
Configure Data Loss Prevention in Concerto

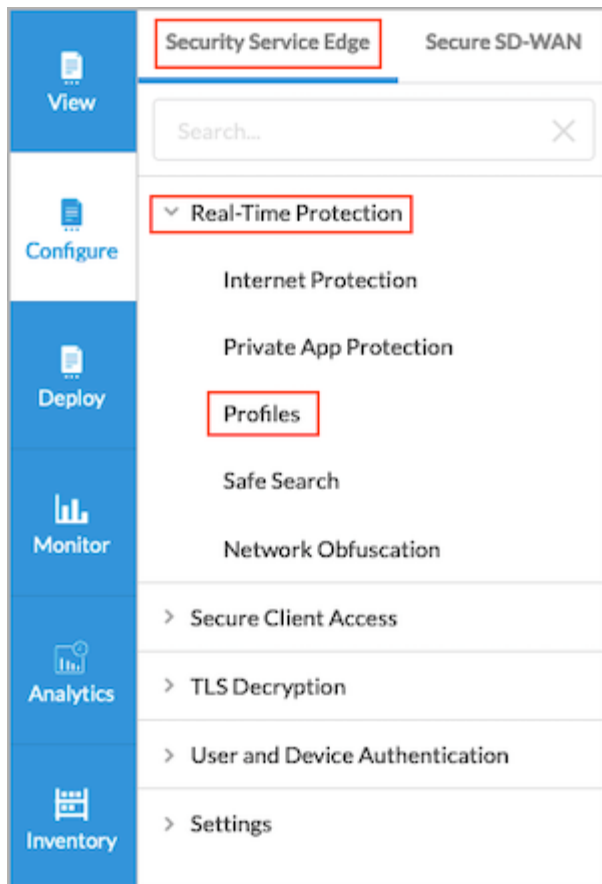
Data loss prevention (DLP) is a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. You use DLP to protect and secure an organization's data and to comply with regulations. The Versa Networks DLP solution oversees, tracks, and reports all data transactions in the network, scanning all content that passes through an organization's ports and protocols to ensure data security in the organization. All the data gathered is sent to Versa Analytics, which generates detailed reports about what data is being used, who is using it, and where the data is sent. These reports are available to users.

To configure DLP in Concerto, you create a DLP profile that you associate with a security policy. To create the DLP profile, you do the following:

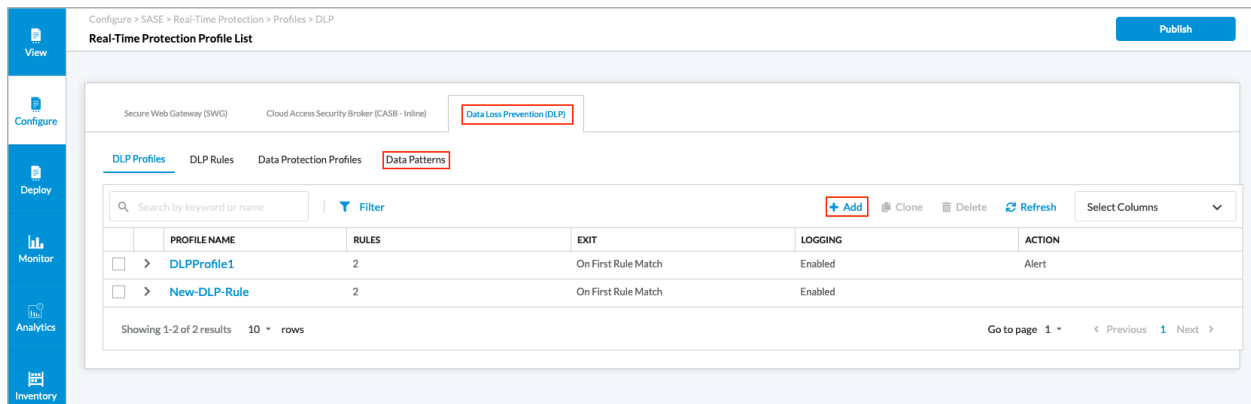
1. Configure data patterns—Data patterns define the specific data strings that you want to filter in a data protection profile. Concerto includes a large number of predefined data patterns that are provided in the Versa security pack (SPack) software, and you can create custom data patterns.
2. Define a data protection profile—You associate data patterns with a data protection profile, and you then use the data protection profile when you create DLP rules.
3. Define DLP rules—You create the rules that are used in a DLP profile to match data.
4. Configure a DLP profile—Create an ordered set of DLP rules that you can then apply to a security policy or to an internet protection rule.

Configure Custom Data Patterns

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



The following screen displays.



2. Select the Data Loss Prevention (DLP) tab, and then select the Data Patterns tab.
3. To customize which columns display, click Select Columns down arrow, and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

Select Columns

☒ Regex
 ☒ Keyword
 ☒ Range Window
 ☒ Range From

Reset

4. Click + Add to add a new data pattern. In the Data Patterns popup window, enter information for the following fields.

Data Patterns

Name

Enter Name

Regex

Enter Regex

Keywords

Range From

Select

Range Window (Bytes)

Enter Value

Field	Description
Name	Enter a name for the data pattern.
Regex	Enter a regular expression to search for in a file, for example, Employee.*Salary.
Keywords	Enter one or more keywords to search for in a file, and then press Enter to add the keyword. When a keyword is found, the DLP engine scans for the regular expression pattern within the given range. Use a comma to separate multiple keywords.
Range From	Select the location to search in the file: <ul style="list-style-type: none"> Anywhere—Start the scan anywhere in the file. Start—Start the scan at the beginning of the file.

Field	Description
Range Window	<p>Enter a range for the search with the file, which is sometimes called the proximity.</p> <p>If you select Range From Anywhere, you do not need to specify a range window, because the entire file is scanned.</p> <p>If you select Range From Start, enter the number of bytes to scan from the start of the file.</p> <p>If you do not enter a range window, the entire file is scanned.</p> <p><i>Range:</i> 1 through 4294967295 bytes <i>Default:</i> 8192 bytes</p>

5. Click Save.

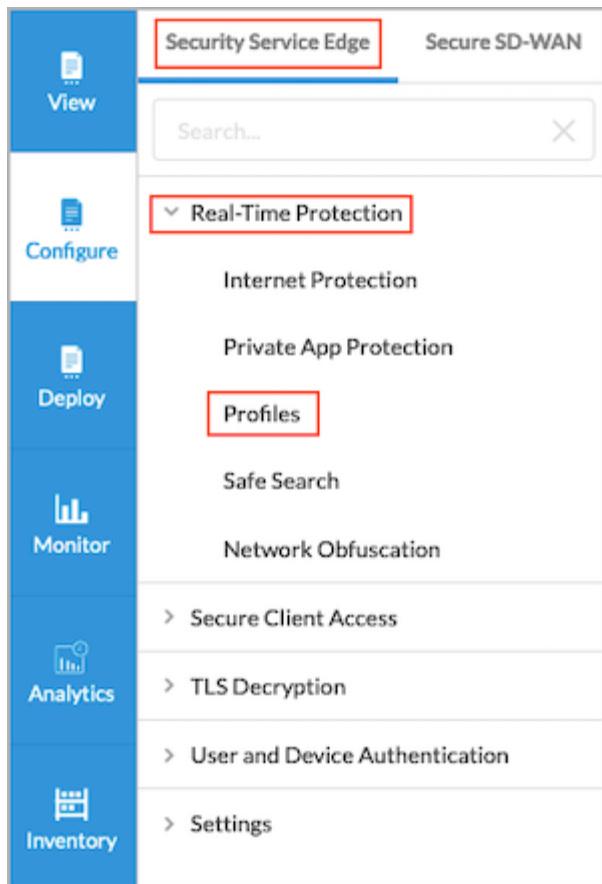
Configure Data Protection Profiles

A data protection profile consists of an ordered set of rules in which each rule has one or more match conditions and an action. You can configure a data protection profile to stop evaluating rules after the first rule that matches (Exit on First Rule Match option) or to evaluate all rules and apply all those that match (default behavior).

