
Configure Offline Data Loss Prevention

Offline 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.

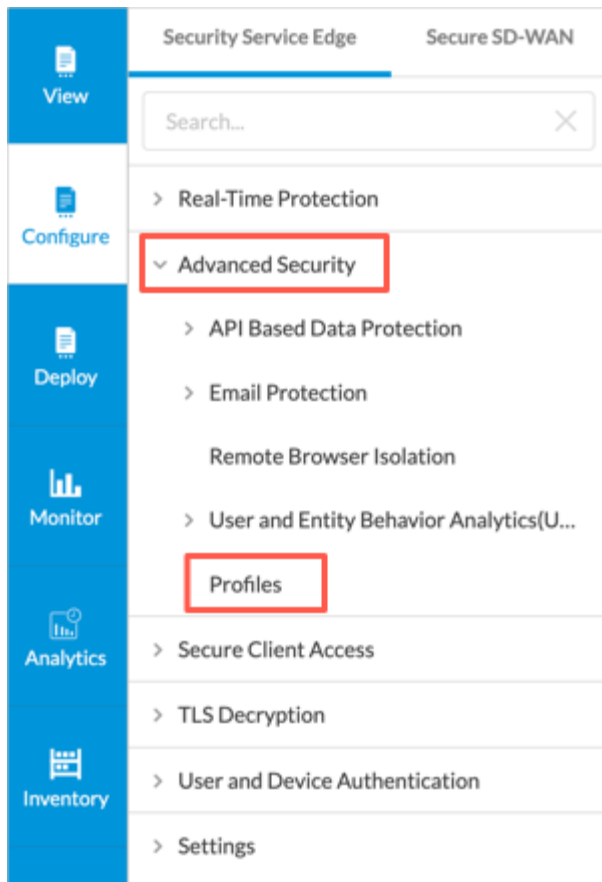
To configure DLP, you create a DLP profile that you associate with a security policy. To create the DLP profile, you do the following:

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.

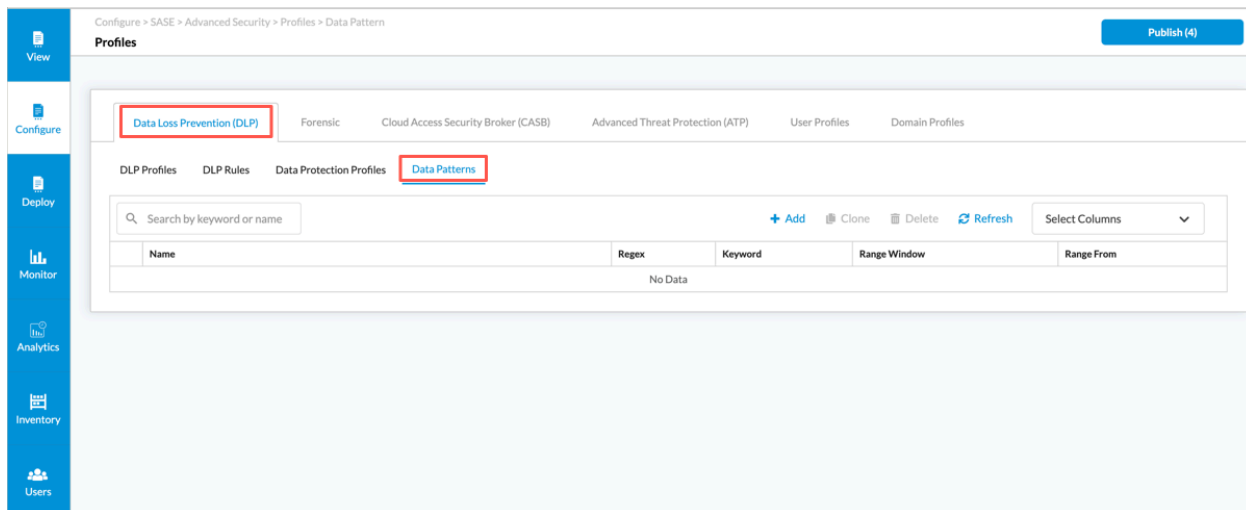
Configure Custom Data Patterns

To configure custom data patterns:

1. Go to Configure > Secure Services Edge > Advanced Security > Profiles.



2. Select the Data Loss Prevention (DLP) tab, and then select the Data Patterns subtab.



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 screen, 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 an exact regular expression to search for in a file, for example, Employee.*Salary.
Keywords	Enter one or more keywords to search for in a file. Once a keyword is found, the DLP engine scans for the regex 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.

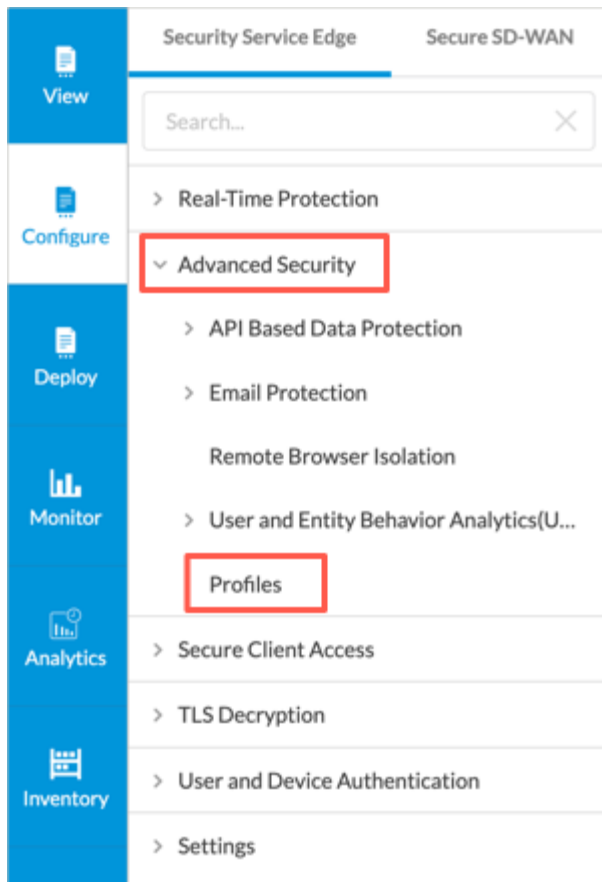
Configure Data Protection Profiles

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).

