Ports 80 and 443. Release 1.9.1 allows inspection of browser traffic (HTTP/HTTPS) on non-standard Web Ports.

A user can view, add, and remove port rules by navigating to **Cloud Web Security > Configure > Enterprise Settings > Non-Standard Web Ports**.



To allow and inspect traffic on Non-Standard Web ports, enter the port number. Click the "+" button on the row to add more Non-Standard Web Ports.

The user can edit existing rules or remove rules by clicking the associated "-" button. After editing, click the **Save Changes** button.

- **Fixed Issue 93272: Resource requests that match a threat category or content category are not blocked.**

When there is a Web Security rule to block a threat category or content category and the domain matching these categories is accessed the website is blocked. However, if the same domain is accessed as a resource on a webpage (for example, clicking on a link that downloads a file), the request is not blocked.

- **Fixed Issue 93278: Web logs that match a content inspection rule may show an incorrect rule matched.**

Web logs that match a content inspection rule show the default rule is matched but never display the actual name of the rule created and configured on the SASE Orchestrator.

- **Fixed Issue 95190: YouTube downloads are erroneously classified as "File Upload" in Weblogs.**

If there is a CASB rule to block or allow YouTube downloads the rule is applied correctly, but the Weblogs show this as "File Upload" instead of "File download", and this impairs an Administrator's ability to assess activity on their network.

- **Fixed Issue 96794: A content filtering rule to block uploads of all file types, blocks login to Microsoft applications.**

When there is a content filtering rule to block uploads of all file types, the rule blocks login to Microsoft applications that require logging in from <https://login.microsoftonline.com/>.

- **Fixed Issue 99661: CASB controls for certain Enterprise Microsoft applications are not working as expected.**

The CASB controls for the following Microsoft applications are not working as expected, when a user configures a "Block" rule. If the user attempts any of these actions, none of them are blocked and the user is able to successfully complete these actions:

- Microsoft Teams - File upload, create, delete
 - Microsoft Outlook - File upload, download, delete
 - Microsoft OneDrive - Delete
 - Microsoft OneNote - Download
- **Fixed Issue 104945: Some websites may not load due to a Cross-Origin Resource Sharing (CORS) issue.**

When a Cloud Web Security policy is enforced and a user accesses certain websites, the page may not load due to a Cross-Origin Resource Sharing (CORS) issue. A user would observe an error similar to *"xxxx has been blocked by CORS policy: The 'Access-Control-Allow-Origin' header contains multiple values '*' "* in the console logs.

- **Fixed Issue 104948: CASB rules for OneDrive are not working on SharePoint OneDrive.**

When there is a CASB rule to block all application controls for OneDrive, the CASB rule do not block the actions for SharePoint.

- **Fixed Issue 104949: If a user creates a CASB rule for Google Drive, this rule does not block folder creation.**

While upload and download are blocked for Google Drive, anyone can create folders in Google Drive.

In Release 1.9.1 and later, a user is unable to create a folder in Google Drive by default and there is no longer a configuration option required for this application.

v1.8.0

Cloud Web Security version 1.8.0 was released on **28 November, 2022**.

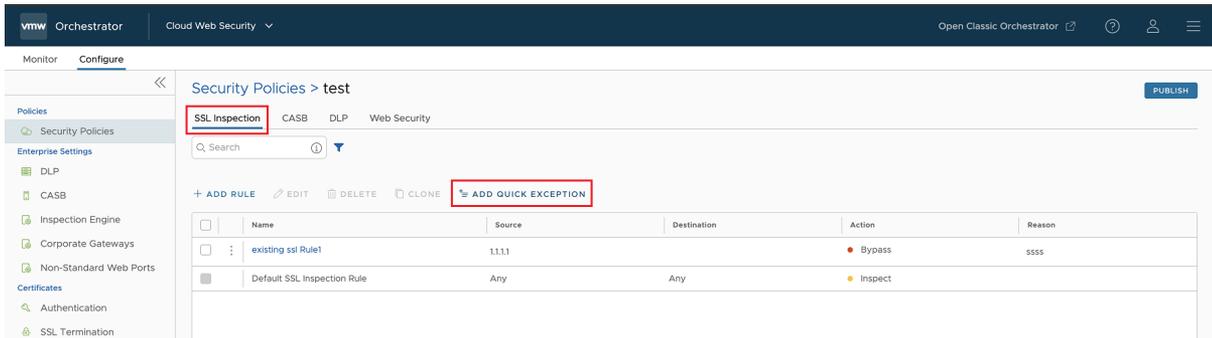
This version adds one new feature:

- **New Feature: Easy SSL Bypass using Quick Exception**

In previous versions of Cloud Web Security, if a user needed to create a rule to bypass the inspection of common web applications, they needed to create a SSL Inspection Rule manually. With the addition of the Easy SSL Bypass feature, the user can quickly create these SSL Inspection Rules.

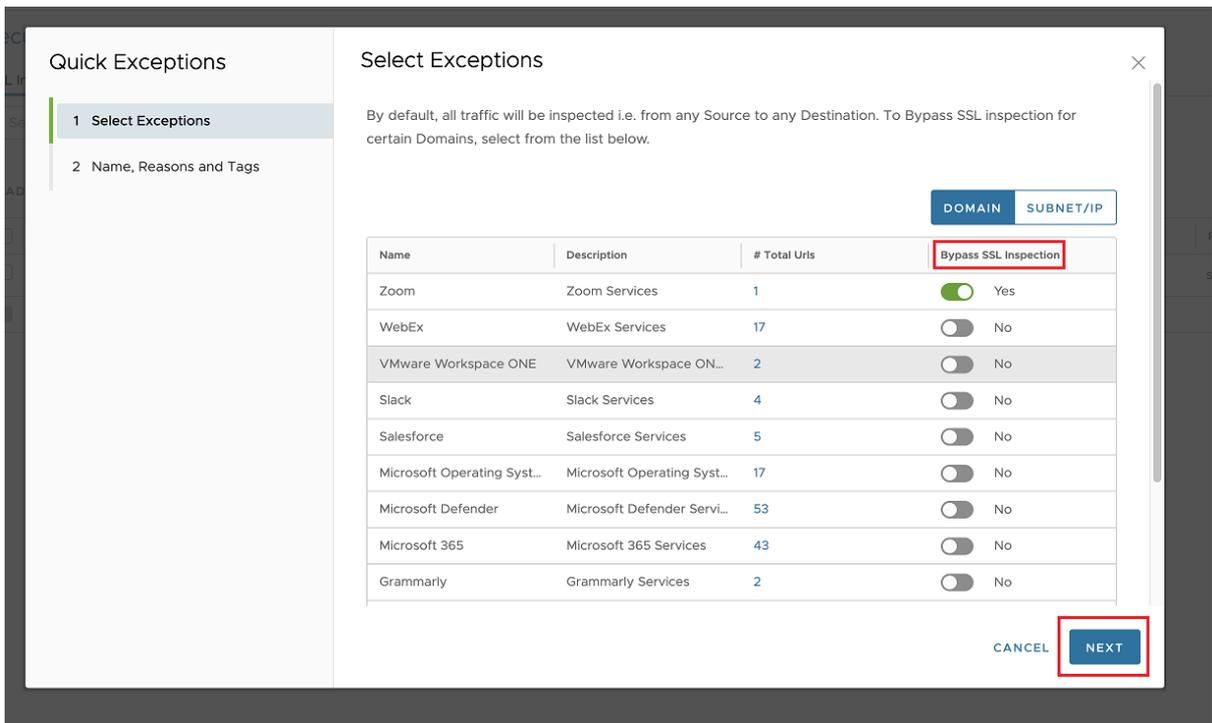
The new feature appears under **Cloud Web Security > Configure > Security Policies** under the **SSL Inspection** tab as a button **Quick Exception**.

Figure 4-1.