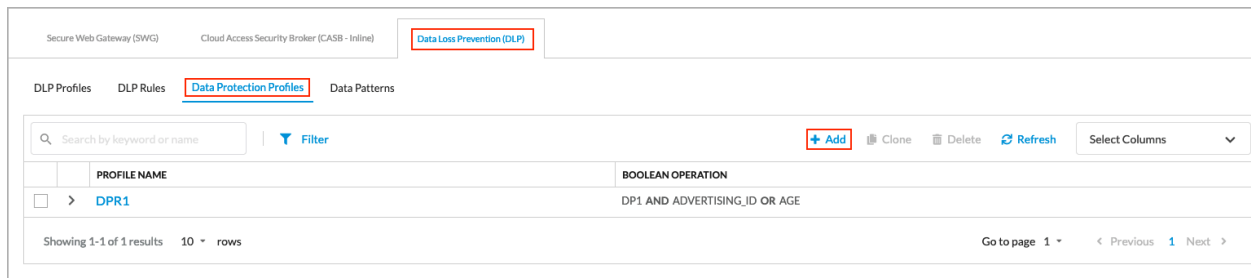
After you create a data protection profile, you can use it as part of the enforcement actions on a policy rule in a security access control policy.

To configure a data protection profile:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



The following screen displays.



2. Select the Data Loss Prevention (DLP) tab, and then select the Data Protection Profiles tab.
3. Click + Add. In Step 1, Select DLP Data Pattern, you can select either user-defined (custom) or predefined data patterns.

Configure > SASE > Real-Time Protection > Profiles > Data Protection

Create Data Protection Profile

1 2 3
SELECT DLP DATA PATTERN **ACTION** **REVIEW & SUBMIT**
 Data Pattern

Add User-Defined Data Pattern
Add Pre-Defined Data Pattern

- a. To select user-defined data patterns, click Add User-Defined Data Pattern, and then select one or more custom data patterns to use in the data protection profile.

Select User-Defined Data Pattern

<input checked="" type="checkbox"/> Selected	DP1
<input checked="" type="checkbox"/> Selected	TestPattern1

Cancel
Save

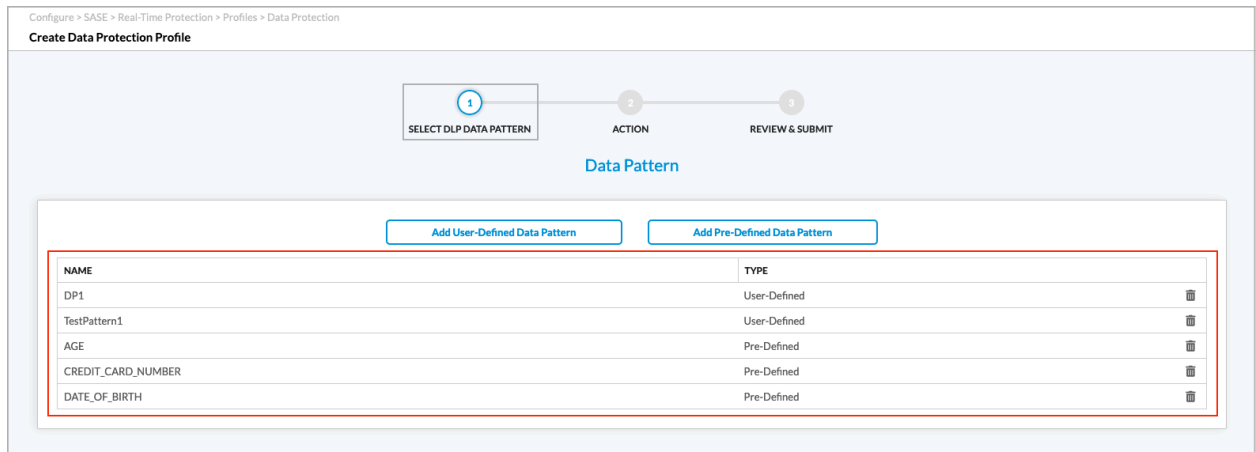
- b. Click Save to add the user-defined data patterns to the data protection profile.
- c. To select predefined data patterns, click Add Predefined Data Pattern, and then select one or more predefined data patterns to use in the data protection profile.

Select Pre-Defined Data Pattern

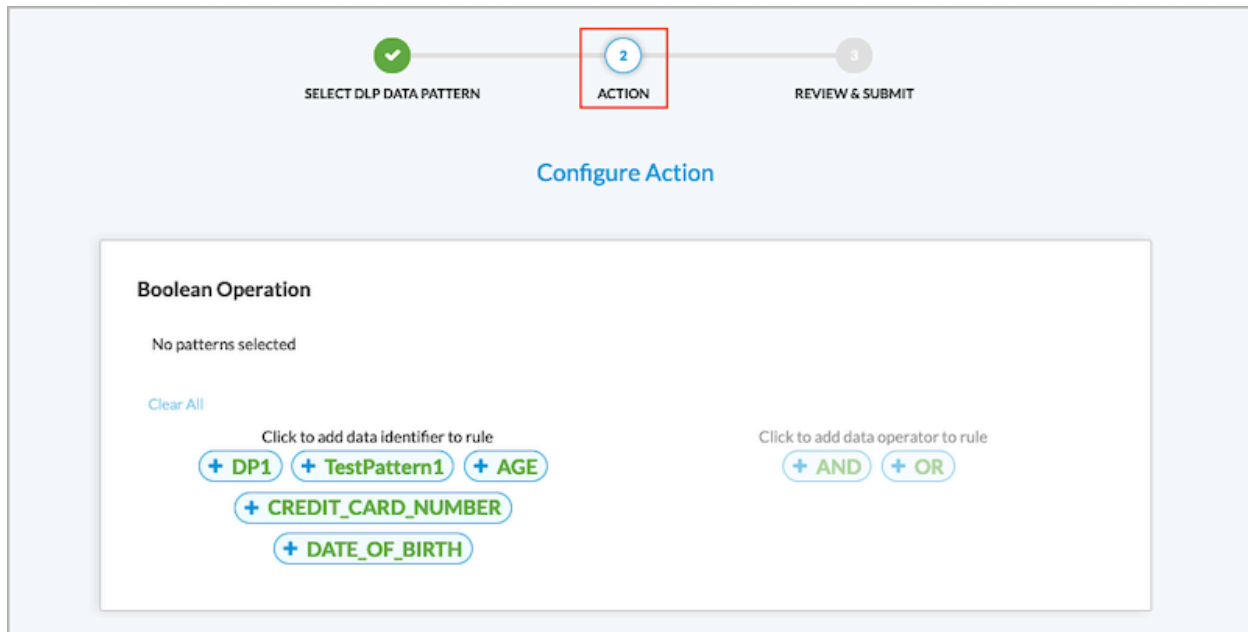
<input checked="" type="checkbox"/> Selected	AGE
<input type="checkbox"/> Unselected	AUSTRALIA_DRIVERS_LICENSE_NUMBER
<input type="checkbox"/> Unselected	AUSTRALIA_MEDICARE_NUMBER
<input type="checkbox"/> Unselected	AUSTRALIA_PASSPORT
<input type="checkbox"/> Unselected	AUSTRALIA_TAX_FILE_NUMBER
<input checked="" type="checkbox"/> Selected	CREDIT_CARD_NUMBER
<input type="checkbox"/> Unselected	DATE
<input checked="" type="checkbox"/> Selected	DATE_OF_BIRTH
<input type="checkbox"/> Unselected	EMAIL_ADDRESS
<input type="checkbox"/> Unselected	GENDER
<input type="checkbox"/> Unselected	ICD10_CODE
<input type="checkbox"/> Unselected	ICD9_CODE

Cancel
Save

- d. Click Save. The Data Pattern screen displays the selected data patterns.



4. Click Next.



5. In Step 2, Action, you create a Boolean operation that defines how to match the selected data patterns. To do this, click a data pattern, click a Boolean operator, and then click a second data pattern to complete the Boolean operation. If a Boolean operation includes multiple data patterns, separate them a Boolean operator. The following example shows a Boolean operation created from the data patterns shown in the previous screenshot:

Boolean Operation

DP1 ▾ AND ▾ AGE ▾ OR ▾ DATE_OF_BIRTH ▾

[Clear All](#)

Click to add data identifier to rule

+ DP1
+ TestPattern1
+ AGE

+ CREDIT_CARD_NUMBER

+ DATE_OF_BIRTH

Click to add data operator to rule

+ AND
+ OR

To replace one data pattern in the Boolean operation with another, click the down arrow next to the data pattern name, and then select a different one.

