

# DLP Configuration Guide

## About This Document

This guide outlines the essential steps to configure Versa Networks' Data Loss Prevention (DLP), helping you quickly deploy and manage policies to protect sensitive data across your network and cloud applications.

Versa Networks' Network DLP provides comprehensive data protection across multiple communication channels including email, web, chat, SaaS applications, and cloud storage. With native SSL/TLS inspection, it applies DLP policies to encrypted traffic and supports a wide range of file types and metadata, including OCR for PDFs and images.

Versa's unified policy engine ensures consistent management across its security and DLP services from a single interface. Integrated with CASB capabilities, it delivers deep visibility and control over sensitive data in both on-premises and cloud environments.

Its intuitive UI, built-in templates, best practices, and analytics make it easy to deploy and manage, while supporting compliance with standards like HIPAA, PCI and GDPR.

## Document Information

|                |                             |
|----------------|-----------------------------|
| <b>Title</b>   | DLP Configuration Guide     |
| <b>Author</b>  | Versa Professional Services |
| <b>Version</b> | V 1.0                       |

## Disclaimer

Information contained in this document regarding Versa Networks (the Company) is considered proprietary.

|  |    |
|--|----|
| <b>Before you begin .....</b>  | 5  |
| <b>How DLP is Configured in Versa.....</b>   | 5  |
| <b>Data Patterns .....</b>   | 5  |
| <b>Data Protection Profiles.....</b>   | 6  |
| <b>DLP Rules.....</b>  | 7  |
| <b>DLP Profile.....</b>  | 7  |
| <b>Use Case 1: (PII) Aadhaar Card Numbers and Indian Mobile Numbers Policy .....</b>   | 8  |
| <b>Configuration steps .....</b>   | 9  |
| <b>Step 1: Create DLP objects.....</b>   | 9  |
| <b>Step 2: Create the TLS decryption rule for the cloud applications we will test (Gmail and Outlook). ....</b>                      | 21 |
| <b>Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.....</b>                     | 21 |
| <b>Step 4. Perform tests and validate the behaviour.....</b>   | 24 |
| <b>Use Case 2: Protecting Confidential HR Forms with Fingerprint DLP .....</b>   | 27 |
| <b>Configuration steps .....</b>   | 28 |
| <b>Step 1: Create DLP objects.....</b>   | 28 |
| <b>Step 2: Create the TLS decryption rule for the cloud applications we will test (SharePoint and Dropbox). ....</b>                 | 39 |
| <b>Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.....</b>                     | 39 |
| <b>Step 4. Perform tests and validate the behaviour.....</b>   | 42 |
| <b>Use Case 3: VIP Customer Data Protection with EDM-Based DLP .....</b>   | 45 |
| <b>Configuration steps .....</b>   | 47 |
| <b>Step 1: Create DLP objects.....</b>   | 47 |
| <b>Step 2: Create the TLS decryption rule for the cloud applications we will test (Gmail, Outlook, SharePoint and Dropbox). ....</b> | 59 |
| <b>Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.....</b>                     | 59 |
| <b>Step 4. Perform tests and validate the behaviour.....</b>   | 62 |
| <b>Use Case 4: Collaboration Chat Monitoring with DLP for Bad Words .....</b>  | 64 |
| <b>Configuration steps .....</b>   | 65 |
| <b>Step 1: Create DLP objects.....</b>   | 65 |

|  |           |
|--|-----------|
| <b>Step 2: Create the TLS decryption rule for the cloud applications we will test (Slack).....</b>               | <b>77</b> |
| <b>Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.....</b> | <b>77</b> |
| <b>Step 4. Perform tests and validate the behaviour.....</b>   | <b>79</b> |
| <b>Appendix A – DLP Rule Types.....</b>  | <b>81</b> |
| <b>Appendix B – DLP Rule Actions .....</b>   | <b>84</b> |
| <b>Appendix C – TLS Decryption Rule Configuration.....</b>   | <b>85</b> |
| <b>Appendix D – Incident_Report_Form_Filled.docx.....</b>  | <b>87</b> |
| <b>About Versa.....</b>  | <b>89</b> |

## Before you begin

Before you proceed with the steps outlined in this document, please ensure you've met the following prerequisites.

- The provider administrator must complete your tenant configuration. If you haven't received this information, please get in touch with your Managed Service Provider or Account Manager for assistance.
- You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.

## How DLP is Configured in Versa

Versa's DLP configuration follows a modular, layered approach — building complex protections from simple, reusable components. The process consists of defining and combining key building blocks in a nested structure:

### Data Patterns

These are the most granular elements of the DLP system. A Data Pattern typically consists of a regular expression (regex) used to detect specific values such as keywords, patterns (e.g., credit card numbers), or sensitive terms. Administrators can define custom patterns or use Versa's rich library of predefined ones.

#### **Recommendations:**

*- Keyword and Regex both are mandatory for predefined, custom patterns, and a data pattern will only match if at least one of the defined keywords is present together with a value that matches the defined regex, within the defined range, as shown in the example below.*

*- The Range Window (Bytes) parameter defines how many bytes around a detected keyword or regex match are inspected to validate context. A value of **100–200 bytes** is generally recommended as it balances accuracy and performance; smaller windows (50–100 bytes) work well when patterns are close together, while larger windows (up to 500 bytes) may be needed if attributes are separated by more text. As a best practice, start with 100 bytes and adjust only if broader context is required.*

### Data Patterns

Name: test-regex1

Regex: [tT][eE][sS][tT][dD][iI][pP]

Keywords: testing X demo X

Press Enter to add

Range From: Anywhere

Range Window (Bytes): 100

## Data Protection Profiles

At the next level, Data Protection Profiles group multiple Data Patterns using logical expressions such as AND, OR, NOT, or proximity operators like NEAR. This allows for the creation of more nuanced conditions to match complex data leakage scenarios. Both custom and predefined patterns can be referenced in a profile.

| Op-<br>era-<br>tor | What it does   | Pseudo-syn-<br>tax          | Matches  | Doesn't match                                  |
|--------------------|--|-----------------------------|--|--|
| AND                | All referenced patterns must be present                          | PATTERN_A AND PATTERN_B     | Text contains both an EMAIL and a CREDIT_CARD      | Only EMAIL or only CREDIT_CARD                 |
| OR                 | Any one of the patterns is enough                                | PATTERN_A OR PATTERN_B      | Either PAN or AADHAAR appears                      | Neither appears                                |
| NOT                | Excludes matches that contain a pattern                          | PATTERN_A AND NOT PATTERN_B | CREDIT_CARD present but no CORP_EMAIL_DOMAIN       | Both CREDIT_CARD and CORP_EMAIL_DOMAIN present |
| NEAR               | Two patterns must occur within n words of each other (any order) | PATTERN_A NEAR/5 PATTERN_B  | "card number is 4111... email me" (<5 words apart) | "card number ... [30 words] ... email"         |

### Recommendations:

- Recommended to configure a Boolean expression with at least 2 or 3 patterns(userdef/predef) with any of the operators.

- A maximum of 10 data patterns can be added to data protection profiles.
- Versa DLP has Predefined Data Protection Profiles, a built-in database of data expressions & rules which are used to classify the data. These expressions or rules are updated with SPACK upgrades, and it is designed to detect most occurrences of sensitive/regulatory data, but not all.

## DLP Rules

DLP Rules consume one or more Data Protection Profiles and define how and when inspection occurs. Each rule includes:

- **Inspection Method:**
  - *Content Analysis*: Efficient scanning of data-in-motion using prefilters.
  - *File DLP*: Inspects based on file attributes (filename, filesize range and/or hash value).
  - *OCR*: Applies policy to text extracted from image-based files.
  - *EDM*: Matches data against exact entries in a user-supplied dataset.
  - *Document Fingerprinting*: Matches documents based on predefined sensitive forms.
- **File Types**: Specify which file types are subject to inspection.
- **Direction/Context**: Specify whether the rule applies to uploads, downloads, or both. Also clarify whether it applies to the header, body, and/or attachments.
- **Actions**: Determine what happens when a match is found — *block, alert, allow*, etc.

**Recommendation:** - **Do not select Header in DLP policy until it's required.**

## DLP Profile

Finally, DLP Profiles aggregate multiple DLP Rules into a single configuration object. These profiles are then applied within policies to enforce DLP across the desired traffic paths.

This nested and reusable design allows organisations to scale DLP policies efficiently while maintaining clarity and control over policy logic.

# Use Case 1: (PII) Aadhaar Card Numbers and Indian Mobile Numbers Policy

This use case demonstrates how Versa Networks' Data Loss Prevention (DLP) can be configured for ACME-ONE, a global enterprise concerned about the leakage of **personally identifiable information (PII)**.

The HR and Compliance departments at ACME-ONE frequently process documents containing **Indian Aadhaar card numbers** and **Indian mobile phone numbers**, both of which are considered sensitive **PII**. To prevent the accidental or intentional exfiltration of this information, the organisation wants to block out-bound transfers (such as external emails with attachments using **Gmail** or **Outlook**) whenever:

- The file or message contains Aadhaar-related keywords (e.g., Aadhaar, UIDAI) and matches Versa's predefined Aadhaar number detection pattern.
- **OR** the file or message contains Indian mobile number patterns.
- **AND** more than 10 Aadhaar numbers **or** more than 10 Indian mobile numbers are found within the same file or transaction.

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named "**PII Protection Policy**" with the following conditions:

| Policy Name           | Conditions  | Details   |
|-----------------------|---|---|
| PII Protection Policy | Aadhaar-related keyword & Aadhaar number pattern <b>AND</b> >10 Aadhaar numbers in a single file/transaction <b>OR</b> Indian mobile number pattern <b>AND</b> >10 Indian mobile numbers in a single file/transaction | 1) Detect Aadhaar details using keywords combined with Versa's predefined Aadhaar pattern. 2) Detect Indian mobile numbers using Versa's predefined mobile number pattern. 3) Trigger when more than 10 Aadhaar <b>or</b> Indian mobile numbers are detected in the same file/transaction upload. Actions include blocking, logging, or quarantining as per the DLP policy. |

## Pre-requisites

- SSE Gateway with VSPA, VSIA or both enabled.
- Authentication via Active Directory (LDAP used in our scenario)

- TLS Decryption enabled for the cloud applications defined for testing.