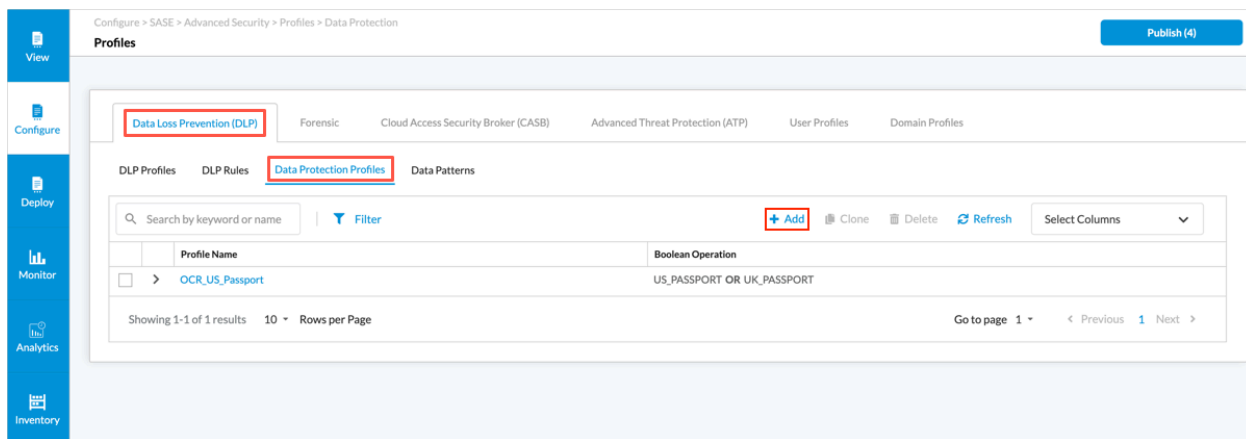
After you create a data protection profile, you can use it as part of the enforcement actions on a policy rule in a security access control policy.

To configure a data protection profile:

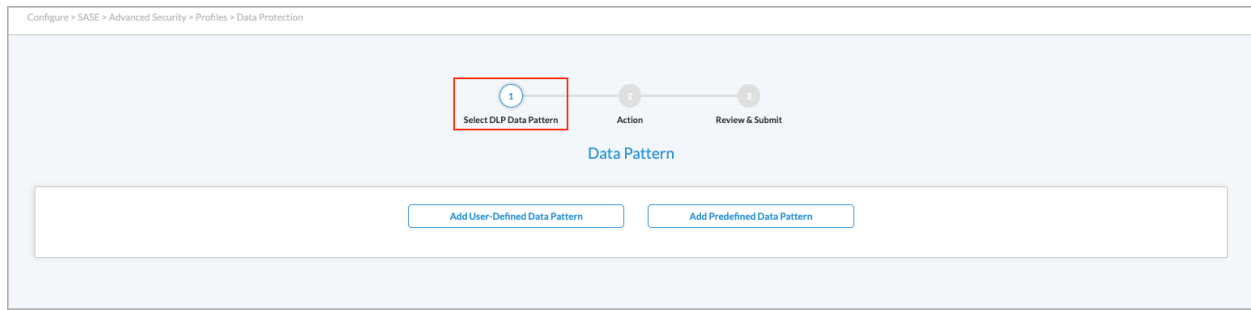
1. Go to Configure > Secure Services Edge > Advanced Security > Profiles.



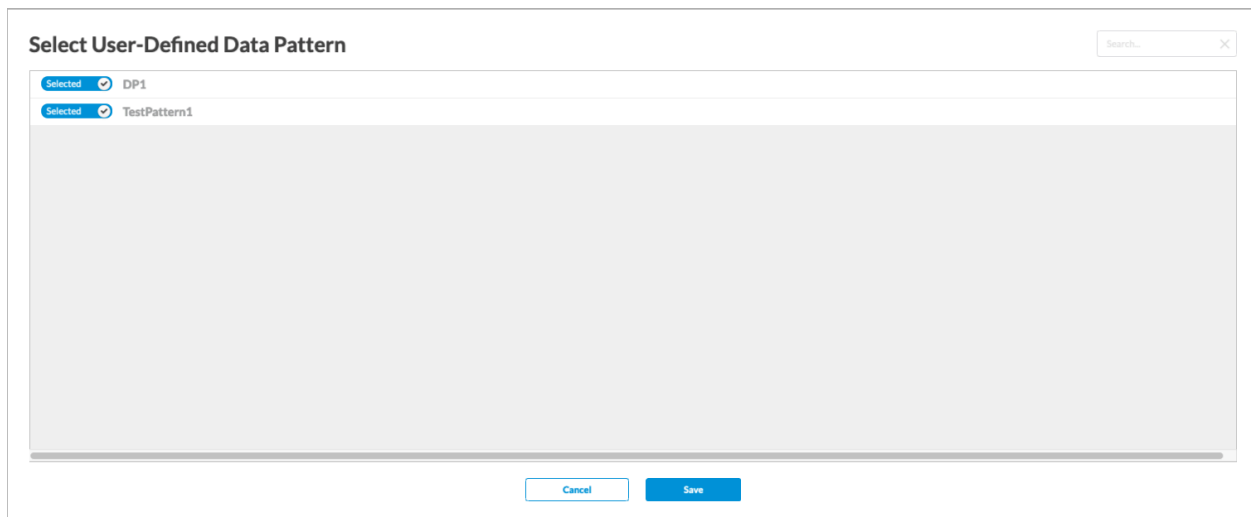
2. Select the Data Loss Prevention (DLP) tab, and then select the Data Protection Profiles subtab.