DP1 ▾

DP1
 TestPattern1
 AGE
 CREDIT_CARD_NUMBER
 DATE_OF_BIRTH

To change the Boolean operator, click the down arrow next to the operator name and then selecting a different one.

AND ▾

AND
 OR

To remove the last element of a Boolean operation, click the down arrow, and then click Remove Selection.

Boolean Operation

DP1 ▾ AND ▾ AGE ▾ OR ▾ DATE_OF_BIRTH ▾

Clear All

Click to add data identifier to rule

+ DP1 + TestPattern1 + CREDIT_CARD_NUMBER + DATE_OF_BIRTH

Click to add data operator to rule

+ AND + OR

Remove Selection

DP1

TestPattern1

AGE

CREDIT_CARD_NUMBER

DATE_OF_BIRTH

6. Click Next.
7. In Step 3, Review and Submit, enter a name for the data protection profile and, optionally, a text description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.

1 2 3 REVIEW & SUBMIT

SELECT DLP DATA PATTERN ACTION

Review your Data Protection configuration below

General

Name * ⓘ Description

Tags

Data Patterns Edit

USER-DEFINED

DP1

TestPattern1

PRE-DEFINED

AGE

CREDIT_CARD_NUMBER

DATE_OF_BIRTH

Action Edit

BOOLEAN OPERATION

DP1 AND AGE OR DATE_OF_BIRTH

Cancel Back Save

8. Review the data protection profile entries.
9. To change any of the information, click the Edit icon in its section, and then make the required changes.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...)

Updated: Wed, 23 Oct 2024 08:39:35 GMT

Copyright © 2024, Versa Networks, Inc.

10. Click Save to create the data protection profile.

Configure DLP Rules

A DLP profile rule consists of the following components:

- Rule type—You can select one or more of the following rule types:
 - Context analysis—Scan data in the HTTP Context, such as HTTP Attachment, HTTP Body, and HTTP Header.
 - Document fingerprinting—Convert a standard form into a sensitive information type, which can then be used to define DLP policy rule. The DLP software examines files that have been fingerprinted and the directory path to these files to determine how similar a candidate file is to a previously fingerprinted file. The DLP software then computes a similarity threshold between the two files and compares the similarity threshold to the configured threshold. The configured threshold is the percentage of content that needs to be similar to the previously fingerprinted file stored in the folder path.
 - Exact data match (EDM)—Validate the match result of a custom or predefined data pattern against a user-provided data set. An exact data match rule can reduce false positives and can help to guarantee precise DLP for entries in the data set.
 - File DLP—Provide protection based on the configured file attributes.
 - Machine Learning—Uses models trained with predefined and custom data for image classification, source code detection, and document fingerprinting.
 - Optical character recognition (OCR)—Converts images to text and applies DLP policies on the converted text data.
- Protocol monitoring—DLP monitoring can scan the HTTP protocol.
- File-type filtering—You can configure data filters based on the file types.

The following table shows the applications supported by DLP and the whether upload and download are supported for each of the listed actions.

Application	Alert	Allow	Alert & Set Label	Allow & Set Label
Box.com				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Supported	Supported
Dropbox				
• Download	Supported	Supported	Supported	Supported

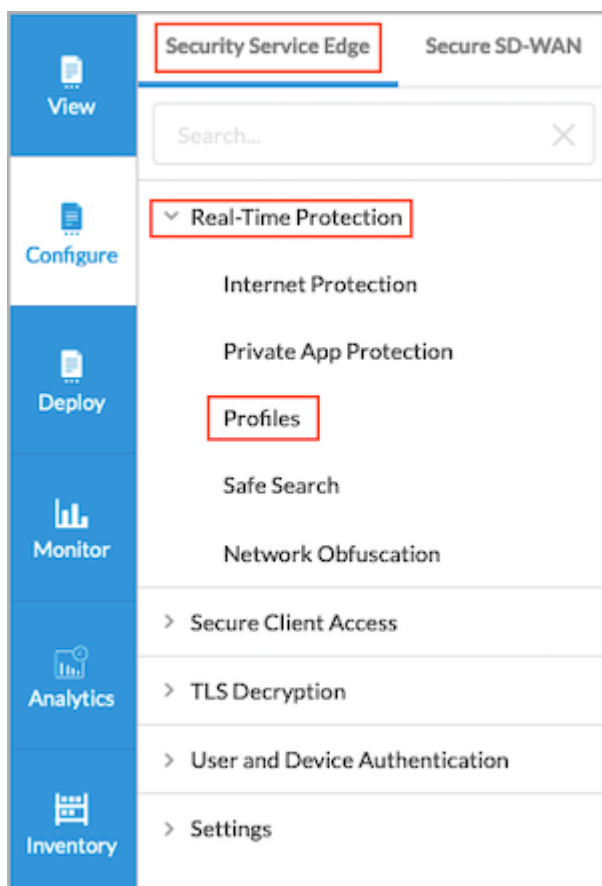
Application	Alert	Allow	Alert & Set Label	Allow & S
• Upload	Supported	Supported	Not Supported	Not Supp
G-Drive				
• Download	Supported	Supported	Supported	Supported
• Upload	Not Supported	Not Supported	Not Supported	Not Supp
Github				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Not Supported	Not Supp
Gmail				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Not Supported	Not Supp
Google Chat				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Not Supported	Not Supp
One Drive				
• Download	Supported	Supported	Supported	Supported

Application	Alert	Allow	Alert & Set Label	Allow & S
• Upload	Supported	Supported	Supported	Supported
Outlook				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Supported	Supported
Salesforce				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Supported	Supported
Slack				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Not Supported	Not Supp
Teams				
• Download	Supported	Supported	Supported	Supported
• Upload	Supported	Supported	Not Supported	Not Supp
Yahoo Mail				
• Download	Supported	Supported	Supported	Supported

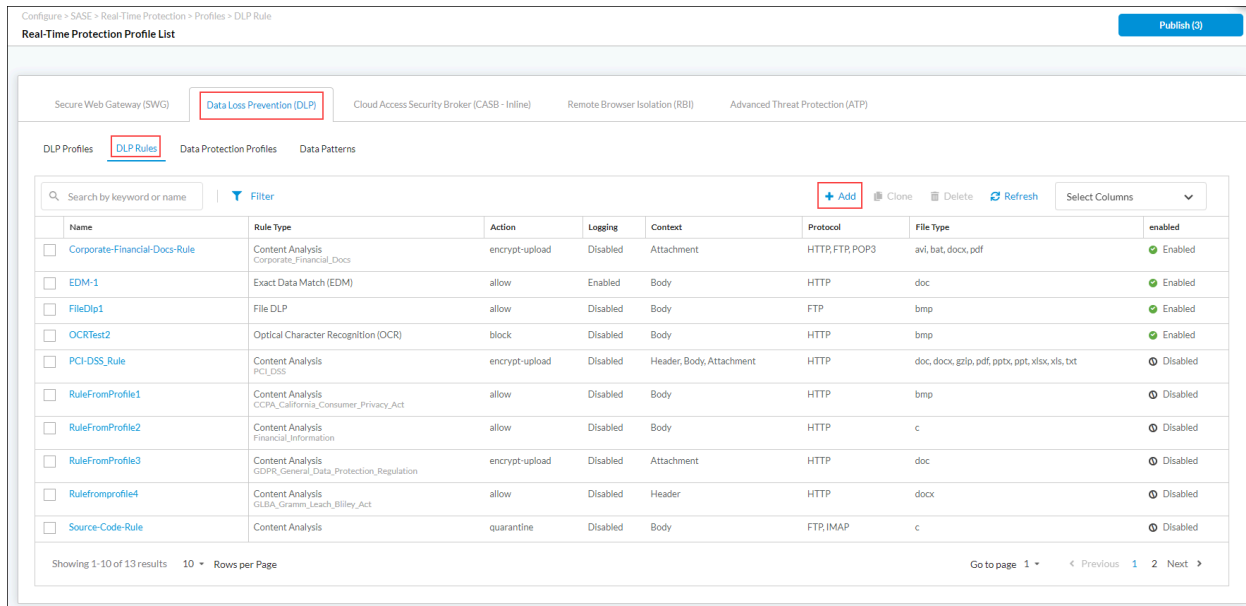
Application	Alert	Allow	Alert & Set Label	Allow & S
<ul style="list-style-type: none"> • Upload 	Supported	Supported	Supported	Supported