## Configuration steps

The DLP configuration consists of the following four steps, which are described in detail below:

1. Create DLP objects
  - Create a **Data Protection Profile** (detection patterns, dictionaries, fingerprinting, etc.).
  - Create a **DLP Rule** (conditions that trigger DLP checks).
  - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (Gmail and Outlook).
3. **Create real-time protection rule** in the Internet Protection Policy that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviours.** Execute test cases, verify detection and enforcement, and record results.

### Step 1: Create DLP objects

#### Creating a Data Pattern for Indian Mobile numbers

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns.** Click + Add, as shown in the image below.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Data Patterns List

Filtering Profiles Malware Protection & IPS Data Loss Prevention (DLP) Cloud Access Security Broker (CASB - Inline) Remote Browser Isolation (RBI) Advanced Threat Protection (ATP)

DLP Rules DLP Profiles Data Protection Profiles Data Patterns

+ Add

| Name    | Regex | Keyword | Range Window | Range From |
|---------|-------|---------|--------------|------------|
| No Data |       |         |              |            |

Next, we define the values with a simple regex for Indian mobile numbers, making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

Data Patterns

Name

Indian\_Mobile\_Numbers

Regex

[6-9]\d{2}\)?[-. ]?\d{3}[-. ]?\d{4}

Keywords

telephone contact Contact Number number

Range From

Anywhere

Range Window (Bytes)

100

## Creating a Data Protection Profile

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Protection.** Click **+ Add**, as shown in the image below.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Data Protection Profiles List

Filtering Profiles Malware Protection & IPS Data Loss Prevention (DLP)

DLP Rules DLP Profiles Data Protection Profiles Data Patterns

Search by keyword or name Filter

Profile Name Boolean Operation

> dlp-discounts dlp\_discounts

> dlp-expression1 dlp\_pattern1

> dlp-INDIA-Aadhaar INDIA\_AADHAAR\_INDIVIDUAL

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 Previous 1 Next

Next, complete the three configuration steps shown in the image below.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Create Data Protection Profile

Select DLP Data Pattern Action Review & Submit

Add User-Defined Data Pattern Add Predefined Data Pattern

Cancel Back Skip to Review Next

**Select DLP Data Pattern:** Select Add Predefined Data Pattern and search for the one you need. In this example, enable **INDIA\_AADHAAR\_INDIVIDUAL**, then click Save. Then click on Add User-Defined Data Pattern and enable **Indian\_Mobile\_Numbers** then click on Save.

**Action:** Click the + icon next to the data identifier **INDIA\_AADHAAR\_INDIVIDUAL** to add it to your Boolean expression. Then, insert the OR operator and click the + icon again to add **Indian\_Mobile\_Numbers**. See the image below.

See the image below.

ACME-ONE

CONFIGURATION

Edit Data Protection Profile: data-protection-profile-Indian\_PII

Select DLP Data Pattern      Action      Review & Submit

Configure Action

Boolean Operation

INDIA\_AADHAAR\_INDIVIDUAL OR Indian\_Mobile\_Numbers

Click to add data identifier to rule      Click to add data operator to rule

1. + INDIA\_AADHAAR\_INDIVIDUAL      2. + OR      3. Indian\_Mobile\_Numbers      4. AND      5. OR      6. NEAR      7. NOT

Cancel      Back      Skip to Review      Next

Once the data identifier has been added, click **Next** to continue.

**Review & Submit:** Assign a name to your Data Protection profile and click **Save**.

ACME-ONE

CONFIGURATION

Edit Data Protection Profile: data-protection-profile-Indian\_PII

General

Name \*  Description

Tags

Data Patterns

User-Defined

Predefined

Action

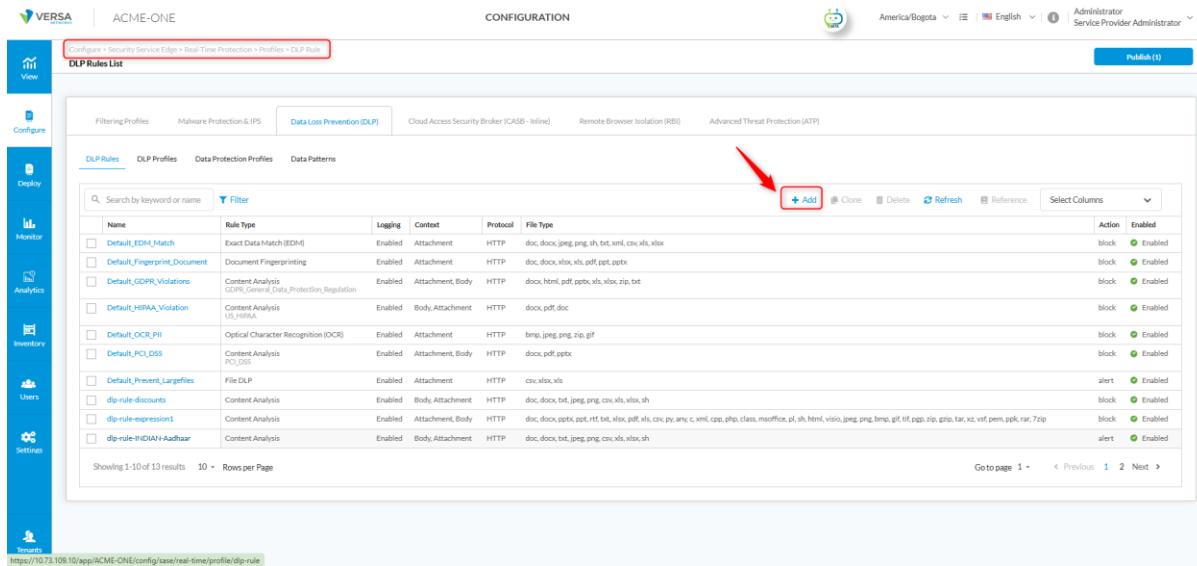
Boolean Operation  
INDIA\_AADHAAR\_INDIVIDUAL OR Indian\_Mobile\_Numbers

Cancel      Back      Save

### Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.



The screenshot shows the VERSA Configuration interface for the 'ACME-ONE' service. The left sidebar has icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main area is titled 'CONFIGURATION' and shows the 'DLP Rules List' under 'Data Loss Prevention (DLP)'. The table header includes columns for Name, Rule Type, Logging, Content, Protocol, File Type, Action, and Enabled. A red arrow points to the '+ Add' button in the top right of the table header. The table lists various DLP rules, such as 'Default\_EDM\_Match', 'Default\_Fingerprint\_Document', and 'Default\_GDPR\_Violations', each with its specific configuration details. The bottom of the table shows pagination: 'Showing 1-10 of 13 results' and '10 - Rows per Page'.

You will now see a menu to select the type of DLP rule. In our case, select **Content Analysis**. For details on the different types of DLP rules, refer to **Appendix A (DLP Rule Types)**.

After selecting **Content Analysis**, six configuration steps will appear:

### Rule Type: Content Analysis

- Severity Level:** Select the severity assigned to the DLP event. Each level has a default value: Low = 1, Medium = 10, High = 20, Critical = 30. The default value for each level specifies the number of occurrences needed to trigger the rule. In the current case, select **Medium**.
- Severity Value:** Define a custom number of occurrences required to trigger the rule (Overwrites the default value associated with the Severity level). The counter starts from 0. For example, if you set the value to 10, the rule will trigger beginning from the 11th DLP event. In this example, no value needs to be set since the Severity Level is set to Medium.
- Predefined/User Defined:** Select **User Defined** and then choose the **Data Protection Profile** we created earlier, named data-protection-profile-AADHAAR.
- Click **Next** to continue.

ACME-ONE

CONFIGURATION

Edit DLP Rule: dip-rule-INDIAN-PII

Rule Type: Content Analysis

File Type

Configure Activity, Protocol & Context

Exclude

Action

Review & Submit

Content Analysis

Severity Level: Medium

Severity Value: 10

Predefined User Defined

All Categories: data-protection-profile-Indian,PII

All Regions: All Regions

Search: ...

Cancel Back Skip to Review Next

**File Type:** Select the file types you want to inspect. For this use case select the checkbox **Select All File Types**.

Click on **Next** to continue.

ACME-ONE

CONFIGURATION

Edit DLP Rule: dip-rule-INDIAN-Aadhaar

Rule Type: Content Analysis

File Type

Configure Activity, Protocol & Context

Exclude

Action

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

Select All File Types

File Types (37)

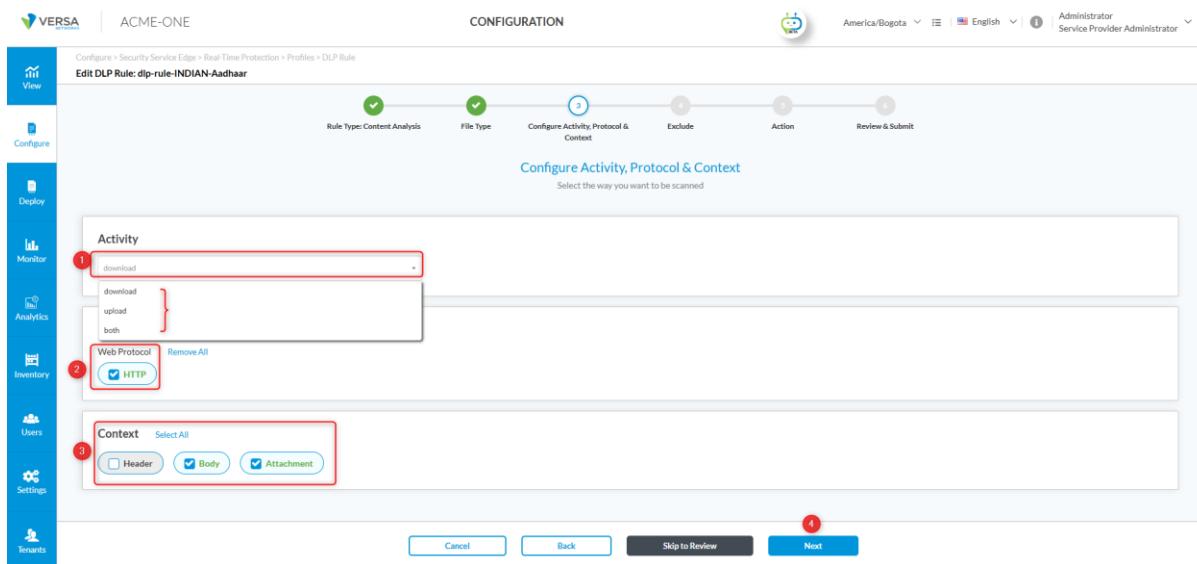
|     |      |      |      |      |       |       |          |      |     |     |      |     |
|-----|------|------|------|------|-------|-------|----------|------|-----|-----|------|-----|
| c   | doc  | docx | xml  | cpp  | php   | class | msoffice | pdf  | pl  | ppt | pptx | rtf |
| sh  | xls  | txt  | xlsx | html | visio | jpeg  | png      | bmp  | gif | tif | pgp  | csv |
| zip | gzip | tar  | xz   | vsf  | pef   | ppk   | rar      | 7zip | py  | any |      |     |