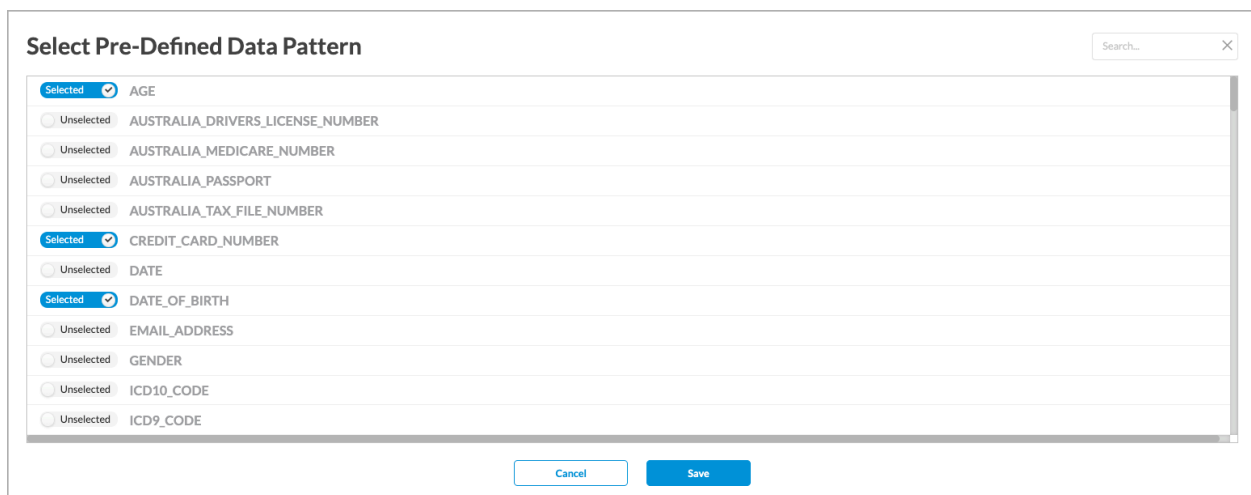
3. To create user-defined profiles, click **+** Add icon. The Data Pattern screen displays. You can add either user-defined (custom) or predefined data patterns.



4. Click Add User-Defined Data Pattern, and then select one or more custom data patterns to use in the data protection profile.



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



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

Configure > SASE > Advanced Security > Profiles > Data Protection

1 Select DLP Data Pattern 2 Action 3 Review & Submit

Data Pattern

Add User-Defined Data Pattern Add Predefined Data Pattern

Name	Type	
AGE	Predefined	
DATE_OF_BIRTH	Predefined	
EMAIL_ADDRESS	Predefined	

8. Click Next.

SELECT DLP DATA PATTERN ACTION REVIEW & SUBMIT

Configure Action

Boolean Operation

No patterns selected

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 + NEAR

9. In Step 2, Action, 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. The Boolean operation can include multiple data patterns, with each separated by a Boolean operator. The following example shows Boolean operation created from the data patterns shown in the previous screenshot:

Boolean Operation

DATE_OF_BIRTH ▾ OR ▾ CREDIT_CARD_NUMBER ▾ NEAR ▾ EMAIL_ADDRESS ▾

[Clear All](#)

Click to add data identifier to rule

+ DATE_OF_BIRTH

+ CREDIT_CARD_NUMBER

+ EMAIL_ADDRESS + IP_ADDRESS

Click to add data operator to rule

+ AND + OR + NEAR

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 + NEAR

Remove Selection

DP1

TestPattern1

AGE

CREDIT_CARD_NUMBER

DATE_OF_BIRTH

10. Click Next.
11. 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.

SELECT DLP DATA PATTERN ACTION REVIEW & SUBMIT

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

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

- 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 of two rule types:
 - 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.
 - Optical character recognition (OCR)—Converts images to text and applies DLP policies on the converted text data.
 - Machine Learning—Uses models trained with predefined and custom data for image classification, source code detection, and document fingerprinting.
- Protocol monitoring—DLP monitoring can scan the HTTP protocol.
- File-type filtering—You can configure data filters based on 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
• Upload	Supported	Supported	Not Supported	Not Supported

Application	Alert	Allow	Alert & Set Label	Allow & S
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
• Upload	Supported	Supported	Supported	Supported
Outlook				

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

Updated: Wed, 23 Oct 2024 08:38:49 GMT

Copyright © 2024, Versa Networks, Inc.

Application	Alert	Allow	Alert & Set Label	Allow & S
• 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
• Upload	Supported	Supported	Supported	Supported

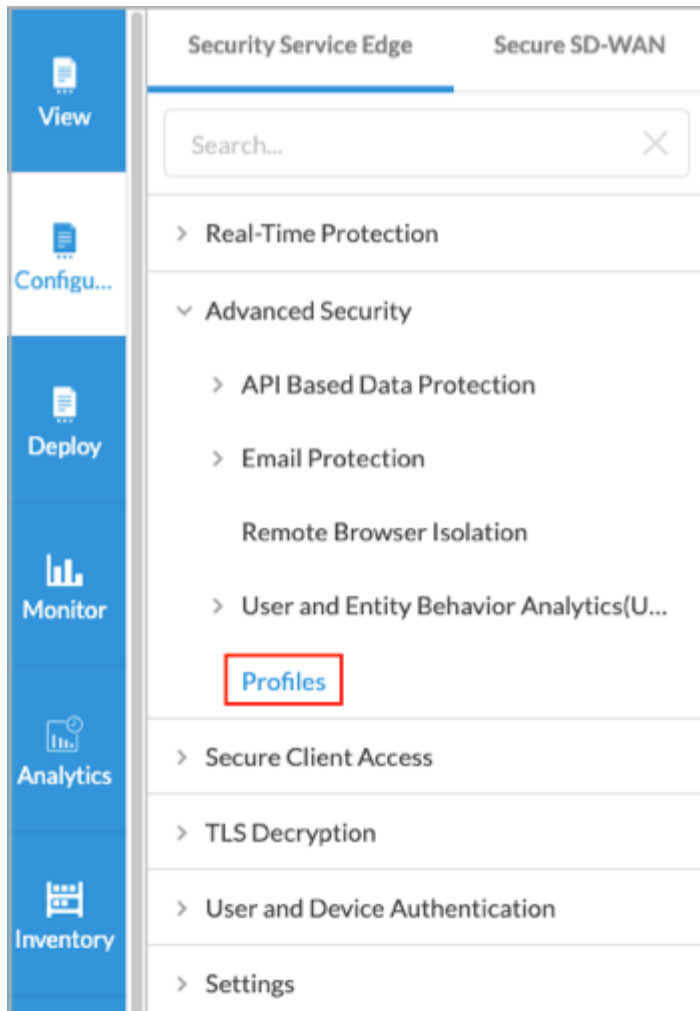
To configure rules to use in DLP profiles:

1. Go to Configure > Secure Services Edge > Advanced Security > Profiles.

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

Updated: Wed, 23 Oct 2024 08:38:49 GMT

Copyright © 2024, Versa Networks, Inc.



The following screen displays.