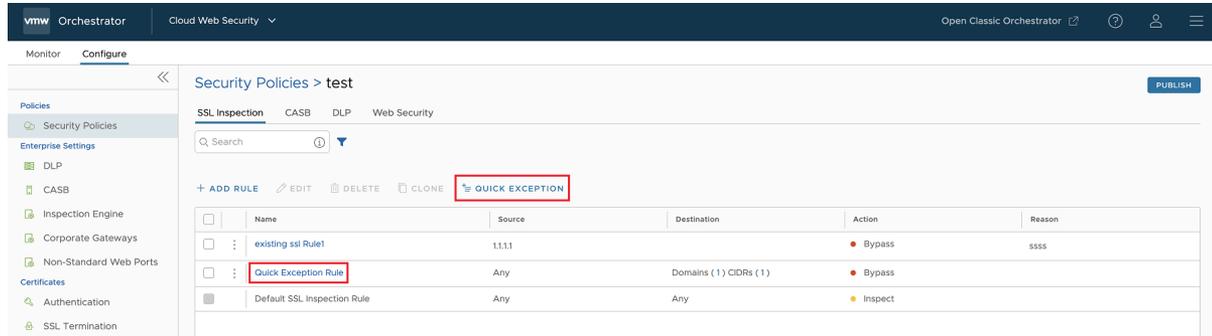
Clicking on **Add Quick Exception** opens a **Quick Exceptions** configuration screen where the user selects one or more applications they want excepted from SSL inspection. When a user selects an application, all the URLs associated with that application are excepted from SSL inspection.

Figure 4-2.



When using the Quick Exception option, one single rule is created, and no additional rules can be created. This rule is always called **Quick Exception Rule** and the name cannot be changed in the Quick Exception wizard.

Figure 4-3.



The rule will always be the second to last rule in the grid and can quickly be accessed by clicking the **Quick Exception Rule** name. Once the Quick Exception Rule is added, the **Add Quick Exceptions** menu option changes to **Quick Exception**, indicating there is an existing **Quick Exception Rule** that can be edited, and no additional rules of this type can be added.

v1.7.0

Cloud Web Security version 1.7.0 was released on **01 November, 2022**.

This version adds a new feature as well as resolving several issues.

The new feature added, and issues resolved in Cloud Web Security version 1.7.0:

- **New Feature: Web Logs now include both a Region field and User Group field for enhanced monitoring.**
 - The **Region** field indicates which SASE PoP was being used for a web event which helps localize which part of the world an event occurred.
 - The **User Group** field indicates the SAML user group, where a SAML configuration is used.

Together, these two added fields enhance a user's ability to monitor web traffic.

- **Fixed Issue 93269: A Cloud Web Security web policy does not block a malicious file download.**

In some instances a user may observe that a malicious file is downloaded despite having a policy configured to block such a download.

- **Fixed Issue 94168: When downloading a password protected file from OneDrive or Dropbox, there is no prompt to enter the password and the user is unable to download the file.**

When downloading a password protected file from any website, the user should be prompted to enter a password as this is the default action in content filtering. But on OneDrive and Dropbox, the file download is blocked without a prompt for password and cannot download the file.

- **Fixed Issue 95190: An administrator observes in their enterprise's weblogs that YouTube downloads are erroneously classified as uploads.**

If there is a CASB rule to block or allow YouTube downloads the rule is applied correctly, but the weblogs show this as a "File Upload" instead of "File download", and this impairs an administrator's ability to assess activity on their network.

- **Fixed Issue 95998: CASB rules for OneDrive do not work.**

If a user creates and applies a CASB rule that allows browser actions while blocking all application controls and then logs into OneDrive and tries all the actions that should be blocked, none of them will be blocked. Actions that are not blocked include creating and deleting folders.

- **Fixed Issue 96274: Certain CASB controls for Microsoft O365 Outlook do not work as expected.**

When there is a CASB rule for Microsoft O365 Outlook to either block, delete, download, upload, or search and the user attempts any of these actions on Microsoft O365 Outlook, none of them are blocked.