File Types (37)

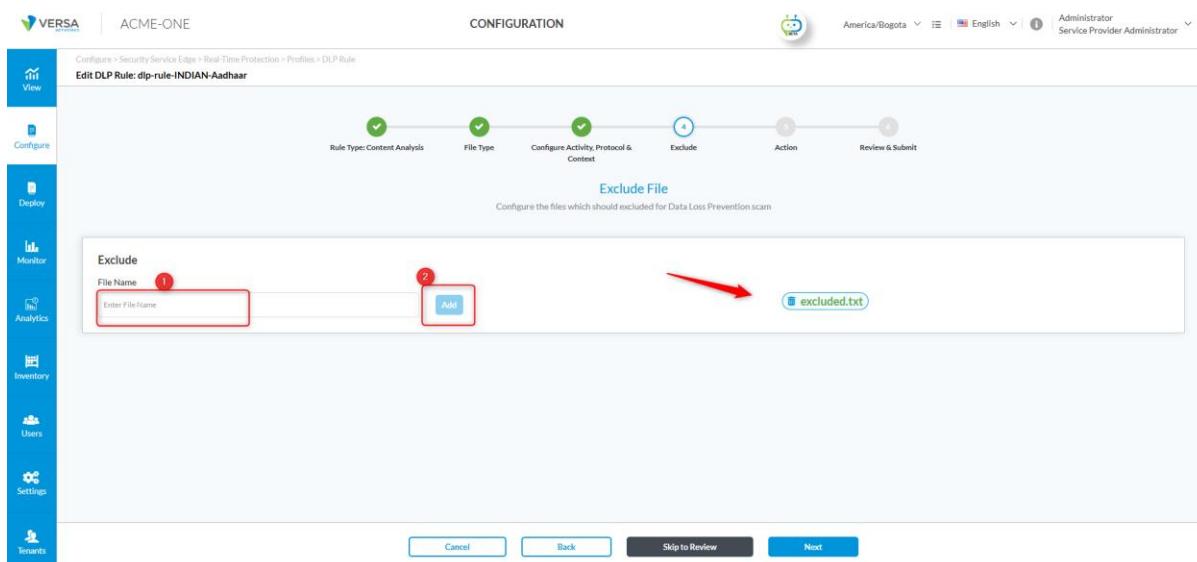
Cancel Back Skip to Review Next

**Configure Activity, Protocol & Context:**

- Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**. This reflects the activity when someone is trying to exfiltrate data.
- Web Protocol:** Select HTTP.
- Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments** and **Body**.



**Exclude:** Specify the file name(s) that should be excluded from DLP inspection.



**Action:** Define the action to be executed when the rule is triggered. Several options are available, such as:

- Allow

- Alert
- Block
- Reject

In our case, we will select **Alert** because we only want a log to be generated in the platform without blocking the user or displaying any pop-up messages. This option is commonly used when tuning DLP rules. For more information on the different actions, refer to **Appendix B: DLP Rule Actions**.

The screenshot shows the 'Edit DLP Rule' screen in the VERSA Configuration interface. The 'Action' dropdown is set to 'Alert' (1). The 'Logging' checkbox is checked (2). The 'Threat Type' dropdown is set to 'File Dlp' (3). The 'Threat Severity' dropdown is set to 'Normal' (4). The interface includes a navigation bar with 'View', 'Configure', 'Deploy', 'Monitor', 'Analytics', 'Inventory', 'Users', 'Settings', and 'Tenants' buttons. The main configuration area shows a progress bar with steps: Rule Type: Content Analysis (green checkmark), File Type (green checkmark), Configure Activity, Protocol & Context (green checkmark), Exclude (green checkmark), Action (blue circle with a question mark), and Review & Submit (grey circle with a question mark). The status bar at the bottom shows 'Cancel', 'Back', 'Skip to Review', and 'Next' buttons.

**Review & Submit:** Verify that your rule matches the example shown in the image below, then click **Save**.

Review your DLP Rule configuration below

**General**

|  |  |
|--|--|
| <p>Name* <a href="#">?</a></p> <input type="text" value="dip-rule-11IDIAN-Aadhaar"/> | <p>Description</p> <input type="text" value="Enter description name"/> |
| <p>Tags</p> <input type="text" value="Press Enter to add"/>                          |  |
| <input checked="" type="checkbox"/> Rule is Enabled                                  |  |

**Match Conditions**

Type of traffic that will be scanned for Data Loss Prevention

|                                       |   |
|---------------------------------------|---|
| <b>File Type</b> <a href="#">Edit</a> | <input type="checkbox"/> doc <input type="checkbox"/> docx <input type="checkbox"/> txt <input type="checkbox"/> jpg <input type="checkbox"/> png <input type="checkbox"/> csv <input type="checkbox"/> xls <input type="checkbox"/> xlsx <input type="checkbox"/> sh |
| <b>Protocol</b> <a href="#">Edit</a>  | <input type="checkbox"/> HTTP   |
| <b>Context</b> <a href="#">Edit</a>   | <input type="checkbox"/> Body <input type="checkbox"/> Attachment   |
| <b>Activity</b> <a href="#">Edit</a>  |   |
| <b>Exclude</b> <a href="#">Edit</a>   | <input type="checkbox"/> excluded.txt   |

**Sensitive Data Type & Data Protection Methods** [Edit](#)

Content Analysis

|                                 |                |                |
|---------------------------------|----------------|----------------|
| User-Defined Data Profile       | Severity Level | Severity Value |
| data-protection-profile-AADHAAR | Critical       | 2              |

**Actions** [Edit](#)

| Action | Set Label | Threat Type | Threat Severity |
|--------|-----------|-------------|-----------------|
| alert  |           | File Dlp    | Normal          |

## Create the DLP Profile:

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.**

**Click + Add**, as shown in the image below.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

DLP Profiles List

Filtering Profiles Malware Protection & IPS Data Loss Prevention (DLP)

DLP Rules DLP Profiles Data Protection Profiles Data Patterns

Add

Complete the six configuration steps shown in the following image.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Create DLP Profile

Select DLP Rules

Select an ordered set of rules in which each rule has one or more match conditions and an action.

Default\_EDM\_Match

Actions: block

Profile

Match Condition: Context Attachment

File Type: docx|pdf|png|jpg|txt|xml|csv|xls|xlsx

Cancel Back Skip to Review Next

**Select DLP Rules:** In the **User Defined Rules** section, search for the rule you created earlier, select it, and click **Next**. It should look like the example shown in the image below.

The screenshot shows the 'Create DLP Profile' step in the VERSA Configuration interface. The 'User-Defined Rules' dropdown is set to 'User-Defined Rules'. A search bar shows 'User-Defined Rules'. A list of rules is displayed, with 'dip-rule-INDIAN-Aadhaar' selected and highlighted with a red box. The 'Next' button at the bottom right is also highlighted with a red box.

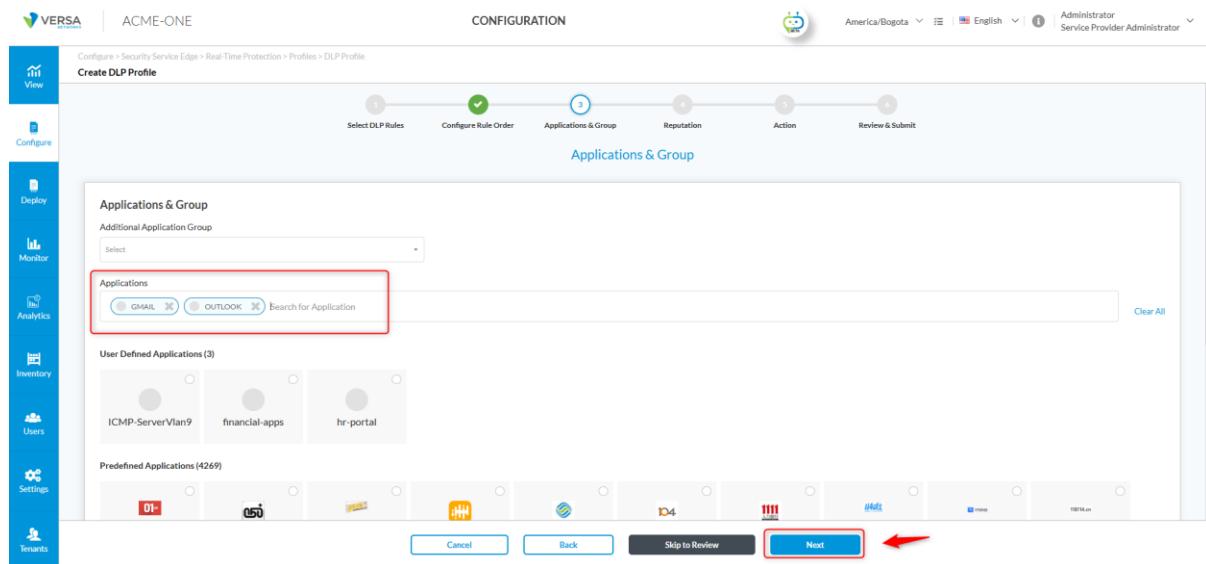
**Configure Rule Order:** You can select any rule and move it up or down to change the DLP processing order. The rule at the top is processed first, and the one at the bottom is processed last. In our case, this does not apply since we have selected only a single rule.

The screenshot shows the 'Configure Rule Order' step in the VERSA Configuration interface. The rule 'dip-rule-INDIAN-Aadhaar' is listed in the order field, which is highlighted with a red box. The 'Next' button at the bottom right is also highlighted with a red box.