Configure > SASE > Advanced Security > Profiles > DLP Rule

Profiles Publish (4)

Data Loss Prevention (DLP) Forensic Cloud Access Security Broker (CASB) Advanced Threat Protection (ATP) User Profiles Domain Profiles

DLP Profiles **DLP Rules** Data Protection Profiles Data Patterns

Search by keyword or name Filter + Add Clone Delete Refresh Select Columns

Name	Rule Type	Action	Logging	Context	Protocol	File Type	enabled
<input type="checkbox"/> API-Rule-EDM	Exact Data Match (EDM)	redaction	Enabled	Attachment, Body	HTTP	html	Enabled
<input type="checkbox"/> API-Rule-EDM-Tokenization	Exact Data Match (EDM)	tokenization	Enabled	Attachment, Body	HTTP	sh	Enabled
<input type="checkbox"/> API_Rule_FileDLP	File DLP	encrypt	Enabled	Attachment, Body, Header	HTTP	pl	Enabled
<input type="checkbox"/> API_Rule_Fingerprint	Document Fingerprinting	block	Enabled	Attachment, Body	HTTP	pdf	Enabled
<input type="checkbox"/> API-Rule-OCR	Optical Character Recognition (OCR)	block	Enabled	Body, Attachment	HTTP	any	Enabled
<input type="checkbox"/> API-Rule-PCI_DSS	Content Analysis PCI_DSS	encrypt	Enabled	Attachment	HTTP	pdf	Enabled
<input type="checkbox"/> API-Rule-SourceCode	Content Analysis SOURCE_CODE_ACT	reject	Enabled	Attachment	HTTP	php, c	Enabled
<input type="checkbox"/> API-Rule-US_HIPAA	Content Analysis US_HIPAA	block	Enabled	Body, Attachment	HTTP	xlsx	Enabled
<input type="checkbox"/> RBI-Rule-PCI_DSS	Content Analysis PCI_DSS	block	Enabled	Attachment	HTTP	pdf	Enabled
<input type="checkbox"/> Rule_ML_US_Passport	Machine Learning	block	Enabled	Attachment, Body	HTTP	jpg, png	Enabled

Showing 1-10 of 10 results 10 Rows per Page Go to page 1 < Previous 1 Next >

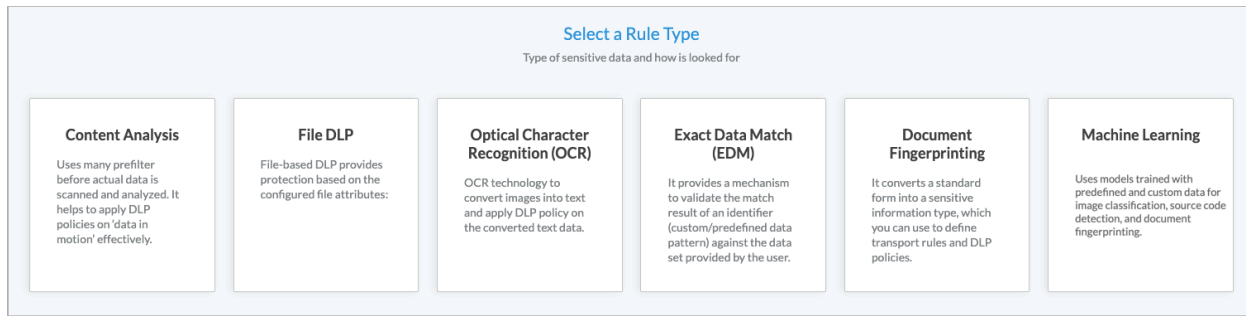
2. Select the Data Loss Prevention (DLP) tab, and then select the DLP Rules tab.
3. To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

Select Columns ▼

- ☒ Rule Type
- ☒ Action
- ☒ Logging
- ☒ Context
- ☒ Protocol
- ☒ File Type

Reset

4. Click + Add to add a DLP rule. The Select a Rule Type screen displays. You can create Content Analysis, File DLP, Optical Character Recognition (OCR), Exact Data Match (EDM), Document Fingerprinting, and Machine Learning 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_COMMISSION_RULES
- US_FINANCIAL_DATA
- US_HIPAA
- US_PATRIOTS_ACT
- US_PHI
- US_PII
- WESTERN_AUSTRALIA_HEALTH_SERVICES_ACT

Configure > SASE > Advanced Security > Profiles > DLP Rule

1
Rule Type: Content Analysis

2
File Type

3
Configure Activity, Protocol & Context

4
Exclude

5
Action

6
Review & Submit

Content Analysis

Severity Level

Select

Severity Value

Predefined
User-Defined

All Categories
All Regions
Search...

☐ Unselected CCPA_California_Consumer_Privacy_Act

☐ Unselected Financial_Information

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 > Advanced Security > Profiles > DLP Rule

1

2

3

4

5

6

File DLP File Type Configure Activity, Protocol & Context Exclude Action Review & Submit

File type

File DLP

File Name

Enter name

File Size

SHA256

Enter sha256s (Separated by new line)

File Label

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.

Configure > SASE > Advanced Security > Profiles > 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

Unselected US_PHI

Unselected PCI_DSS

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 > Advanced Security > Profiles > 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.

1. Drag and drop the CSV file into the window, or click Select CSV File to upload the file.

2. To hash the CSV file, click Hash the File.

3. 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

- a. In the File Name 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.
- b. 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

- c. In the Data Pattern column, select a data pattern to apply to each entry. Click Remove to remove an entry from the CSV file.
- d. 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 > Advanced Security > Profiles > 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:** 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

1

2

3

4

5

6

Machine Learning

File Type

Configure Activity, Protocol & Context

Exclude

Action

Review & Submit

Machine Learning

☐ Source Code Detection
 ☐ Finger Printing

Image Classification

- 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 > Advanced Security > Profiles > DLP Rule

Rule Type: 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 (84)

avi	bat	bmp	cab	c	dll	doc	docx
dwg	coff	xml	applelist	cpp	php	mach_o	wav

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 > Advanced Security > Profiles > DLP Rule

Rule Type: Content Analysis 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

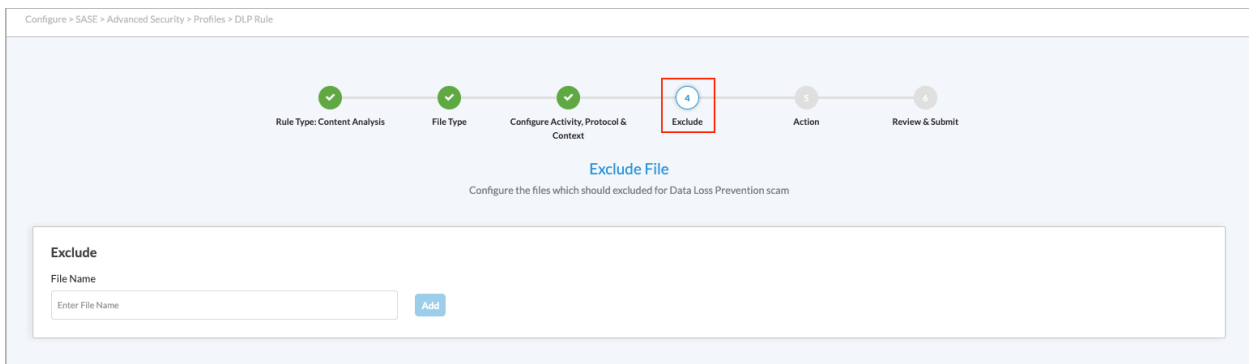
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Offline_Data_Loss_...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Offline_Data_Loss_...)