To configure rules to use in DLP profiles:

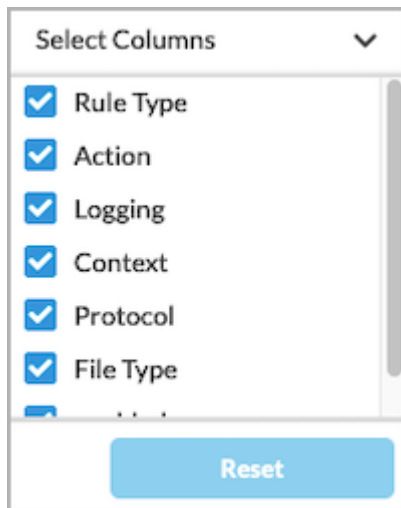
1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



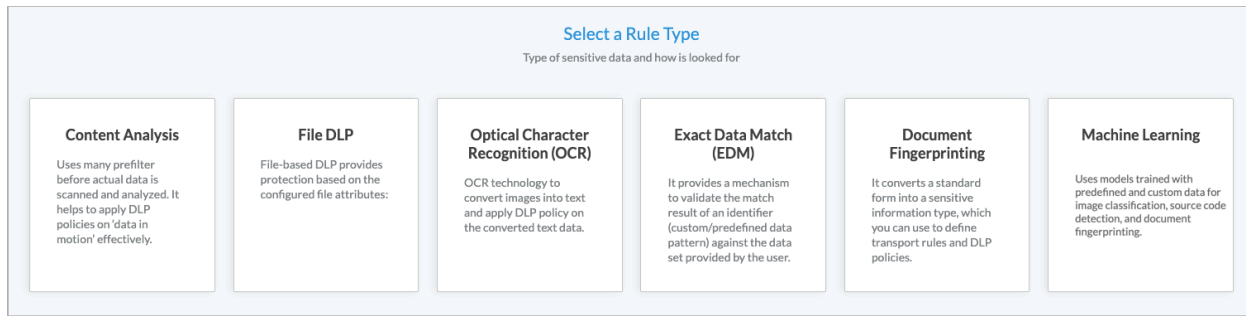
The following screen displays.



2. Select the Data Loss Prevention (DLP) tab, and then select the DLP Rules tab.
3. To customize which columns display, click Select Columns down arrow, and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.



4. Click + Add to add a DLP rule. The Select a Rule Type screen displays. You can create Content Analysis, Exact Data Match (EDM), File DLP, Document Fingerprinting, Machine Learning, and Optical Character Recognition (OCR) rule types. The following sections describe how to configure the DLP file types.



5. **Configure a Content Analysis Rule**—To create a content analysis rule, click the Content Analysis box in the Select a Rule Type screen. The following screen displays, which lists all predefined data protection profiles by default. The pre-defined profiles are:

- AUSTRALIA_FINANCIAL_DATA
- CCPA_California_Consumer_Privacy_Act
- Financial_Information
- GDPR_General_Data_Protection_Regulation
- GLBA_Gramm_Leach_Bliley_Act
- PCI_DSS
- SOCIAL_SECURITY_NUMBER_CONFIDENTIALITY_ACT2000
- SOURCE_CODE_ACT
- UK_ACCESS_TO_MEDICAL_REPORTS_Act1988
- UK_FINANCIAL_DATA
- UK_PII
- US_DRIVERS_LICENSE_NUMBER_ALL_STATES
- US_FEDERAL_TRADE_COMISSION_RULES
- US_FINANCIAL_DATA
- US_HIPAA
- US_PATRIOTS_ACT
- US_PHI
- US_PII
- WESTERN_AUSTRALIA_HEALTH_SERVICES_ACT

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1 **CONTENT ANALYSIS**
2 FILE TYPE
 3 CONFIGURE ACTIVITY, PROTOCOL & CONTEXT
 4 EXCLUDE
 5 ACTION
 6 REVIEW & SUBMIT

Content Analysis

Pre-Defined
User-Defined

All Categories ▾
 All Regions ▾
 Search... ✕

<input type="radio"/> Unselected	CCPA_California_Consumer_Privacy_Act
<input type="radio"/> Unselected	Corporate_Financial_Docs
<input type="radio"/> Unselected	Financial_Information
<input type="radio"/> Unselected	GDPR_General_Data_Protection_Regulation
<input type="radio"/> Unselected	GLBA_Gramm_Leach_Bliley_Act
<input type="radio"/> Unselected	Healthcare
<input type="radio"/> Unselected	Intellectual_Property
<input type="radio"/> Unselected	Legal

Cancel
Back
Skip to Review
Next

6. To view the custom data protection profiles, click User Defined.
7. To add the DLP rule for analysis, click one predefined or one user-defined data protection profile. You can select only one data protection profile, which can be either a predefined or a user-defined profile. To filter the data protection profiles by category, click All Categories. To filter the data protection profiles by region, click All Regions.
8. **Configure a File DLP Rule**—To create a file DLP rule, click File DLP in the Select a Rule Type screen. In the File DLP screen, enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > DLP Rule
Create DLP Rule

1 FILE DLP 2 FILE TYPE 3 CONFIGURE ACTIVITY, PROTOCOL & CONTEXT 4 EXCLUDE 5 ACTION 6 REVIEW & SUBMIT

File type

File DLP

File Name
Enter name

File Size
Enter Min MB
Enter Max MB

SHA256

File Label
Enter input Add

Cancel Back Skip to Review Next

Field	Description
Filename	Enter a name for the file.
File Size (Group of Fields)	
<ul style="list-style-type: none"> Enter Minimum 	Enter the minimum size of the DLP file, and then select the size unit, either megabytes (MB), gigabytes (GB), kilobytes (KB), or bytes. The configured action is taken on all files that are smaller than the minimum size and that match the configured file type. If you set the minimum size to 0, the maximum DLP file size is used for the action.
<ul style="list-style-type: none"> Enter Maximum 	Enter the maximum size of the DLP file, and then select the size unit, either megabytes (MB), gigabytes (GB), kilobytes (KB), or bytes. The configured action is taken on all the files that are larger than the maximum size that match the configured file type.
SHA256	Enter the secure hash algorithm 256-bit (SHA256) value. To enter multiple SHA256 values, separate them by a new line.
File Label	Enter a file label, and then click Add.

9. **Configure an Optical Character Recognition Rule**—To create an optical character recognition (OCR) rule, click Optical Character Recognition in the Select a Rule Type screen. The following screen displays, which lists all predefined data protection profiles by default.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...)

Updated: Wed, 23 Oct 2024 08:39:35 GMT

Copyright © 2024, Versa Networks, Inc.

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1 OCR: Data Protection Methods 2 File Type 3 Configure Activity, Protocol & Context 4 Exclude 5 Action 6 Review & Submit

Optical Character Recognition (OCR)

Data Protection Methods: DLP Profile Data Pattern

Predefined User-Defined

All Categories All Regions Search...

Unselected CCPA_California_Consumer_Privacy_Act

Unselected Financial_Information

Unselected GDPR_General_Data_Protection_Regulation

Unselected GLBA_Gramm_Leach_Bliley_Act

Cancel Back Skip to Review Next

10. To view the custom data protection profiles, click User Defined.
11. To add the DLP rule for analysis, click one predefined or one user-defined data protection profile. You can select only one data protection profile, which can be either a predefined or a user-defined profile. To filter the data protection profiles by category, click All Categories. To filter the data protection profiles by region, click All Regions.
12. **Configure an Exact Data Match Rule**—To create an exact data match rule, click Exact Data Match (EDM) in the Select a Rule Type screen. The following screen displays.