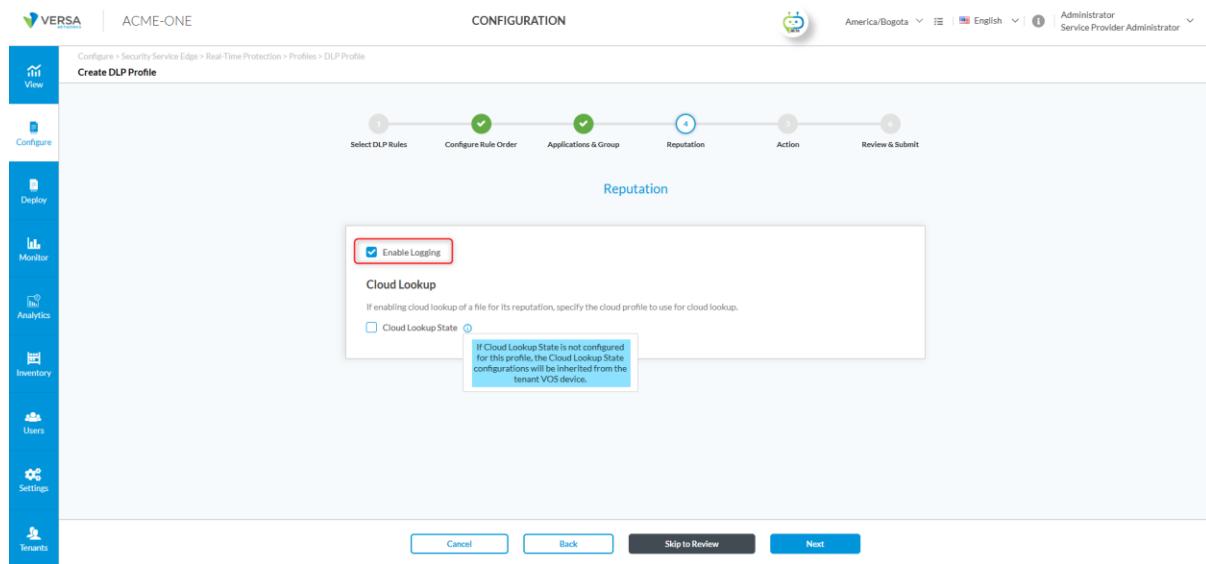
**Applications & Group:** In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select **Gmail** and **Outlook**, then click **Next**, as shown in the image below.

**Notes:** - In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.

- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.



**Reputation:** Select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is not required. Click **Next**.



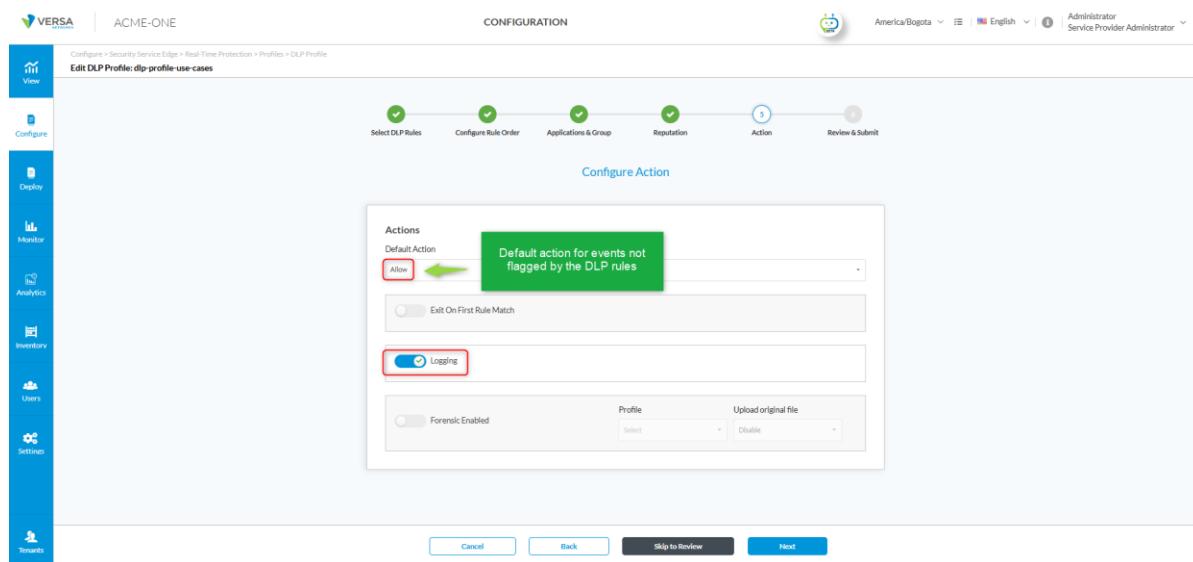
**Action:** Specify the following as shown in the screenshot below:

**Actions:** Set the default action to **Allow**. The default action is applied if none of the scanned data matches a rule.

**Logging:** Click on the toggle button to enable logging.

Exit on First Rule Match: Leave the default action set to **disabled**.

*Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.*



**Review & Submit:** Assign a name, then review the configuration and click the **Save** button.

## Step 2: Create the TLS decryption rule for the cloud applications we will test (Gmail and Outlook).

To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., Gmail and Outlook).

If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

## Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

Navigate to **Configure > Security Service Edge > Real-Time Protection > Internet Protection**.

**Click + Add**, as shown in the image below.

ACME-ONE CONFIGURATION

Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

| Rule Name          | Applications & URLs | Users & Groups | Endpoint Posture                                  | Network Layer 3-4                 | Geo Locations                                   | Security Enforcement                     |
|--------------------|---------------------|----------------|---|-----------------------------------|---|--|
| Implicit_Drop_Quic | All Applications    | All Users      | Endpoint Information Profile (EIP)<br>All devices | Services<br>Implicit-QUIC-UDP-443 | Not Available<br>All Geo locations are selected | All Geo locations are selected<br>Action |

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 < Previous 1 Next >

Then, complete the seven configuration steps shown in the following image.

ACME-ONE CONFIGURATION

Create Internet Protection Rule

Match Criteria

Applications & URLs

By default, we've included all applications to match.

Applications

Applications Group Applications Application Category

Predefined Applications (Selected: 2 of 4269)

|          |         |       |           |         |        |        |       |        |
|----------|---------|-------|-----------|---------|--------|--------|-------|--------|
| 01NET    | 05OPLUS | 0ZZO  | 1005ONET  | 10086CN | 104COM | 1111TW | 114LA | 115COM |
| 18814.cn | 11D     | 1337X | 123456789 | 15      | 103    | 1111TW | 114LA | 115COM |

Cancel Back Skip to Review Next

**Applications & URLs:** Select the applications to which we will apply our DLP module. In our case, we choose Gmail and Outlook.

**Users & Groups:** Select our test group and then click **Next**. In our case, it can be the (VIP) group coming from our LDAP-AD.

**Endpoint Posture:** You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

**Geolocation:** You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

**Network Layer 3-4:** You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

**Security Enforcement:** Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **dip-profile-use-cases**, which is the one we created. Click **Next**.

**Review & Validate:** Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.

Finally, publish the changes applied in Concerto and proceed with the verifications.

## Step 4. Perform tests and validate the behaviour.

To perform tests, we need to understand which key pair values will cause our selected Data Pattern (**INDIA\_AADHAAR\_INDIVIDUAL**) to match our data samples. This is part of our Predefined **DLP Patterns**

**DLP Pattern Name:** INDIA\_AADHAAR\_INDIVIDUAL

**Keywords:** (aadhaar|aadhaar card)

**Pattern Conditions:**

- Detects a **12-digit Aadhaar number** that starts with digits 2–9.
- Supports different formatting styles, such as continuous digits (123412341234) or with separators (e.g., 1234-5678-9123 or 1234 5678 9123).
- Ensures the detected number is not part of a larger alphanumeric string.

Based on the above and also considering our custom data pattern created in Step 1, we generated some samples to create the .txt file and run the tests.

Filename: Test1.txt

-----  
Aadhaar Numbers: 6472 4756 5971 6904 5289 0788 7885-6256-1067 8950-0527-1593 019114027248 7617-8729-4609 855106136654 111048062360 8558 4853 3876 462740952344 763753879522 679336449441 1255 3766 1539 2904-0323-2864 7932-7598-9884 7285 2101 3902 618131683916 4168-9830-2972 0595-3528-6334 7088 6925 2334 Mobile Numbers: 8168718125 +91 6883553941 08511396286 08087536420 0-9344714963 91 9050767250 0-6642953071 9772829100 0-7555887505 9497707487 +919947360842 +919086832700 6361279769 +91 8772342864 07606012845 919099828766 8773658291 9555473795 91-9465257534 91-6948732713

-----  
Now, compose an email from Gmail or Outlook and attach **Test1.txt**, which should be allowed because the **Alert** action does not block but generates an alert log for the DLP event. When checking the logs in **Concerto > Analytics > DLP Logs**, you should see something similar to the images below.

VERSAAACME-ONEANALYTICS

DLP Logs > Nothing selected

ACME-ONE all Last 30 mins

DLP Logs

Show Domain Names

Set filters here... Apply | Clear | Copy Filter

Show 10 entries

| Receive Time                | Appliance | Application | User             | Match Type           | Match String                               | Match Component      | Action | Pattern               | Data Profile                               | Profile               | File Name                     |
|-----------------------------|-----------|-------------|------------------|----------------------|--|----------------------|--------|-----------------------|--|-----------------------|-------------------------------|
| Aug 28/2025, 3:22:46 PM -05 | demo1     | gmail       | vp1@acme-one.com | ContentAnalysisMatch | data-protection-profile-Indian_PII_Profile | ContentAnalysisMatch | alert  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII_Profile | dip-profile-use-cases | Test1.txt                     |
| Aug 28/2025, 3:31:18 PM -05 | demo1     | gmail       | vp1@acme-one.com | ContentAnalysisMatch | Cache Hit                                  | ContentAnalysisMatch | alert  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII_Profile | dip-profile-use-cases | Test1.txt                     |
| Aug 28/2025, 3:37:41 PM -05 | demo1     | owa         | vp1@acme-one.com | ContentAnalysisMatch | Cache Hit                                  | ContentAnalysisMatch | alert  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII_Profile | dip-profile-use-cases | CreateAttachmentFromLocalFile |
| Aug 28/2025, 3:37:41 PM -05 | demo1     | owa         | vp1@acme-one.com | ContentAnalysisMatch | Cache Hit                                  | ContentAnalysisMatch | alert  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII_Profile | dip-profile-use-cases | CreateAttachmentFromLocalFile |
| Aug 28/2025, 3:38:14 PM -05 | demo1     | owa         | vp1@acme-one.com | ContentAnalysisMatch | Cache Hit                                  | ContentAnalysisMatch | alert  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII_Profile | dip-profile-use-cases | CreateAttachmentFromLocalFile |

Showing 1 to 5 of 5 entries

Print | Next

## Switch from Alert to Block Action

With the DLP rule validated as working properly, change the action from **Alert** to **Block** for this DLP rule (Refer to Step 1, Create DLP Rule to make this change). As a best practice, DLP rules are usually deployed in **Alert** mode first to fine-tune detections, and only then switched to **Block** mode once they are validated. When using **Block**, the logs will reflect the blocked action instead of an alert. In addition, the user session will be dropped, and the client will display a pop-up notification with the violation message, as shown below.