Updated: Wed, 23 Oct 2024 08:38:49 GMT

Copyright © 2024, Versa Networks, Inc.

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.



The screenshot shows the configuration interface for a DLP rule. At the top, a breadcrumb trail reads "Configure > SASE > Advanced Security > Profiles > DLP Rule". Below this is a progress bar with six steps: "Rule Type: Content Analysis", "File Type", "Configure Activity, Protocol & Context", "Exclude" (highlighted with a red box and a blue circle with the number 4), "Action", and "Review & Submit". The "Exclude" step is active, and the main area is titled "Exclude File" with the subtitle "Configure the files which should be excluded for Data Loss Prevention scan". Below the title is a form with the label "Exclude" and "File Name". There is a text input field with the placeholder "Enter File Name" and a blue "Add" button to its right.

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

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

Updated: Wed, 23 Oct 2024 08:38:49 GMT

Copyright © 2024, Versa Networks, Inc.

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 > Advanced Security > Profiles > DLP Rule

✓

Rule Type: Content Analysis

✓

File Type

✓

Configure Activity, Protocol & Context

✓

Exclude

5

Action

6

Review & Submit

Action

Select the default action for the profile

Action

Select

☐ Logging

Notification Profile

Select

Labels

Select

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 6, Review and Submit, review the configuration entries

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

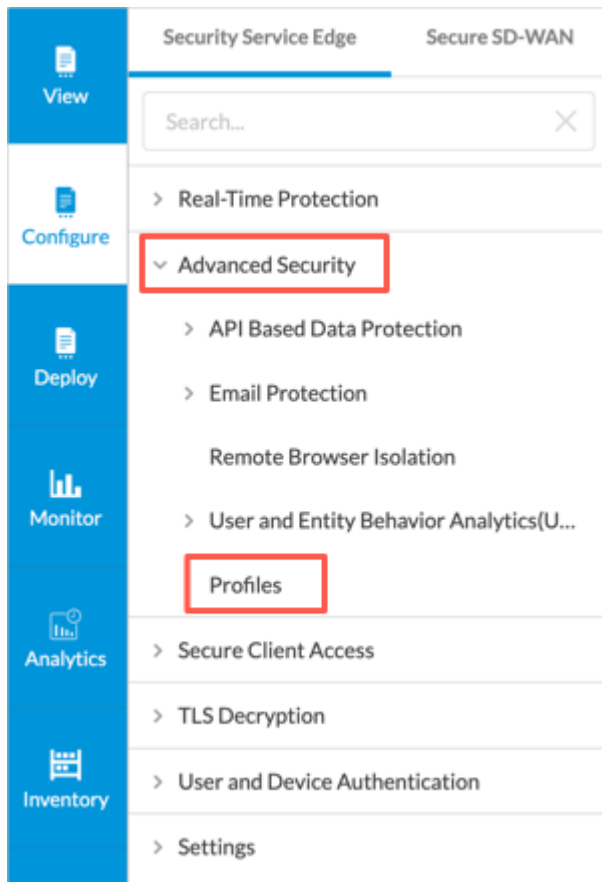
30. Click Save to create the DLP rule.

Configure DLP Profiles

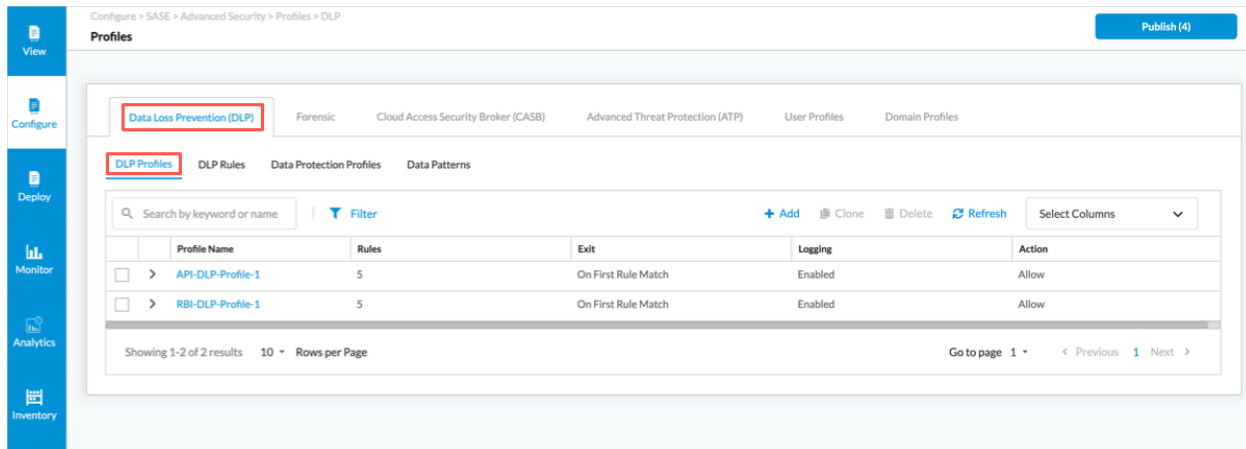
A DLP profile consists of one or more DLP rules.