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1 Exact Data Match 2 File Type 3 Configure Activity, Protocol & Context 4 Exclude 5 Action 6 Review & Submit

Exact Data Match (EDM)

Expression

Create Expression Or Upload File Or Select File Name

Boolean Operation

No Expression Selected

13. To create an expression, click Create Expression, and then enter information for the following fields.

Create Expression

Expression Name

expr1

Data Pattern

Select Option

Enter Value

Add


Cancel

Save

Field	Description
Name	Enter a name for the expression.
Data Pattern	Select a data pattern.
Enter Value	Enter a value for the expression, the click Add.

14. Click Save.
15. To upload a CSV file that contains a list of exact data matches, click Upload File.
 - a. Drag and drop the CSV file into the window, or click Select CSV File to upload the file.
 - b. To hash the CSV file, click Hash the File.
 - c. Click Save.

Upload Exact Data Match List



Drag and Drop File or Replace

Select CSV File

☒ Hash the File

Cancel

Save

16. To select a filename, click Select File Name. The Select Filename screen displays.

Select File Name

File Name

Select v Get Columns

Cancel
Save

- i. In the Filename field, select a filename. Note that this list shows the names of CSV files that were previously uploaded. For information about uploading CSV files, see the [Manage DLP Files and Folders](#), below.
- ii. Click Get Columns. The screen displays the columns for each field in the CSV file.

Select File Name

File Name

dlp_edm_test2.csv Get Columns

Field Name	Expression Name	Data Pattern	Action
SNO	Expr0-SNO	Select Option v	Remove
MRID	Expr1-MRID	Select Option v	Remove
SSN	Expr2-SSN	Select Option v	Remove

Cancel
Save

- iii. In the Data Pattern column, select a data pattern to apply to each entry. Click Remove to remove an entry from the CSV file.
- iv. Click Save.

17. **Configure a Document Fingerprinting Rule**—To create a document fingerprinting rule, click the Document Fingerprinting in the Select a Rule Type screen, and then enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1
 Document Fingerprinting

2
 File Type

3
 Configure Activity, Protocol & Context

4
 Exclude

5
 Action

6
 Review & Submit

Document Fingerprinting

Document Fingerprinting

Folder Name

Select v

Similarity Threshold

Field	Description
Folder Name	Select a folder.
Similarity Threshold	<p>Enter the percentage of content that needs to be similar to the previously fingerprinted file stored in the folder path.</p> <p><i>Range:</i> 1 through 100</p> <p><i>Default:</i> None</p>

18. **Configure a Machine Learning Rule**—Versa's ML based classifiers augment automated identification of sensitive data. The following options are available:

- **Image Classification:** Versa's cutting edge ML model classifies predefined images like Credit card, Debit card, social security number, driving license, passport etc.
 Besides the predefined images, Versa's ML model empowers user to train model with the proprietary images.
 The new trained model will detect proprietary and predefined images as well.
 The name or tag of the images can be configured in the 'Image classification' configuration.
- **Source code detection:** It is very common to upload source code to generative AI model like chatGPT. Classical DLP needs a strong parser to detect different snippet of source code of each language. Versa's source detection model is trained with 15+ different type of source code like C, C++, perl, java, ruby, python etc.
 Any small snippet of source code is detected by Source code detection model.
- **Document fingerprint:** Each organizations possess proprietary document types and templates, personalized forms etc.
 Versa's Document fingerprinting detection reads all the document empty template, form and store them in vector database.
 Any data filled in the given template or forms are detected by Document fingerprint classifier.

To create a machine learning rule, click Machine Learning in the Select a Rule Type screen, and then enter information for the following fields.

Configure > SASE > Advanced Security > Profiles > DLP Rule

Machine Learning

☐ Source Code Detection ☐ Finger Printing

Image Classification

Enter Image Name

- Source Code Detection—Click to enable source-code detection.
- Finger Printing—Click to enable finger printing
- Image Classification—Enter the name of an image to classify.

19. Click Next to go to Step 2, File Type in the Create DLP Rule screen.
20. Select one or more file types to be analyzed. To search for specific file types, use the search box. To select all file types, click Select All File Types.

Concerto supports the following file types:

- c
- class
- cpp
- doc
- docx
- html
- msoffice
- pdf
- php
- pl
- ppt
- pptx
- rtf
- sh
- txt
- xls
- xlsx

- xml

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1 CONTENT ANALYSIS 2 FILE TYPE 3 CONFIGURE ACTIVITY, PROTOCOL & CONTEXT 4 EXCLUDE 5 ACTION 6 REVIEW & SUBMIT

File type that will be scanned for Data Loss Prevention













Select file type that will be scanned for Data Loss Prevention

File Type

Search for File Type

☐ Select All File Types

File Types (19)

 c	 doc	 docx	 xml	 cpp	 php
 	 	 	 	 	

Cancel Back Skip to Review Next

21. Click Next.
22. In Step 3 Configure Activity, Protocol, and Context, enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1 CONTENT ANALYSIS 2 FILE TYPE 3 CONFIGURE ACTIVITY, PROTOCOL & CONTEXT 4 EXCLUDE 5 ACTION 6 REVIEW & SUBMIT

Configure Activity, Protocol & Context

Select the way you want to be scanned

Activity

Select

Protocol

Web Protocol [Select All](#)


☒ HTTP

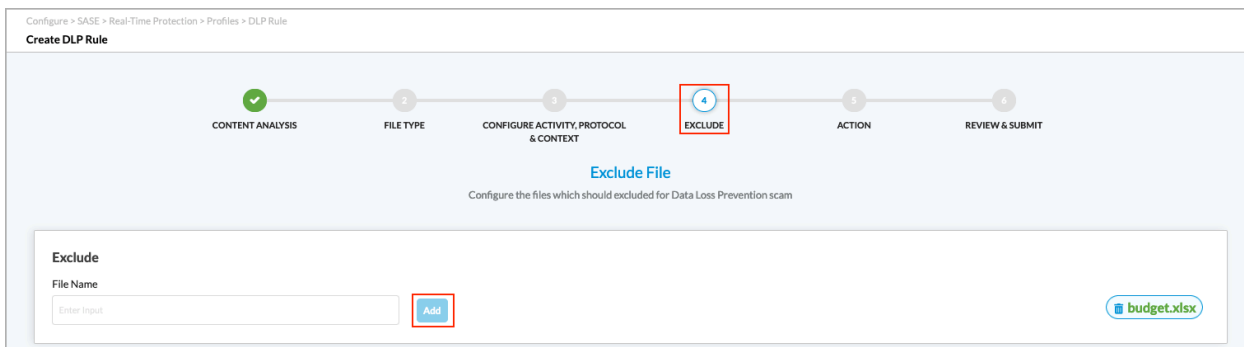
Context [Select All](#)

☒ Header ☐ Body ☐ Attachment

Cancel Back Skip to Review Next

Field	Description
Activity	<p>Select the direction of the traffic on which to apply the rule:</p> <ul style="list-style-type: none"> Both—Apply the rule to both download and upload traffic. Download—Apply the rule when the client requests data from a server. Upload—Apply the rule when the client posts data to a server.
Protocol	<p>Click the protocol to scan:</p> <ul style="list-style-type: none"> Web Protocol <ul style="list-style-type: none"> HTTP
Context	<p>Select one or more HTTP contexts of data to scan:</p> <ul style="list-style-type: none"> Attachment—Data in an attachment Body—Data in the body Header—Data in the header of a packet

23. Click Next.
24. In Step 4, Exclude, in the Filename field, enter the names of a file to exclude, for example, budget.xlsx, and then click Add. The filename displays to the right of the Add button. You can exclude multiple files. To delete a filename from the list, click the  Trash icon next to the filename.



Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

1 CONTENT ANALYSIS 2 FILE TYPE 3 CONFIGURE ACTIVITY, PROTOCOL & CONTEXT 4 EXCLUDE 5 ACTION 6 REVIEW & SUBMIT

Exclude File

Configure the files which should be excluded for Data Loss Prevention scan

Exclude

File Name

Enter Input

Add

budget.xlsx

25. Click Next.
26. In Step 5, Action, enter information for the following fields.

The following table shows the applications supported by DLP and whether file-name matching is supported for upload and download.