VERSABER

Reporting

Dashboard

Logs

DLP Logs

Nothing selected

ACME-ONE all Last 30 mins

DLP Logs

Show Domain Names

Set filters here... Apply | Clear | Copy Filter

Show 10 entries

| Receive Time                  | Appliance | Application | User              | Match Type           | Match String | Match Component      | Action | Pattern               | Data Profile                       | Profile              | File Name | File Type |
|-------------------------------|-----------|-------------|-------------------|----------------------|--------------|----------------------|--------|-----------------------|------------------------------------|----------------------|-----------|-----------|
| Aug 28th 2025, 3:06:24 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:24 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:12 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:11 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:08 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:08 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:06 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:06 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:06 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:04 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |
| Aug 28th 2025, 3:06:04 PM -05 | demo1     | gmail       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit    | ContentAnalysisMatch | block  | Indian_Mobile_Numbers | data-protection-profile-Indian_PII | dp-profile-use-cases | Test1.txt | txt       |

Showing 1 to 10 of 48 entries

Previous 1 2 3 4 5 Next

The screenshot shows a Gmail inbox interface. The left sidebar includes 'Compose', 'Inbox' (selected), 'Starred', 'Snoozed', 'Sent', 'Drafts' (25), and 'More'. The 'Labels' section has a '+' sign. The main area shows the 'Primary' tab with 1 new message. The message list includes 'ChatGPT', 'Google', 'Google', 'Google', 'me, Mail 2', 'me', 'me', 'Google', 'Dropbox', 'Dropbox', and 'Google'. The message content shows 'test' in the recipient field and 'test' in the body. A 'Test1.txt (1K)' file is attached. A 'VERSAscan' watermark is visible in the top right. A yellow box highlights the 'Policy violation detected by DLP' message. The message content is as follows:

**VERSAscan**

**Policy violation detected by DLP**

Please contact your IT administrator for further information.

|             |                 |
|-------------|-----------------|
| Application | gmail           |
| Action      | upload          |
| Activity    | Test1.txt       |
| URL         | mail.google.com |

**OK**

This window will auto-close in 18 seconds

## Use Case 2: Protecting Confidential HR Forms with Fingerprint DLP

This use case demonstrates how ACME-ONE leverages **Fingerprint-based DLP** in Versa Networks to protect sensitive HR documents that must not leave the corporate environment.

The HR department at ACME-ONE manages a "**Confidential Employee Disciplinary Form**", which contains predefined fields such as:

- Employee Name
- Employee ID
- Date of Incident
- Description of Violation
- Manager Comments
- HR Review Outcome

Although the specific details in each form may vary, the overall structure, layout, and field labels remain consistent.

To prevent the **exfiltration of these documents through web-based uploads to cloud storage services such as SharePoint and Dropbox**, Versa's Fingerprint DLP engine is configured to detect **document similarity** against a registered template of the "Confidential Employee Disciplinary Form."

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named "**Confidential HR Form Protection**" with the following conditions:

| Policy Name                      | Conditions   | Details  |
|----------------------------------|--|--|
| <b>HR Form Protection Policy</b> | Document fingerprint match with $\geq 50\%$ similarity | <p>1) Register the "Confidential Employee Disciplinary Form" as a fingerprinted document in Versa DLP.</p> <p>2) Trigger the policy if outbound traffic contains a <b>web upload attempt</b> of a file with <math>\geq 50\%</math> similarity to the fingerprinted template via SharePoint or Dropbox.</p> <p>3) Actions include Alerting, blocking and logging.</p> |

### Pre-requisites

- SSE Gateway with VSIA enabled.
- Authentication via Active Directory (LDAP used in our scenario)
- TLS Decryption enabled for the cloud applications defined for testing.

## Configuration steps

The DLP configuration consists of the following steps, which are described in detail below:

1. Create DLP objects
  - Create a **DLP Sub-Folder** and **upload the confidential file**.
  - Create a **DLP Rule** (conditions that trigger DLP checks).
  - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (**SharePoint** and **Dropbox**).
3. **Create real-time protection rule** that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviour.** Execute test cases, verify detection and enforcement, and record results.

### Step 1: Create DLP objects

For our rule type (**Document Fingerprinting**), we need to create a folder where the confidential document will be stored. This document will be used to generate corresponding fingerprint hash. We must also define and upload the confidential file. Once this is completed, we can define the DLP rule by selecting the folder that already contains our file and then proceed with the standard configuration steps that we will demonstrate.

#### Create Folder:

Navigate to **Configure > Security Service Edge > Settings > Files and Folders**.

Click **+ Add**, as shown in the image below.

Next, a window called **Add Folder** will appear with two sections to configure:

- **Where should folder be placed?**: From the dropdown list, select **DLP/Fingerprints**.
- **Folder Name**: Enter a descriptive name, for example: **ACME-ONE-Fingerprinted-Files-HR**.

Once completed, the configuration window will look as follows:

## Upload File:

Navigate to **Configure > Security Service Edge > Settings > Files and Folders**.

Click **+ Upload File**, as shown in the image below.

The screenshot shows the VERSA Configuration interface. The left sidebar has a blue background with white icons and labels. Red boxes with numbers 1 through 9 highlight specific areas: 1 points to the 'Security Service Edge' section, 2 points to the 'Configure' section, 3 points to the 'Settings' section, 4 points to the 'Files And Folders' section, 5 points to the 'Upload File' button, 6 points to the 'Add Folder' button, 7 points to the 'Refresh' button, 8 points to the 'Select Columns' button, and 9 points to sub-folders like 'BGP Peer Policies' and 'LAN Interface'. The main content area is titled 'File & Folder Management' and shows a table of files with columns for File Count, Checksum, File Size, Date Modified, Modified By, and Actions. The table contains several entries, including a row for 'Files-HR'.

| File Count | Checksum | File Size | Date Modified          | Modified By   | Actions |
|------------|----------|-----------|------------------------|---------------|---------|
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |
| -          | -        | -         | 9/15/2025, 12:14:36 PM | Administrator | [Edit]  |
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |
| -          | -        | -         | 7/9/2025, 1:26:56 PM   | Administrator | [Edit]  |

Next, a window called **Upload File** will appear with three sections to configure:

- **Hash the file:** We can leave the default option selected (checked).
- **Where should folder be placed?:** From the dropdown list, select **DLP/Fingerprints/ACME-ONE-Fingerprinted-Files-HR** which is the sub-folder we defined before.
- **Upload File:** Click and select the file from the corresponding location. In our case we are uploading the file

Once completed, the configuration window will look as follows:

Finally, click on **Upload** to complete the process.

## Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.

You will now see a menu to select the type of DLP rule. In our case, select **Document Fingerprinting**. For details on the different types of DLP rules, refer to **Appendix A (DLP Rule Types)**.

After selecting **Document Fingerprinting**, six configuration steps will appear:

## Document Fingerprinting:

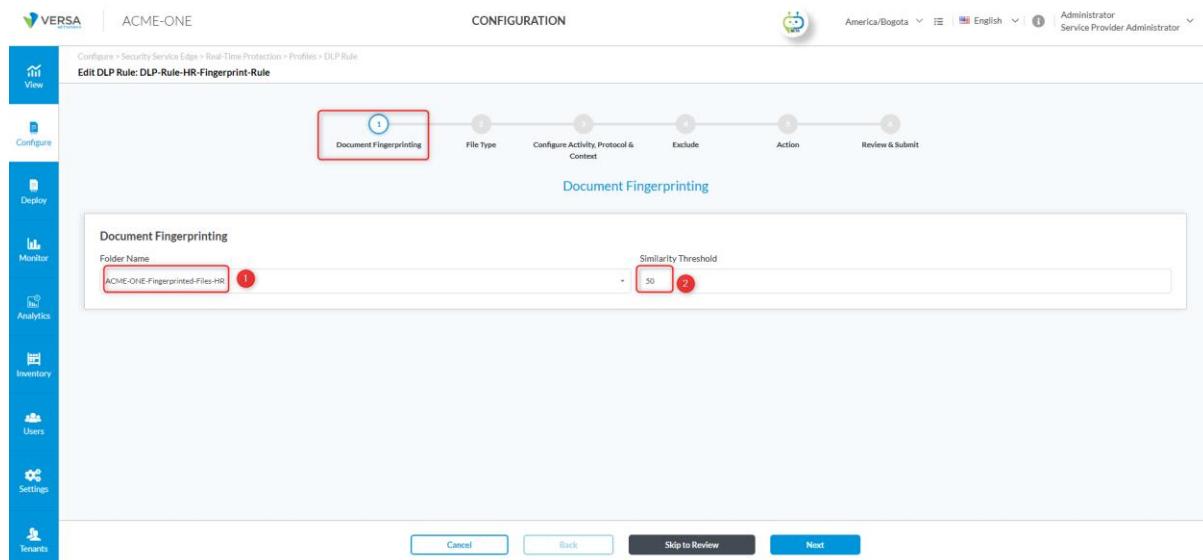
**Folder Name:** Click on the dropdown list and select the folder ACME-ONE-Fingerprinted-Files-HR.

**Similarity Threshold:** Defines the minimum level of content overlap required between an uploaded user document and the reference (sample) document. For example, if the threshold is set to 60% and the computed similarity is 70%, the document will be considered a match. Conversely, if the threshold is set to 80%, the same document would not be considered a match. For this case, please select 50%.

Once completed, the configuration window will look as follows:

Notes:

- **Avoid False Matches on Blank Forms:** If the computed similarity is **95% or higher**, Versa assumes the uploaded document is effectively blank or unmodified, and the document will not be considered a match. Ensure user-filled forms include sufficient new content to lower the similarity below 95%, enabling meaningful evaluation.
- **Recommended Thresholds for Fully Completed Forms:** For user-submitted, fully completed forms, set the similarity threshold between **30% and 60%** to detect and match against the original template reliably.
- **Tailor the Threshold:** Adjust the similarity threshold based on form type and expected variation. Use **lower thresholds** for structured, fully completed forms and **higher thresholds** for loosely modified templates.