To configure a DLP profile:

1. Go to Configure > Secure Services Edge > Advanced Security > Profiles.



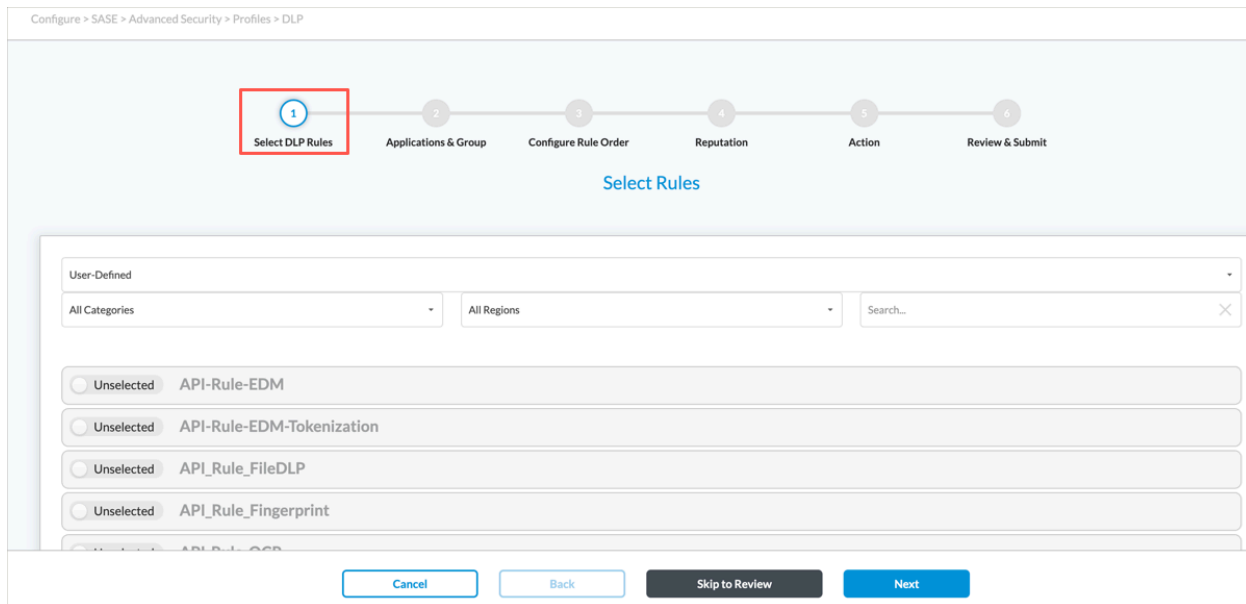
2. In the Data Loss Prevention (DLP) tab, select DLP Profiles tab.



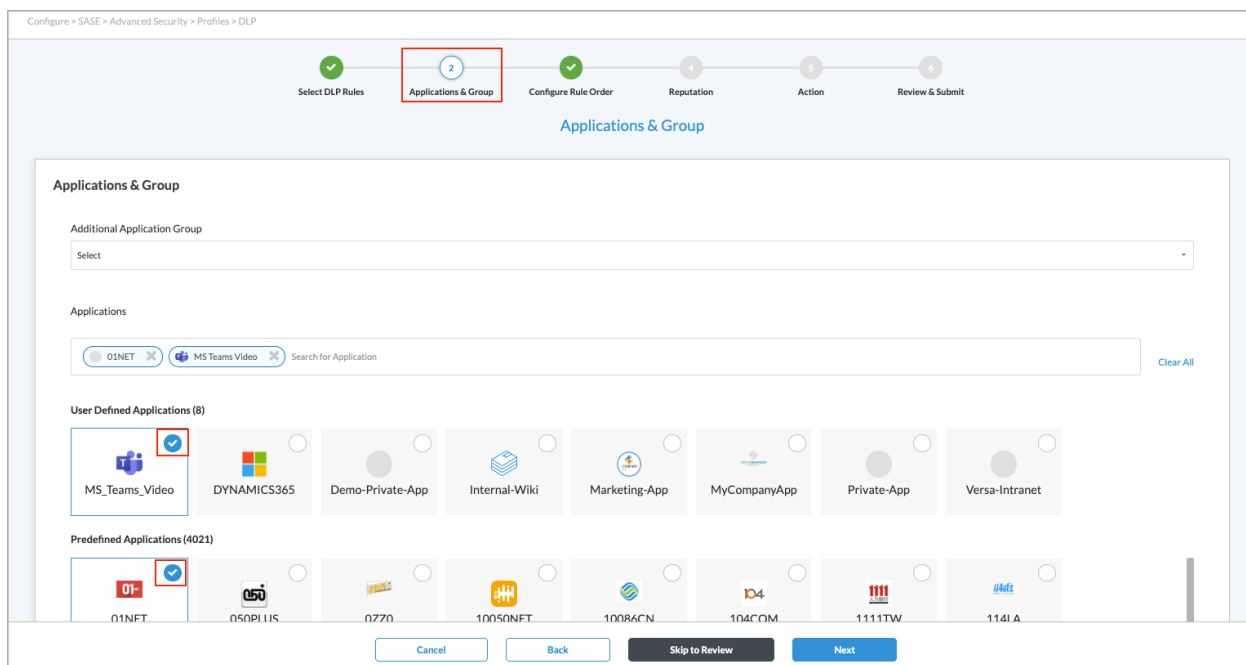
- To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.



- Click + Add to add a new DLP profile. The Select Rules screen displays with Step 1, Select DLP Rules selected by default.



5. 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.
6. Click Next to go to Step 2, Applications and Group.



7. If any application groups have been defined, you can select a group from the list.
8. Select one or more user-defined and/or predefined applications.
9. Click Next to go to Step 3, Configure Rule Order. If you selected two or more DLP rules on 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.

Configure > SASE > Advanced Security > Profiles > DLP

1

2

3

4

5

6

Select DLP RulesApplications & GroupConfigure Rule OrderReputationActionReview & Submit

Configure Rule Order

1

2

3

4

5

API-Rule-EDM
API-Rule-EDM-Tokenization
API_Rule_FileDLP
API_Rule_Fingerprint
API-Rule-OCR

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

Configure > SASE > Advanced Security > Profiles > DLP

1

2

3

4

5

6

Select DLP RulesApplications & GroupConfigure Rule OrderReputationActionReview & Submit

Reputation

☐ Enable Logging

Cloud Lookup
If enabling cloud lookup of a file for its reputation, specify the cloud profile to use for cloud lookup.

☐ Cloud Lookup State ⓘ

Cancel

Back

Skip to Review

Next

Field	Description
Enable Logging	Click to enable logging.
Cloud Lookup State	Click to enable the cloud lookup state. If the cloud lookup state is not configured for this profile, the cloud lookup state configurations are inherited from the tenant VOS device.