Applications	Download	Upload
Box	Supported	Supported
Dropbox	Supported	Not supported
Github	Supported	Supported
Gmail	Supported	Supported
Google Chat	Supported	Not supported
Google Docs	Supported	Not supported
Google Drive	Supported	Not supported
MS Teams (web)	Supported	Not supported
Office365	Supported	Not supported
OneDrive	Supported	Not supported
Salesforce	Supported	Supported
Service Now Developer Console	Supported	Supported
Sharepoint	Supported	Not supported
Slack	Supported	Supported
Yahoo Mail	Supported	Not supported

Configure > SASE > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

✓

✓

✓

✓

5

6

Rule Type: Content Analysis

File Type

Configure Activity, Protocol & Context

Exclude

Action

Review & Submit

Action

Select the default action for the profile

Action

Select

☐ Logging

Notification Profile

Select

Labels

Select

Cancel

Back

Skip to Review

Next

Field	Description
Action	<p>Select an action to take if the traffic matches the rule:</p> <ul style="list-style-type: none"> ◦ Alert—Allow traffic to pass and log it to Versa Analytics ◦ Allow—Allow traffic to pass without logging it to Versa Analytics ◦ Block—Drop the traffic without sending a notification to the client host that originated the traffic. ◦ Encrypt—Encrypt the traffic before sending it. ◦ Encrypt Upload—Encrypt the file and send it to the customer-provided cloud portal. To decrypt the file and view its contents, use a symmetric key. The session is rejected. ◦ Quarantine—Send the traffic to the customer-provided cloud portal without encrypting it. ◦ Redaction—If a rule match is detected in an editable, text-based file, change the content of the matched packet to random characters. Redaction is supported for exact data matches (EDMs) for file types .c, .html, .php, .sh, .txt, and .xml. ◦ Reject—Drop the traffic and send a notification to the client host indicating that the traffic was dropped.
Logging	Click to enable LEF logging to Analytics, which logs all actions to Versa Analytics, except for actions that explicitly do not log. If you do not enable logging, no logging information is sent to Versa Analytics.
Notification Profile	Select a notification profile. To configure a notification profile, see Configure SASE User-Defined Objects .
Set Label	Click Set Label or Remove Label to set or remove a sensitivity label on a file before uploading or downloading it.
Enter Label	Enter the text of the label to be set or removed.

27. Click Next.

28. In Step 5, Review and Submit, review the configuration entries

29. To change any of the information, click the  Edit icon and then make the required changes.

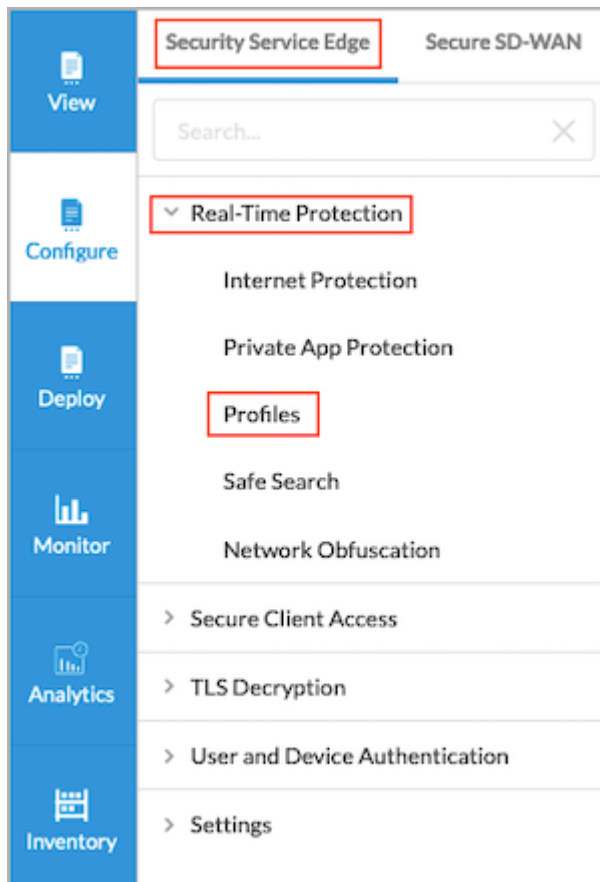
30. Click Save to create the DLP rule.

Configure DLP Profiles

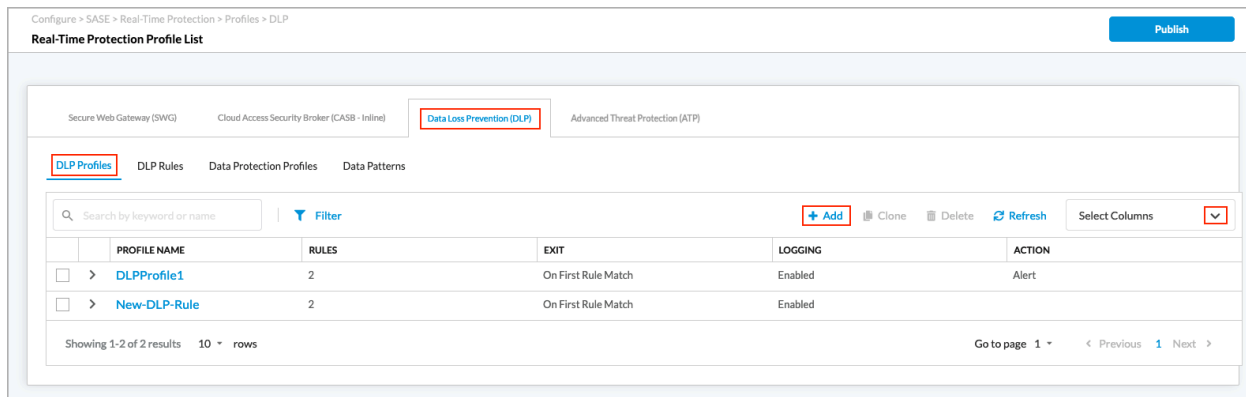
A DLP profile consists of one or more DLP rules.

To configure a DLP profile:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



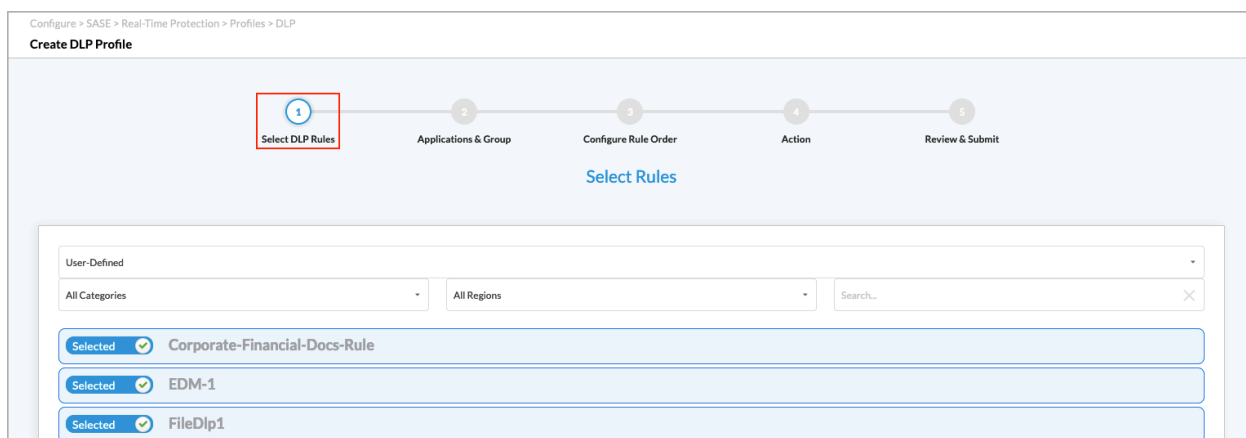
2. Select the Data Loss Prevention (DLP) tab. The following screen displays.



3. Select the DLP Profiles subtab.
4. To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.



5. Click the + Add icon to add a new DLP profile. The Create DLP Profile screen displays.



6. In Step 1, Select DLP Rules, select one or more DLP rules. To filter the types of rules that are displayed, use the User-Defined, All Categories, and All Regions boxes.