Click **Next** to continue.

**File Type:** Select the file types you want to inspect. For this use case select: **.docx** and **.pdf**.

**NOTE:** - **Supported File Types:** **PDF, DOC, and DOCX.**

Click on **Next** to continue.

### Configure Activity, Protocol & Context:

**Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**.

**Web Protocol:** Select **HTTP**.

**Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments**.

**Exclude:** We can skip this step since the use case does not require excluding any files.

Click on **Next** to continue.

The screenshot shows the VERSA Configuration interface for 'Edit DLP Rule: DLP-Rule-HR-Fingerprint-Rule'. The left sidebar includes 'View', 'Configure', 'Deploy', 'Monitor', 'Analytics', 'Inventory', 'Users', 'Settings', and 'Tenants'. The main area is titled 'CONFIGURATION' and shows a flow: 'Document Fingerprinting' (green checkmark), 'File Type' (grey), 'Configure Activity, Protocol & Context' (green checkmark), 'Exclude' (highlighted with a red box), 'Action' (green checkmark), and 'Review & Submit' (grey). Below the flow is a section titled 'Exclude File' with a sub-section 'Exclude'. It contains a 'File Name' input field with 'Enter File Name' placeholder text and an 'Add' button. At the bottom are buttons for 'Cancel', 'Back', 'Skip to Review' (disabled), and 'Next' (highlighted with a red arrow).

### Action:

Define the action to be executed when the rule is triggered. Several options are available including:

- Allow
- Alert
- Block
- Reject

In our case, we will select **Block**. For more information on the different actions, refer to **Appendix B: DLP Rule Actions**.

ACME-ONE

CONFIGURATION

Edit DLP Rule: DLP-Rule-HR-Fingerprint-Rule

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

Action: Block (1)

Logging (2)

Threat Type: Document Fingerprint (3)

Threat Severity: Critical (4)

Next

**Review & Submit:** Verify that your rule matches the example shown in the image below, then click **Save**.

Review your DLP Rule configuration below

**General**

Name: DLP-Rule-HR-Fingerprint-Rule

Description: Testing DLP Fingerprinting

Tags: Press Enter to add

Rule Is Enabled:

**Match Conditions**

Type of traffic that will be scanned for Data Loss Prevention

**File Type**: docx, pdf, doc

**Protocol**: HTTP

**Context**: Attachment

**Activity**: Upload

**Exclude**:

**Sensitive Data Type & Data Protection Methods**

Folder Path: ACME-ONE-Fingerprinted-Files-HR

Similarity Threshold: 50

**Actions**

| Action | Set Label | Threat Type          | Threat Severity |
|--------|-----------|----------------------|-----------------|
| block  |           | Document Fingerprint | Critical        |

## Create the DLP Profile:

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.**

**Click + Add**, as shown in the image below.

Then, complete the six configuration steps shown in the following image.

**Select DLP Rules:** In the **User Defined Rules** section, search for the rule you created earlier. Select it and click **Next**. It should look like the example shown in the image below.

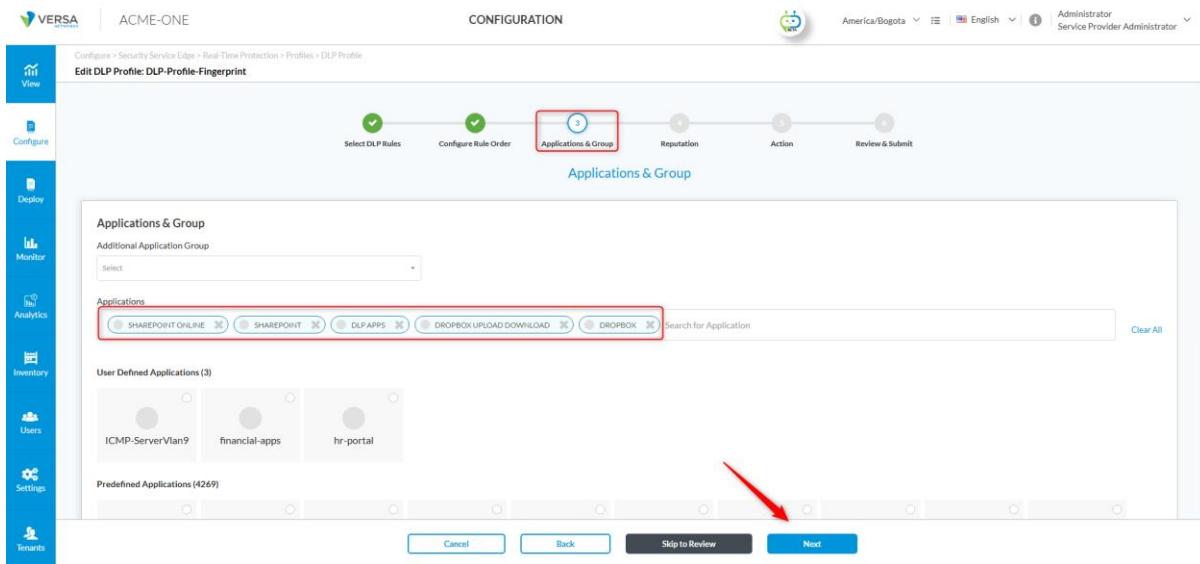
The screenshot shows the VERSA Configuration interface for editing a DLP profile. The top navigation bar includes 'ACME-ONE', 'CONFIGURATION', and 'Administrator'. The left sidebar has icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, and Tenants. The main content area is titled 'Edit DLP Profile: DLP-Profile-Fingerprint'. A progress bar at the top shows 'Select DLP Rules' (1), 'Configure Rule Order' (2), 'Applications & Group' (3), 'Reputation' (4), 'Action' (5), and 'Review & Submit' (6). The 'Select DLP Rules' step is highlighted with a red box. Below it, a dropdown menu shows 'User-Defined Rules' selected (2). A list of rules is displayed, with 'DLP-Rule-HR-Fingerprint-Rule' selected (3). To the right, a detailed view of the selected rule 'Default\_EDM\_Match' is shown, including 'Actions' (block), 'Profile', and 'Match Condition' (Context: Attachment, File Type: docx/doc/docx/doc/docx). At the bottom, buttons for 'Cancel', 'Back', 'Skip to Review', and a large blue 'Next' button are visible. A red arrow points from the text above to the 'Next' button.

**Configure Rule Order:** We can skip this step since only a single rule has been selected, so click **Next** to continue.

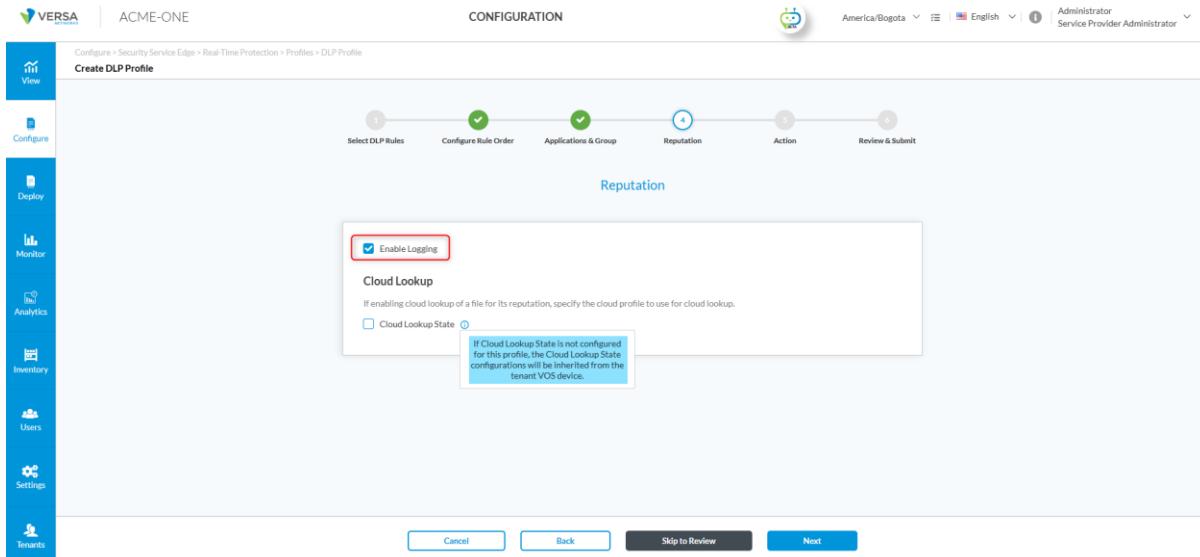
**Applications & Group:** In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select the related apps for **SharePoint** and **Dropbox**, then click **Next**, as shown in the image below.

Notes:

- In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.
- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.



**Reputation:** Select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is optional; for more information, you can visit the following link: [How to Configure Cloud Lookup](#).



## Action:

**Actions:** Set the default action to **Allow**. The default action is applied if none of the scanned data matches a rule.

**Logging:** Click on the toggle button to enable logging.

**Exit on First Rule Match:** Leave the default action set to **disabled**.

*Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.*

**Review & Submit:** Review the configuration, then click the **Save** button.

## Step 2: Create the TLS decryption rule for the cloud applications we will test (SharePoint and Dropbox).

To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., SharePoint and Dropbox).

If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

## Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Internet Protection.**

**Click + Add**, as shown in the image below.

ACME-ONE      CONFIGURATION

Administrator Service Provider Administrator

Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

| Rule Name          | Applications & URLs | Users & Groups | Endpoint Posture                                  | Network Layer 3-4                 | Geo Locations                                   | Security Enforcement                     |
|--------------------|---------------------|----------------|---|-----------------------------------|---|--|
| Implicit_Drop_Quic | All Applications    | All Users      | Endpoint Information Profile (EIP)<br>All devices | Services<br>Implicit-QUIC-UDP-443 | Not Available<br>All Geo locations are selected | All Geo locations are selected<br>Action |

Showing 1-6 of 6 results    10 + Rows per Page    Go to page 1 + < Previous 1 Next >

Then, complete the seven configuration steps shown in the following image.

ACME-ONE      CONFIGURATION

Configure > Security Service Edge > Real-Time Protection > Internet Protection

Edit Internet Protection Rule: Real-time-policy-DLP-Fingerprint

By default, we've included all applications to match.