11. Click Next to go to Step 5, Action. Enter information for the following fields.

Configure > SASE > Advanced Security > Profiles > DLP

✓

Select DLP Rules

✓

Applications & Group

✓

Configure Rule Order

✓

Reputation

5

Action

6

Review & Submit

Configure Action

Actions

Default Action

Select

☐ Exit On First Rule Match
☐ Logging
☒ Forensic Enabled
☐ Upload original file

Cancel

Back

Skip to Review


Next

Field	Description
Default Action	<p>Click the down arrow and select a default action. The default action is applied if none of the scanned data matches a rule.</p> <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.
Forensics Enabled	Enable forensics on uploaded original files.
Upload Original File	Upload an original file. This option is only selected if select Forensic Enabled.

12. Click Next.

13. In Step 6, 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.

The screenshot shows the 'Review & Submit' step of a DLP configuration process. At the top, a progress bar indicates the following steps: 'Select DLP Rules', 'Applications & Group', 'Configure Rule Order', 'Reputation', 'Action', and 'Review & Submit' (which is highlighted with a red box and a blue circle containing the number 6). Below the progress bar, the text 'Review your DLP configuration below' is displayed. The main form area is titled 'General' and contains three sections: 'Name' with a text input field and a blue circular icon; 'Description' with a text input field containing the placeholder 'Enter description name'; and 'Tags' with a text input field containing the placeholder 'Press Enter to add'. Below these sections is a 'Select DLP Rules' section with an 'Edit' icon. At the bottom of the form, there are three buttons: 'Cancel', 'Back', and 'Save'.

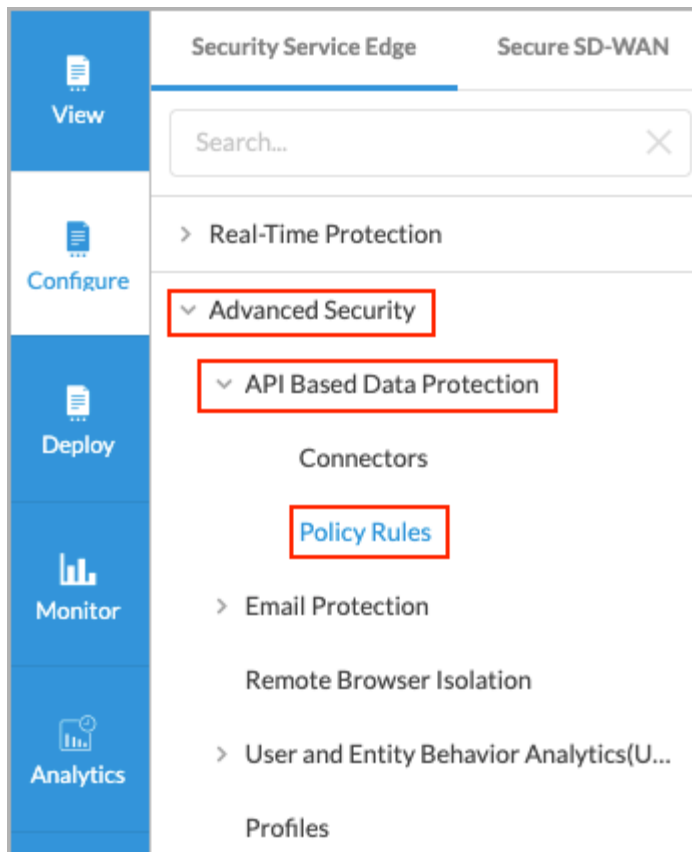
14. Review the configuration.
15. To change any of the information, click the  Edit icon and then make the required changes.
16. After review, click Save to create the new DLP profile.

Associate a DLP Profile with SaaS Applications

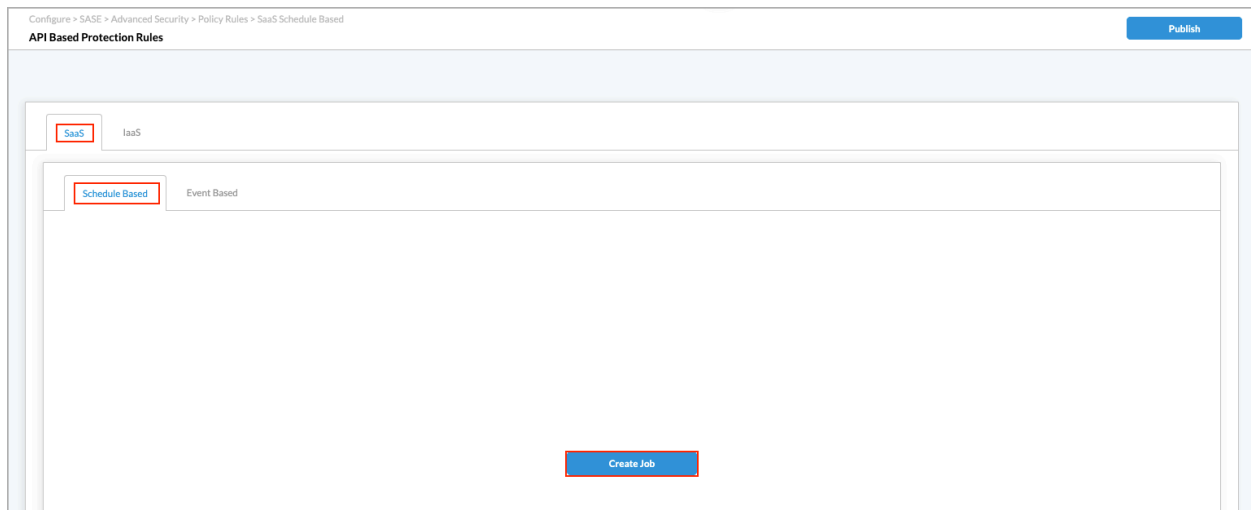
To oversee, track, and report all data transactions in the network and to scan all content that passes through an organization's ports and protocols to ensure data security in the organization, you can associate a DLP profile with SaaS applications. DLP provides a set of tools and processes for detecting 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 SaaS application:

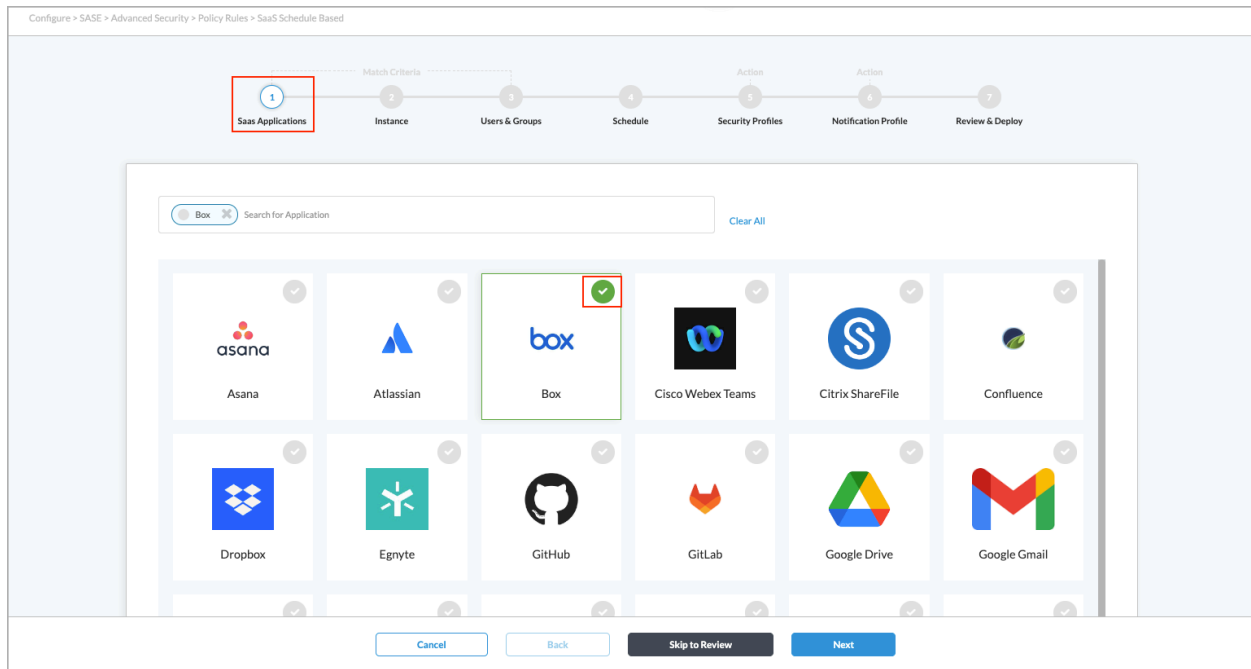
1. Go to Configure > Advanced Security > API Based Data Protection > Policy Rules.



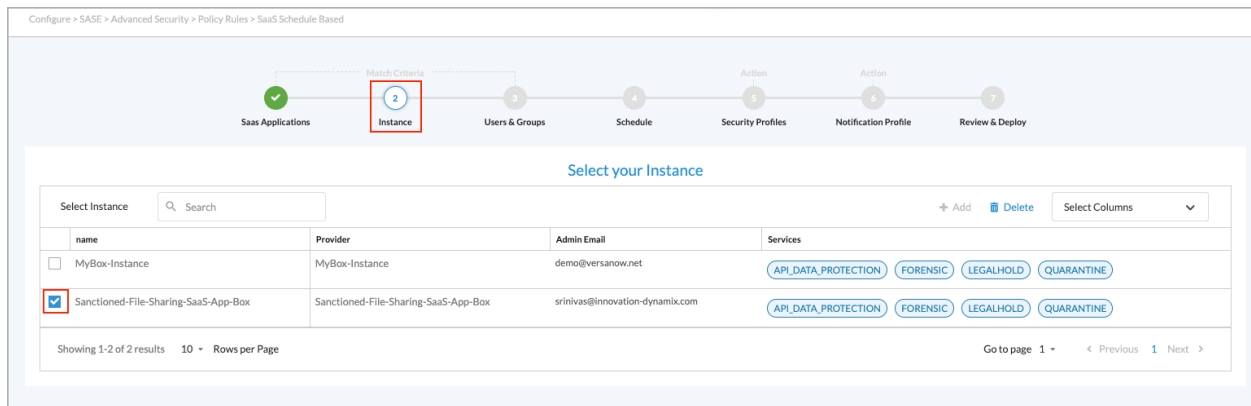
The following screen displays.



2. Select the SaaS tab, then select either Schedule Based or Event Based and click Create Job. This example uses the Schedule Based option. The following screen displays with Step 1, SaaS Applications, selected by default.



3. Click an application, then click Next.



4. In the Step 2, Instance screen, select an instance, then click Next.
5. In the Step 3, Users & Groups screen, select the specific users or groups for the security posture, or click Next to accept the default settings and move to the next step.
6. In Step 4, Schedule, select a schedule and enter the required information.

Configure > SASE > Advanced Security > Policy Rules > SaaS Schedule Based

Select Schedule

Schedule

Which scan type would you like to choose?

Now ☐ Non Recurring Time ☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly ☐

7. Click Next to go to the Step 5, Security Profiles screen.

Configure > SASE > Advanced Security > Policy Rules > SaaS Schedule Based

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

☒ **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)** Offline Cloud Access Security Broker (CASB) Advanced Threat Protection (ATP)

Data Loss Prevention Enabled ☒

API-DLP-Profile-1 [+ Create New](#)

API-DLP-Profile-1
Exit On First Rule Match: Enabled Default Action: Allow

Order	Name	Rule Type	Activities	Context	Protocol	File Type
1	API-Rule-EDM	Exact Data Match (EDM)	redaction	Attachment, Body	HTTP	html
2	API-Rule-EDM-Tokenization	Exact Data Match (EDM)	tokenization	Attachment, Body	HTTP	sh
3	API-Rule-PCI_DSS	Content Analysis	encrypt	Attachment	HTTP	pdf
4	API-Rule-US_HIPAA	Content Analysis	block	Body, Attachment	HTTP	xlsx
5	Rule_ML_US_Passport	Machine Learning	block	Attachment, Body	HTTP	jpg, png

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#)

8. Click Profiles, then select the Data Loss Prevention (DLP) tab.
9. Click the slider bar to enable Data Loss Prevention, then select a profile from the drop-down list. The details of the profile display.
10. Click Next to go to Step 6, Notification Profile, and select a notification profile, if desired..
11. Click Next to go to Step 7, Review & Deploy, and then enter a name for the rule.

Configure > SASE > Advanced Security > Policy Rules > SaaS Schedule Based

Please give your rule a name:

General

Name * ⓘ

Rule Name

Description

Enter description name

Tags

Press Enter to add

☒ Rule is Enabled

Cancel Back Save

12. Click Save.

Additional Information

[Configure SASE Internet Protection Rules](#)