7. Click Next to go to Step 2, Applications & Group. Enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > DLP

Create DLP Profile

1

Select DLP Rules

2

Applications & Group

3

Configure Rule Order

4

Action

5

Review & Submit

Applications & Group

Applications & Group

Additional Application Group

Select

Applications

Search for Application

User Defined Applications (2)

CustomApp1

sf

Predefined Applications (4018)

01NET

050PLUS

0ZZ0

10050NET

10086CN

104COM

1111TW

114LA

115COM

118114CN

11ST

123PEOPLE

Cancel

Back

Skip to Review

Next

Field	Description
Additional Application Group	Select an additional application group. You can select only one group. Note that only user-defined application groups are listed.
Applications	Enter the name of an application to search for.
User Defined Applications	Select one or more user-defined applications.
Predefined Applications	Select one or more predefined applications.

8. Click Next to go to Step 3, Configure Rule Order.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...)
Updated: Wed, 23 Oct 2024 08:39:35 GMT
Copyright © 2024, Versa Networks, Inc.

30

Configure > SASE > Real-Time Protection > Profiles > DLP

Create DLP Profile

1 Select DLP Rules 2 Applications & Group 3 **Configure Rule Order** 4 Action 5 Review & Submit

Configure Rule Order

1	Corporate-Financial-Docs-Rule
2	FileDlp1
3	PCI-DSS_Rule

9. If you select two or more DLP rules in the Select DLP Rules screen, you can change the order in which the rules are processed by dragging and dropping the rules to the desired order. For example, the following screen shows that the rules have been reordered so that the FileDlp1 rule is processed first, followed by Corporate-Financial-Docs-Rule and then PCI-DSS_Rule.

1	FileDlp1
2	Corporate-Financial-Docs-Rule
3	PCI-DSS_Rule

10. Click Next to go to Step 4, Action. Enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > DLP

Create DLP Profile

1 Select DLP Rules 2 Applications & Group 3 Configure Rule Order 4 **Action** 5 Review & Submit

Configure Action

Actions

Default Action

Select v

☐ Exit On First Rule Match

☐ Logging

Field	Description
Default Action	Click the down arrow, and the select a default action. The default action is applied if none of the scanned data matches a rule.

Field	Description
	<ul style="list-style-type: none"> Alert Allow Block Reject
Exit on First Rule Match	Click to exit rule processing after the first match occurs.
Logging	Enable logging of the DLP rules processing. All logs are sent to Versa Analytics.

11. Click Next.
12. In Step 5, Review & Submit. Enter a name for the DLP rule and, optionally, a description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the rules.

Configure > SASE > Real-Time Protection > Profiles > DLP

Create DLP Profile

Progress bar: Select DLP Rules (✓), Applications & Group (✓), Configure Rule Order (✓), Action (✓), Review & Submit (5, highlighted)

Review your DLP configuration below

General

Name * ⓘ Description

Tags

Applications & Group [Edit](#)

Predefined Applications	User Defined Applications	Additional Application Group
	CustomApp1	

Buttons: Cancel, Back, Save

13. Review the configuration.
14. To change any of the information, click the Edit icon and then make the changes.
15. After review, click Save to create the new DLP profile.

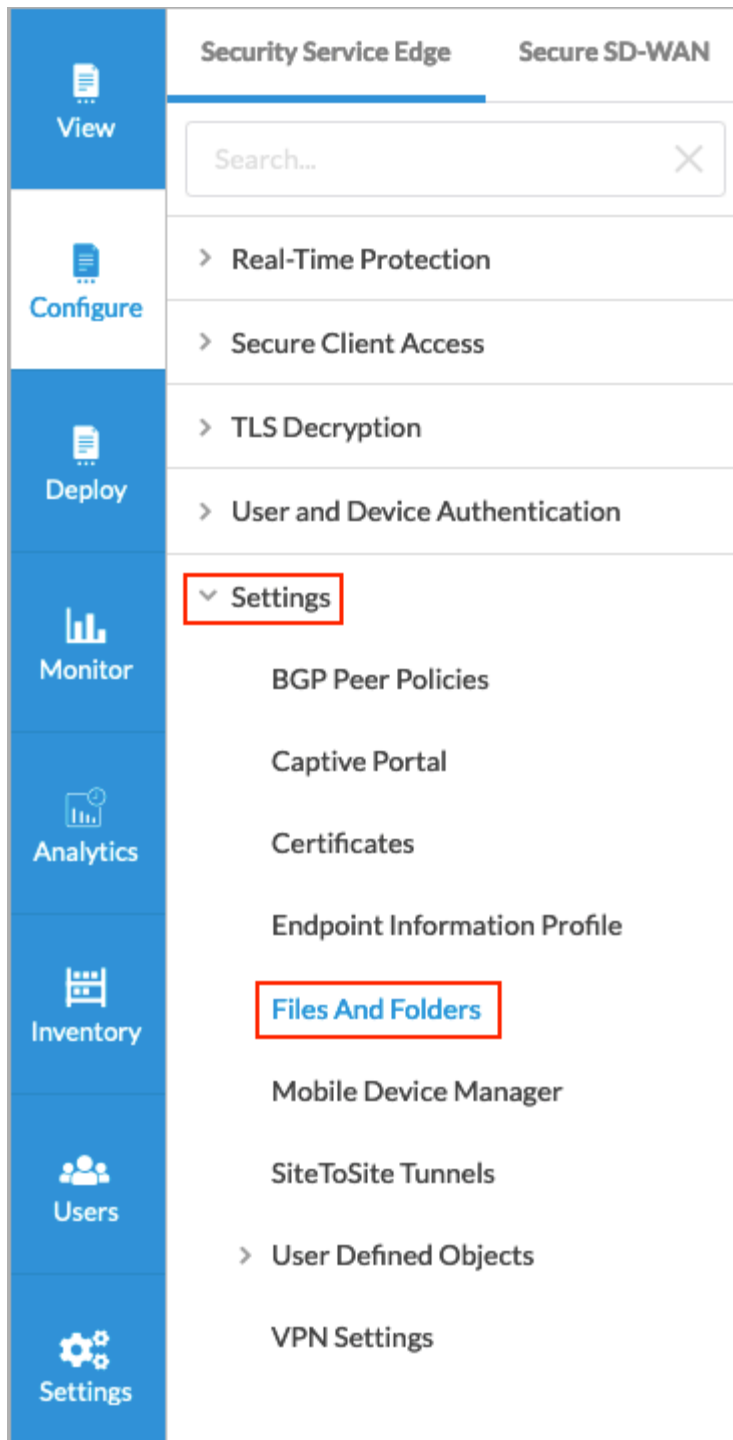
You can use the DLP profiles when you configure internet protection rules. For more information, see [Configure SASE Internet Protection Rules](#).

Manage DLP Files and Folders

You can upload files and then perform exact data matching or document fingerprinting on them. You can create folders to manage the files. By default, the DLP software creates three folders: DLP, EDM, and Fingerprints. You can create additional folders. After you upload the files, you can use them when you create exact data match or document fingerprinting rules.

To manage DLP files and folders:

1. Go to Configure > Settings > Files and Folders.



2. Select Files and Folders in the left navigation bar. The following screen displays. Note that the ➤ Expand icon displays only when a folder contains files.

Configure > SASE > Settings > File & Folder Management

File & Folder Management Publish

Below are all the File & Folder Management

Search + Add Folder Upload File Refresh Select Columns

>	Name	Date Modified	Modified By	File Count	Checksum	File Size	Actions
▼	DLP	3/20/2023, 1:39:01 PM	Administrator			-	
▼	EDM	3/20/2023, 1:39:01 PM	Administrator	2		-	
	dlp_edm_test2.csv	3/22/2023, 10:37:01 PM	Administrator		bf005f5f29d75de6f018890e3749...	1.83 KB	
	dlp_edm_test1.csv	3/23/2023, 12:34:10 AM	Administrator		81c28ba85c9f4f3764ec2cca0601...	1.83 KB	
▼	Fingerprints	3/20/2023, 1:39:01 PM	Administrator			-	
	Folder1	7/26/2023, 9:52:18 PM	Administrator			-	

- To customize which columns display, click Select Columns down arrow, and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

Select Columns

▼

- ☒ Date Modified
- ☒ Modified By
- ☒ File Count
- ☒ Checksum
- ☒ File Size

Reset

- Click the **+ Add Folder** icon to add a new folder. In the Add Folder screen, enter information for the following fields.

Add Folder

Enter the name of the sub-folder

Where should folder be placed?