- **Fixed Issue 96790: User is unable to determine the exact security policy being acted on in a web request due to lack of clarity in logs.**

In this issue the logs only display policy headers (which are just identification codes) acting on a web request versus explicitly stating which policy is being invoked. The only way a user could determine which policy was being used was by taking the policy header and then opening the Network tab to map that policy header to the policy names.

- **Fixed Issue 98047: A CASB rule to block uploads and downloads of files to Microsoft SharePoint and Microsoft Word, Cloud Web Security does not block file uploads and downloads.**

When there is a CASB rule to block uploads and downloads to Microsoft O365 SharePoint or Microsoft Word, and the user tries to upload or download a Word file to, or from SharePoint, the upload and download actions are not blocked.

v1.6.1

Cloud Web Security version 1.6.1 was released on **15 September 2022**.

The following features are added in Cloud Web Security version 1.6.1

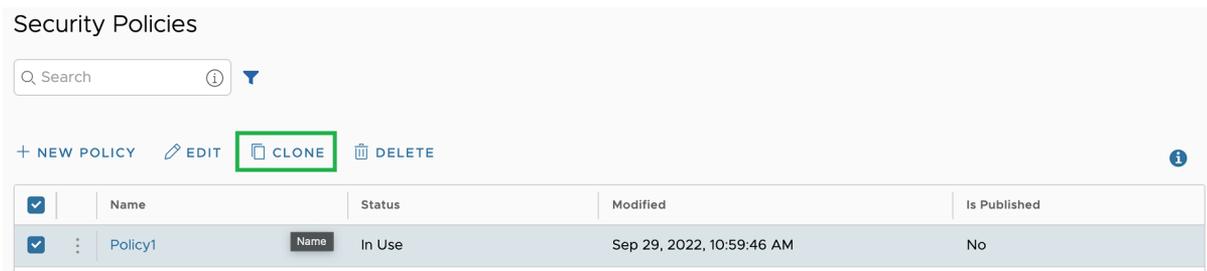
- **New Feature: Web Proxy**

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

- **New Feature: Cloning a Security Policy.**

Release 1.6.1 introduces the ability to clone security policies that can also be stored as a backup.

This feature also includes cloning capabilities for different rule types within a security policy, for example: SSL Inspection, CASB, DLP and Web Security.



v1.5.2

Cloud Web Security version 1.5.2 was released on **03 September, 2022**.

Issues resolved in Cloud Web Security version 1.5.2

- **Fixed Issue 94734: A user sees confusing file categories with vague names "Other Downloads" and "Other Documents".**

While creating Cloud Web Security rules, the user sees file categories, "Other Downloads" and "Other Documents" which are not very clear as to what they affect. The issue is resolved by reducing the ambiguity by renaming "Other Downloads" to "Other Files and Documents", and "Other Documents" to "Miscellaneous Documents".

v1.5.1

Cloud Web Security version 1.5.1 was released on **30 August, 2022**.

Issues resolved in Cloud Web Security version 1.5.1

- **Fixed Issue 93206: MEGA downloads are not blocked by a CASB rule configured to block them.**

If a user creates a CASB rule for application "Mega" to block both uploads and downloads and then logs into mega.io and attempts to upload or download a file, the user would observe that file uploads are correctly blocked, but downloads are not.

- **Fixed Issue 93208: Gmail attachment downloads are blocked whether there is a rule or not and no log is generated for the event.**

Whether a CASB rule is configured to block Gmail attachment downloads or not, when a user tries to download a Gmail attachment just by clicking on the download icon for the attachment, the download is blocked but there is no log recorded. This issue does not occur if the user tries to download the attachment in a new tab.

- **Fixed Issue 93209: Certain files that are identified as malware are not blocked by a content filtering rule configured to block them.**

When there is a Content Filtering rule to block uploads and downloads of malware files, some files are blocked and some files are not blocked.