Applications

Application Group   Applications   Application Category

Predefined Applications (Selected: 4 of 4269)

|          |         |       |          |         |        |        |       |        |
|----------|---------|-------|----------|---------|--------|--------|-------|--------|
| 01NET    | 05OPLUS | 0ZZO  | 1005ONET | 10086CN | 104COM | 1111TW | 114LA | 115COM |
| 18814.cn | 11D     | 1337X | 18888    | 15      | 183    | 18888  | 18888 | 18888  |

Cancel   Back   Skip to Review   Next

**Applications & URLs:** Select the applications to which we will apply our DLP module. In our case, we choose SharePoint and Dropbox.

**Users & Groups:** Select our test group and then click Next. In our case, it can be the (VIP) or (HR) group coming from our LDAP-AD.

**Endpoint Posture:** You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

**Geolocation:** You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

**Network Layer 3-4:** You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

**Security Enforcement:** Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **DLP-Profile-Fingerprint**, which is the one we created. Click **Next**.

**Review & Validate:** Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.

Review your Internet Protection Policy configurations below.  
Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

### General

Name\*  Description

Tags

Rule is Enabled

### Applications & URLs

[Edit](#)

Applications [Custom Selection](#)

- Applications | 4
  - Dropbox
  - SHAREPOINT

### Users & Groups

[Edit](#)

Users & Groups AD-DC1  
User Risk Bands All Risk Bands

Users Device Groups All Device Groups

User Group | 2

- Name
- vip
- hr

### Endpoint Posture

[Edit](#)

### GEO Locations

[Edit](#)

Source  All source Geo locations are selected  
Destination  All destination Geo locations are selected

### Network Layer 3-4

[Edit](#)

Services

- All Services
- destination

Zones

- Internet

### Security Enforcement

[Edit](#)

Enforcements DLP-Profile-Fingerprint

Finally, publish the changes applied in Concerto and proceed with the verifications.

## Step 4. Perform tests and validate the behaviour.

To perform the tests, we only need to upload from SharePoint and Dropbox the test file that corresponds to the confidential form once completed. Below, you can see the original (blank) and the one used in the test (filled).

*Filename: Incident\_Report\_Form\_Blank.docx*

---

### **Confidential Employee Incident Report Form**

This form is intended for the reporting of workplace incidents and policy violations. All submissions are confidential and will be reviewed by the HR Compliance Department. Please complete all required sections. Additional evidence or extended narratives should be attached as separate documents. Do not exceed the provided space in each section.

#### **Section 1 – Employee Information**

Employee Name: \_\_\_\_\_

Department: \_\_\_\_\_

Position: \_\_\_\_\_

Date of Incident: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

#### **Section 2 – Type of Violation**

Please check one or more categories that best describe the violation (mandatory selection):

- Code of Conduct
- Confidentiality Breach
- Workplace Harassment
- Safety Violation
- Other (please specify) \_\_\_\_\_

#### **Section 3 – Description of Violation**

Provide a concise summary of the violation in 3-4 sentences maximum. If additional details are needed, attach a supporting document.

Description (do not exceed space provided):

---

---

---

#### **Section 4 – Witnesses**

List up to 2 witnesses with name and department. Additional names must be attached separately.

1. \_\_\_\_\_

2. \_\_\_\_\_

#### **Section 5 – Co-Workers Involved**

List any co-workers directly involved in the incident. Specify their role or relation to the case.

1. \_\_\_\_\_

2. \_\_\_\_\_

#### **Section 6 – Acknowledgement**

By signing this form, the reporting employee confirms that the information provided is accurate to the best of their knowledge. The HR Compliance Department will review the case and take the appropriate action as outlined in company policy.

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Filename: Incident\_Report\_Form\_Filled.docx

---

### Confidential Employee Incident Report Form

This form is intended for the reporting of workplace incidents and policy violations. All submissions are confidential and will be reviewed by the HR Compliance Department. Please complete all required sections. Additional evidence or extended narratives should be attached as separate documents. Do not exceed the provided space in each section.

#### Section 1 – Employee Information

Employee Name: John Doe

Department: IT Security

Position: Senior Security Analyst

Date of Incident: 09 / 12 / 2025

#### Section 2 – Type of Violation

Please check one or more categories that best describe the violation (mandatory selection):

Confidentiality Breach  
 Code of Conduct  
 Workplace Harassment  
 Safety Violation  
 Other (please specify) \_\_\_\_\_

#### Section 3 – Description of Violation

Provide a concise summary of the violation in 3-4 sentences maximum. If additional details are needed, attach a supporting document.

Description:

On September 12th, 2025, an employee was observed uploading a confidential HR policy document to a personal Dropbox account. The file contained sensitive disciplinary procedures. The incident was detected by the DLP monitoring system and reported for investigation.

#### Section 4 – Witnesses

List up to 2 witnesses with name and department. Additional names must be attached separately.

1. Jane Smith – HR Department
2. Michael Brown – IT Department

#### Section 5 – Co-Workers Involved

List any co-workers directly involved in the incident. Specify their role or relation to the case.

1. Alice Johnson – Co-worker who shared the document link internally.
2. N/A

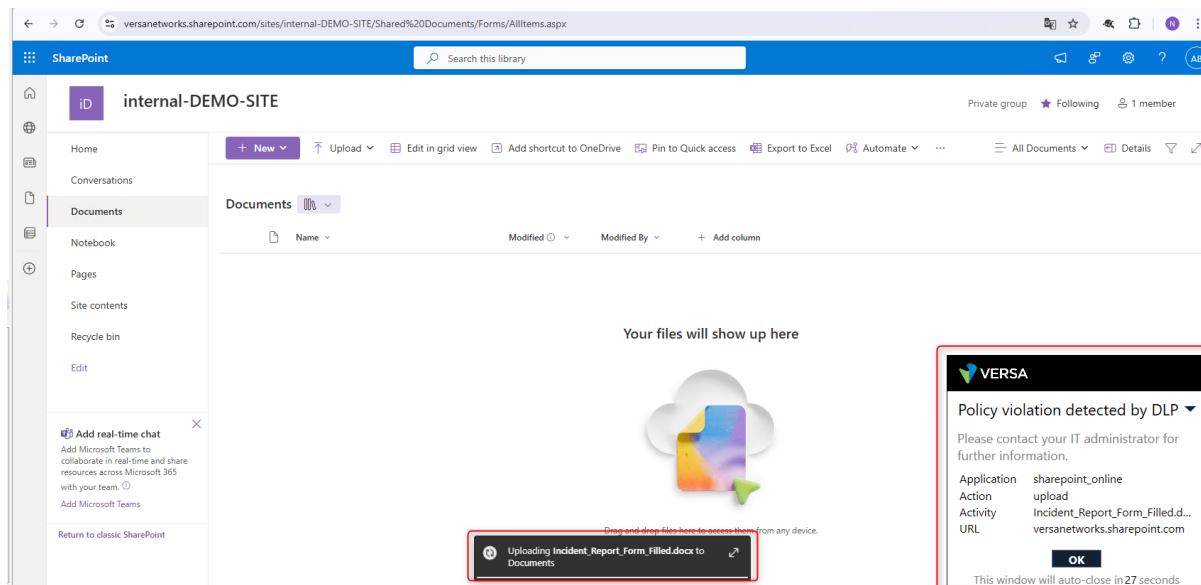
#### Section 6 – Acknowledgement

By signing this form, the reporting employee confirms that the information provided is accurate to the best of their knowledge. The HR Compliance Department will review the case and take the appropriate action as outlined in company policy.

Employee Signature: John Doe Date: 09 / 12 / 2025

Now, Upload from SharePoint or Dropbox the file called *Incident\_Report\_Form\_Filled.docx*, which should be blocked because the **Block** action was selected. See the images below.

SharePoint test



internal-DEMO-SITE

Search this library

Upload Edit in grid view Add shortcut to OneDrive Pin to Quick access Export to Excel Automate ... All Documents Details

Home Conversations Documents Notebook Pages Site contents Recycle bin Edit

Add real-time chat Add Microsoft Teams to collaborate in real-time and share resources across Microsoft 365 with your team. Add Microsoft Teams

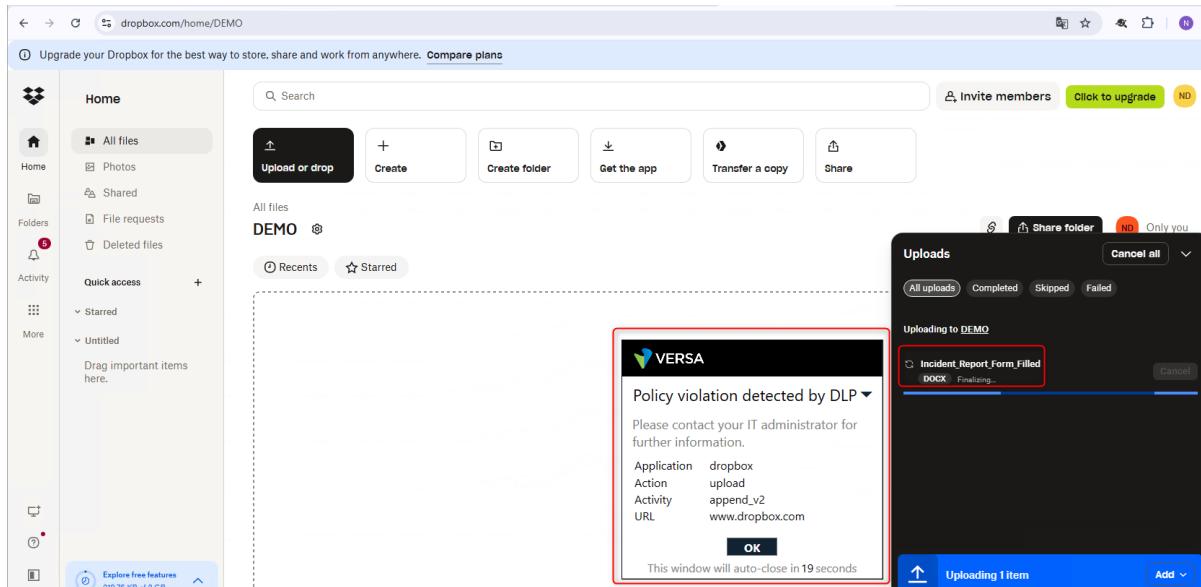
Return to classic SharePoint

Your files will show up here

Uploading Incident\_Report\_Form\_Filled.docx to Documents

VERSА Policy violation detected by DLP ▾ Please contact your IT administrator for further information. Application sharepoint\_online Action upload Activity Incident\_Report\_Form\_Filled.d... URL versanetworks.sharepoint.com OK This window will auto-close in 27 seconds

## Dropbox test



Home

All files Photos Shared File requests Deleted files

Upload or drop Create Create folder Get the app Transfer a copy Share

DEMO

Recents Starred

VERSА Policy violation detected by DLP ▾ Please contact your IT administrator for further information. Application dropbox Action upload Activity append\_v2 URL www.dropbox.com OK This window will auto-close in 19 seconds

Uploads Cancel all Only you

Uploading to DEMO

Incident\_Report\_Form\_Filled DOCX Finalizing...