Select

Folder Name

Cancel

Add

Field	Description
Where should the folder be placed?	Select the location for the new folder.
Folder Name	Enter a name for the new folder.

- Click Add to add the new folder.
- To upload a new file, click the  Upload Folder icon. In the Upload File screen, enter information for the following fields.

×

Upload File

Uploaded files will be added to:

Where should folder be placed?

Select

▼

☒ Hash the File

Upload File

Cancel

Upload

Field	Description
Where should the folder be placed?	Select the folder in which to place the file
Hash the File	Click to perform a hash operation on the file that you are uploading.
Upload File	Click to upload a file, and then select the file to upload from the pop-up window. For EDM processing, files must be in .csv format. For document fingerprinting processing, files must be in .doc, .docx., or .pdf format.

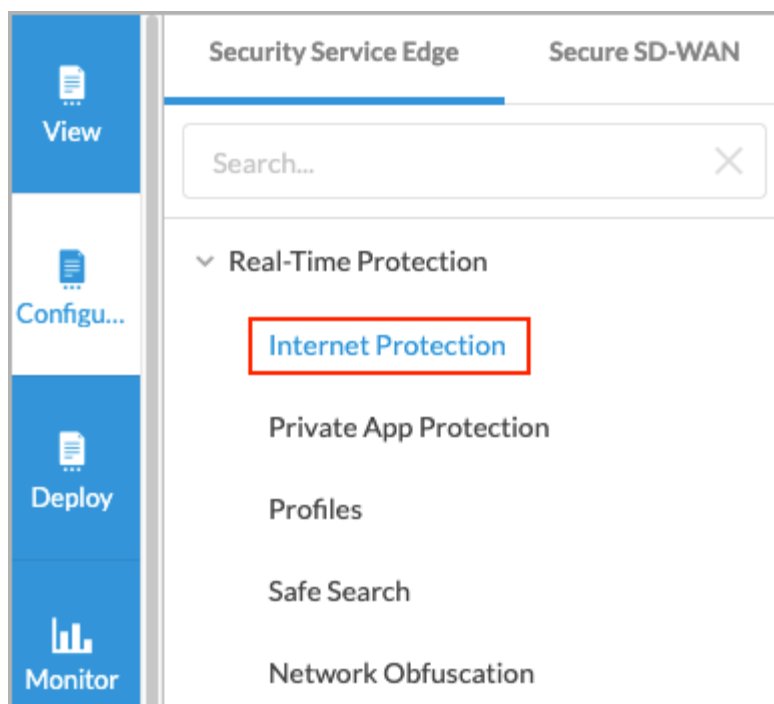
7. Click Upload to upload the file.

Associate a DLP Profile with a SASE Internet Protection Rule

To oversee, track, and report all data transactions in the network and to scan all content that passes through an organization's ports and protocols to ensure data security in the organization, you can associate a DLP profile with a SASE internet protection rule. DLP provides a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. You use DLP to protect and secure an organization's data and to comply with regulations.

To associate a DLP profile with a SASE internet protection rule:

1. Go to Configure > Real-Time Protection > Internet Protection.



2. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays. For more information, see [Configure SASE Internet Protection Rules](#).
3. In the Security Enforcement screen, select Profiles, and then select the Data Loss Prevention (DLP) tab.

Configure > SASE > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Applications

Users & Groups

Endpoint Information Profile (EIP)

GEO Locations

Network Layer 3-4

Security Enforcement

Review & Deploy

We have preselected your security enforcements, below
You can unselect and customize any configuration you'd like to enforce.

☐

Allow

Allow all traffic that matches the rule to pass

☐

Deny

Drop all traffic that matches the rule

☐

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

Profiles

Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Advanced Threat Protection (ATP)

Remote Browser Isolation (RBI)

Data Loss Prevention Enabled

DLPProfile1

+ Create New

DLPProfile1

Exit On First Rule Match : Enabled Default Action : Alert

Order	Name	Rule Type	Activities	Context	Protocol	File Type
1	Source-Code-Rule	Content Analysis	quarantine	Body	FTP,IMAP	c
2	Corporate-Financial-Docs-Rule	Content Analysis	encrypt-upload	Attachment	HTTP,FTP,POP3	avi, bat, docx, pdf

Cancel

Back

Skip to Review

Next

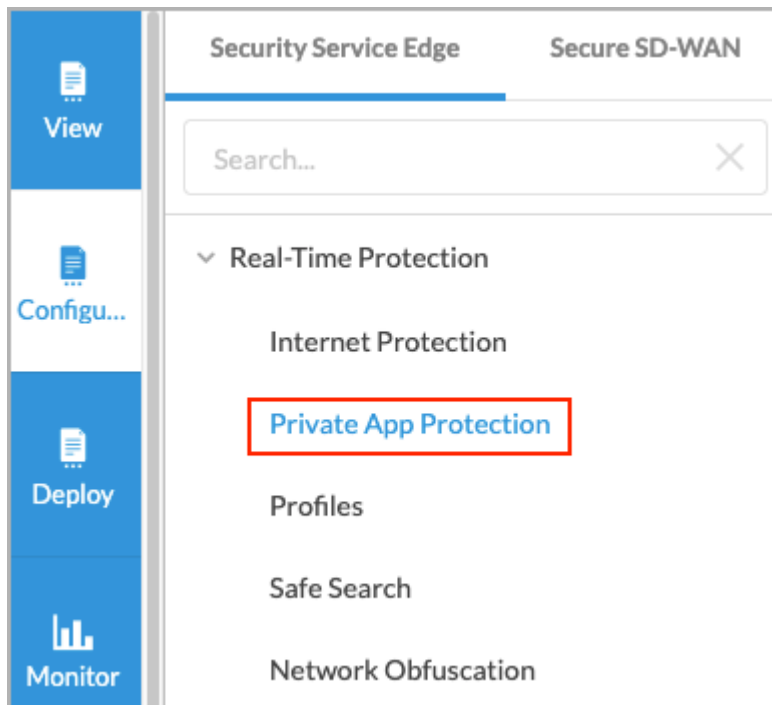
4. Click the slider bar to enable DLP.
5. Select a DLP profile from the drop-down list.
6. Click Next.
7. In the Review & Deploy, review your selections and make any needed updates.
8. Click Save.

Associate a DLP Profile with a Private Application Protection Rule

You can associate a DLP profile with a private application protection rule. DLP provides a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. You use DLP to protect and secure an organization's data and to comply with regulations.

To associate a DLP profile with a private application rule:

1. Go to Configure > Real-Time Protection > Private Application Protection.



2. In the Private Application Protection Rules List screen, click + Add to create a rule. The Create Private Application Protection Rule screen displays.
3. Select the Security Enforcement screen, and then select Profiles.

Configure > SASE > Real-Time Protection > Private App Protection

Create Private App Protection Rule

1

Applications

2

Users & Groups

3

Endpoint Information Profile (EIP)

4

GEO Locations

5

Network Layer 3-4

6

Security Enforcement

7

Review & Deploy

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

✓

Allow

Allow all traffic that matches the rule to pass

☐

⊘

Deny

Drop all traffic that matches the rule

☐

⊘

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

ⓘ

✓

Profiles

Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Data Loss Prevention (DLP)

Remote Browser Isolation (RBI)

Data Loss Prevention Enabled

☒

DLPProfile1

+ Create New

DLPPProfile1

Exit On First Rule Match: Enabled Default Action: Alert

Order	Name	Rule Type	Activities	Context	Protocol	File Type
1	Source-Code-Rule	Content Analysis	quarantine	Body	FTP, IMAP	c
2	Corporate-Financial-Docs-Rule	Content Analysis	encrypt-upload	Attachment	HTTP, FTP, POP3	avi, bat, docx, pdf

Cancel

Back

Skip to Review

Next

4. Select the Data Loss Prevention (DLP) tab.
5. Click the slider bar to enable DLP.
6. Select a DLP profile from the drop-down list.
7. Click Next.
8. In the Review & Deploy, review your selections and make any needed updates.
9. Click Save.

Additional Information

[Configure SASE Internet Protection Rules](#)

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Data_Loss_Prevent...)

Updated: Wed, 23 Oct 2024 08:39:35 GMT

Copyright © 2024, Versa Networks, Inc.