- **Fixed Issue 93210: A DLP rule to block text input matching a dictionary is not applied to LinkedIn messages.**

When there is a DLP rule to block text input that matches a dictionary and messages are sent on LinkedIn that matches the dictionary, the message is not blocked.

- **Fixed Issue 93211: YouTube downloads are not blocked by a CASB rule configured to block them.**

If a user creates a CASB rule to block YouTube downloads and then tries to download any video on YouTube, the download is not blocked.

- **Fixed Issue 93213: CASB rules that work at first may not work when a browser page is refreshed.**

When there is a CASB rule to block actions like search, search feature in the application is blocked. Now if the URL in the browser has the search parameters and the page is refreshed the search results are not blocked.

- **Fixed Issue 93214: A Content Filtering rule configured to block the downloading of All Files does not block JPEG downloads.**

A Content Filtering rule to Block downloading of "All Files" (which should include all picture formats) does not block JPEG downloads. Without the fix the workaround is to use a custom File type option and add the file extensions that should be blocked (for example, JPEG).

- **Fixed Issue 93217: Upload of certain file types is not blocked on Google Drive (G-Drive) even if the file content matches a DLP rule.**

Files with extensions .doc, .docx, .ppt, and .pptx are not blocked on G-Drive even if the file content matches a DLP rule.

- **Fixed Issue 93225: Cloud Web Security may not match a website to the correct threat category resulting in the website not being blocked.**

A user could configure a rule to block all threat categories with a URL filtering rule, and some sites that should be categorized as malicious are not blocked.

- **Fixed Issue 93262: A Cloud Web Security rule configured to apply to a specific user group is not applied.**

When there is a security rule that should be applied only to users in the specified group, it is not enforced. As a result, all of the rules that should be applied to the users in the group are not.

- **Fixed Issue 93268: CASB Control rules not applied to Microsoft Teams.**

A CASB control policy to allow browsing to the Microsoft Teams Web application but which blocks all other actions does not stop users from posting content.

- **Fixed Issue 94369: When a user configures a rule to Block either "All Documents" or all "All Files, the user would observe uploads being blocked that do not match the respective rule.**

- When applying a rule to Block "All Documents", a user would observe that not only are Document uploads blocked, but File and Archive uploads are blocked as well.
- When applying a rule to Block "All Files", a user would observe that not only are File uploads blocked, but Document and Archive uploads are blocked as well.

v1.5.0

Cloud Web Security version 1.5.0 was released on **10 August, 2022**.

Issues Resolved in Cloud Web Security version 1.5.0.

- **Fixed Issue 87027: Cloud Web Security logs include resource-type logs, which can clutter the Logs view.**

The Orchestrator UI had no option to allow the user to toggle on and off the resource logs so that they could better identify more relevant logs.

- **Fixed Issue 88813: Security Web Policies tab component show two tabs selected at the same time when CASB is not licensed.**

The tab component entered a bad state due to the way we were disabling and hiding tabs.

- **Fixed Issue 89718: The VMware SASE Orchestrator cannot load the DLP Predefined Dictionaries.**

There is an issue on the Orchestrator backend that results in the UI being unable to get the DLP Predefined Dictionaries. This issue does not affect Customer Defined Dictionaries and they load properly.

- **Fixed Issue 89752: For a Cloud Web Security customer using a Standard License, the CASB feature is not fully visible on the VMware SASE Orchestrator UI.**

This lack of visibility for the CASB feature includes:

- The **Configure > CASB** menu item and view.
- The **Monitor > CASB Analysis** menu item and view.
- The API these particular components use.
- **Fixed Issue 91054: For a customer using VMware Cloud Web Security, a user may encounter multiple usability issues on the VMware SASE Orchestrator UI when attempting to configure Single Sign-On Authentication (SAML).**

The issues a user could encounter while configuring Single Sign-On in the Cloud Web Security service include:

- Certificate errors showing on the main Authentication page instead of on the Certificate page.
- A user can sometimes save an invalid certificate.
- Changing a certificate can sometimes reset the other values on the Authentication form.
- Individual fields do not show validation messages inline with the field.
- When saving the Authentication page, the Orchestrator UI does not show a progress spinner.
- The Verbose Debugging tooltip shows "t+2hrs" instead of an actual time. • In some languages, the Single Sign-On toggle label wraps to more than one line.
- The **Save Changes** footer layout is incorrect on short screens.

All of the listed issues are resolved with the fix for **#91054**.

- **Fixed Issue 91683: A user is unable to add a CIDR IP address to the Source for SSL Inspection Rule in Cloud Web Security.**

Both the configuration wizard and the API do not accept a CIDR IP in Source for an SSL Inspection Rule, and the fix corrects this issue.

- **Fixed Issue 91697: When using a Cloud Web Security wizard to configure an SSL Inspection, URL Filtering, Content Filtering, Content Inspection rule, when the Finish/Update button is clicked, the wizard stops responding and the user cannot complete the rule configuration.**

The issue is caused by the Cloud Web Security backend server rejecting a configuration value entered while using the wizard and the result is the The Finish/Update button stops responding once it receives this validation error.

- **Fixed Issue 92082: For a customer using VMware Cloud Web Security, the customer may observe that the Content Filtering rules do not honor the configured domain.**

The Content Filtering rules override the configured domain provided if the user has also selected ALL for Categories. Or, if the user selects NONE for Categories, the wizard defaulted this choice to mean ALL Categories, hence the domains were not honored here as well. This is caused by an issue in the content filtering wizard and API. If the user configures at least one Category, the Domain is honored.

On an Orchestrator without this fix, the user would need to configure specific categories along with domains, and then the Orchestrator would honor domains in content filtering.

- **Fixed Issue 93341: When using the CASB Visibility feature a user will observe issues with Certificates and the "Company Founded" date.**

In CASB Visibility a user can observe the Orchestrator UI list a certificate as expired when the certificate is still valid and would be renewed when it actually was expired. The other issue is that numerous applications will show as "Founded in 1970" under **Application Details** when the application is clearly much more recent in origin.

Known Issues

5

- **Issue 93202: Blocking Google Drive create in CASB Control rule does not block folder creation.**

If a user configures a CASB Control rule to block Google Drive create, it does not block the creation of a folder. However the CASB rule does block the creation of new Google Docs, Sheets, and other Google applications. In other words, a user accessing Google Drive would get a folder, but no actual content would make it into the folder.

Workaround: There is no workaround for this issue and the user needs to be aware that this behavior exists for a CASB rule affecting Google Drive.

- **Issue 96847: CASB rules are not applied to Microsoft applications which are based on a personal account.**

If a user configures a CASB rule to block an action for a Microsoft application (Teams, OneDrive, Sharepoint, etc.), a user would observe the rules being applied properly if the Microsoft application is base on a corporate/business account. However, if the Microsoft application is based on a personal account, none of the actions are blocked. This includes actions like post, like, upload, download, and delete.

Workaround: Ensure that no users are using personal accounts if CASB rules are being used for Microsoft applications.

- **Issue 96848: OneDrive uploads show the user as "unknown user".**

This issue impacts an administrator's ability to configure user-based rules for OneDrive uploads as the user is not specified.

This issue is the result of OneDrive's use of a different domain for uploads (api.onedrive.com) versus the actual domain loaded in the browser (onedrive.live.com). The Cloud Web Security user authentication cookie for live.com is not passed to onedrive.com because of restrictions common to all web browsers and the OneDrive user cannot be identified.

- **Issue 111002: Customers are unable to publish a Security Policy which contains CASB rules which include the applications Telegram, Jira, or Confluence.**

Cloud Web Security deleted Telegram, Jira, and Confluence from the list of CASB application. As a result any CASB rules that are configured with these applications become invalid when they are published.

Workaround: Delete each CASB security rule which uses any of the applications mentioned above, and create new rules without those apps and publish.