Uploading 1 item Add

You can find the sample in Appendix D – *Incident\_Report\_Form\_Filled.docx*.

When checking the logs in **Concerto > Analytics > DLP Logs**, you should see something similar to the images below.

| Application       | User              | Match Type          | Match String | Match Component     | Action | Pattern     | Data Profile                  | Profile                 | File Name                        |
|-------------------|-------------------|---------------------|--------------|---------------------|--------|-------------|-------------------------------|-------------------------|----------------------------------|
| dropbox           | vip1@acme-one.com | FingerPrintingMatch | Cache Hit    | FingerPrintingMatch | block  | Fingerprint | Fingerprint threshold matched | DLP-Profile-Fingerprint | append_v2                        |
| sharepoint_online | vip1@acme-one.com | FingerPrintingMatch | Cache Hit    | FingerPrintingMatch | block  | Fingerprint | Fingerprint threshold matched | DLP-Profile-Fingerprint | Incident_Report_Form_Filled.docx |

## Use Case 3: VIP Customer Data Protection with EDM-Based DLP

This use case demonstrates how ACME-ONE leverages **EDM-based DLP** in Versa Networks to prevent sensitive customer records from being leaked by employees in Finance or VIP Management. These employees regularly access the **VIP Customers Database** and frequently use cloud collaboration platforms and email services.

The Finance and VIP Management departments at ACME-ONE manage a **VIP Customers Database** containing highly sensitive information, such as:

- Customer Full Name
- Customer ID / Account Number
- Email Address
- Phone Number
- Contract Reference Number

Since these records represent ACME-ONE's top customers, preventing their unauthorized disclosure is a business-critical requirement. Unlike fingerprinting entire forms, **EDM provides field-level matching against the structured database**, ensuring that even partial extracts (e.g., a CSV export) are detected.

To reduce the risk of intentional or accidental exfiltration via platforms commonly used by Finance and VIP staff, Versa's EDM DLP engine is configured to detect matches against the registered VIP customer database when data is transmitted through:

**Cloud storage apps:** SharePoint web, Dropbox web.

**Email services:** Outlook (Office 365), Gmail

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named "**VIP Customer Data Protection**" with the following conditions:

| Policy Name                         | Conditions   | Details  |
|-------------------------------------|--|--|
| <b>VIP Customer Data Protection</b> | EDM match with<br>≥ 1 field hit from<br>VIP database | 1) Register the VIP customer database as an EDM source in Versa DLP.<br>2) Trigger the policy if outbound traffic contains data matching any field from the EDM source via SharePoint, Dropbox, Outlook, or Gmail. 3) Actions include <b>Blocking, and Logging</b> . |

## Pre-requisites

- SSE Gateway with VSIA enabled.
- Authentication via Active Directory (LDAP used in our scenario)
- TLS Decryption enabled for the cloud applications defined for testing.

## Configuration steps

The DLP configuration consists of the following steps, which are described in detail below:

1. Create DLP objects
  - o Create a **DLP Pattern for USA mobile numbers, Contract id and Customer id**.
  - o Create a **DLP Rule** (conditions that trigger DLP checks).
  - o Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (**SharePoint, Dropbox, Outlook** and **Gmail**).
3. **Create real-time protection rule** that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviour.** Execute test cases, verify detection and enforcement, and record results.

### Step 1: Create DLP objects

For our use case (**EDM – Exact Data Match**), we need to upload our database through Concerto and then select the columns that contain sensitive information, mapping each column to a data pattern (either predefined or customized). It is important to have already defined any custom data patterns to be used, before reaching this step. In our case, we will define a custom data pattern for USA mobile numbers, contract IDs, and customer IDs, and we will use a predefined one for emails. After that, we will define the DLP rule, where we must configure the Boolean expression that determines the match condition.

#### Creating a Data Pattern for USA Mobile numbers

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns.** Click + Add, as shown in the image below.

Next, we define the values with a simple regex for USA mobile numbers, making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

## Creating a Data Pattern for Contract id

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns. Click + Add.**

Next, we define the values with a simple regex for Contract id based on our Database , making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

**Data Patterns**

Name: contract\_reference\_number\_ctr

Regex: [cC][tT][rR][\_][0-9][4][\_][0-9][4] (highlighted with a red box)

Keywords: contract, reference (highlighted with a red box)

Range From: Anywhere

Range Window (Bytes): 200

### Creating a Data Pattern for Customer id

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns. Click + Add.**

Next, we define the values with a simple regex for Customer id based on our Database , making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

**Data Patterns**

Name: customer\_id\_account\_number\_cust

Regex: [cC][uU][sS][tT][\_][0-9][6] (highlighted with a red box)

Keywords: customer, account (highlighted with a red box)

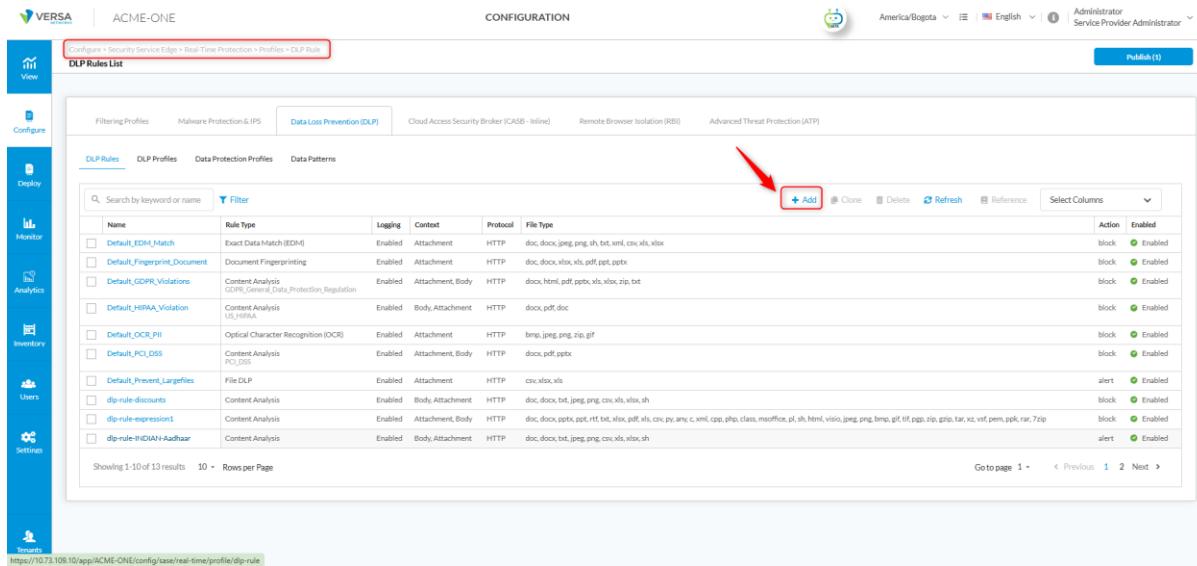
Range From: Anywhere

Range Window (Bytes): 200

### Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule.**

Click + Add, as shown in the image below.



The screenshot shows the Versa Configuration interface for the 'ACME-ONE' service. The left sidebar has icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main area is titled 'CONFIGURATION' and shows the 'DLP Rules List'. The table header includes columns for Name, Rule Type, Logging, Content, Protocol, File Type, and Action. The 'Action' column shows 'Enabled' for most rules and 'Enabled' for the 'Add' button. The table lists various DLP rules, such as 'Default\_EDM\_Match', 'Default\_Fingerprint\_Document', and 'Default\_GDPR\_Violations'. The bottom of the table shows pagination: 'Showing 1-10 of 13 results' and '10 - Rows per Page'.

You will now see a menu to select the type of DLP rule. In our case, select **Exact Data Match (EDM)**. For details on the different types of DLP rules, refer to **Appendix A (DLP Rule Types)**.

After selecting **Exact Data Match (EDM)**, six configuration steps will appear. We will describe them below:

### Exact Data Match:

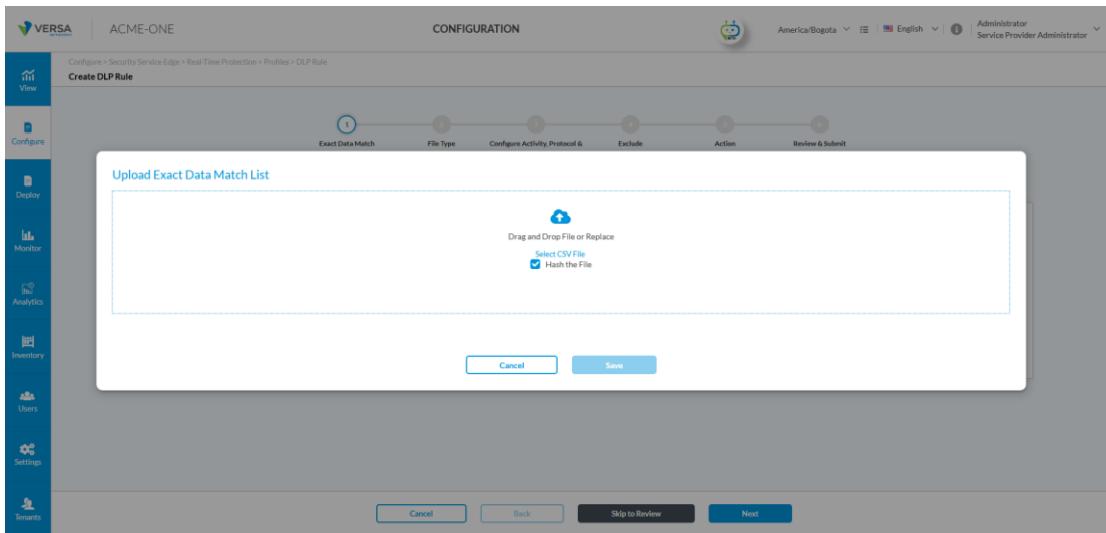
1. **Expression:** We have the following three options:

**Create Expression:** The user defines a boolean expression without relying on a database. This expression can use either predefined or customized data patterns.

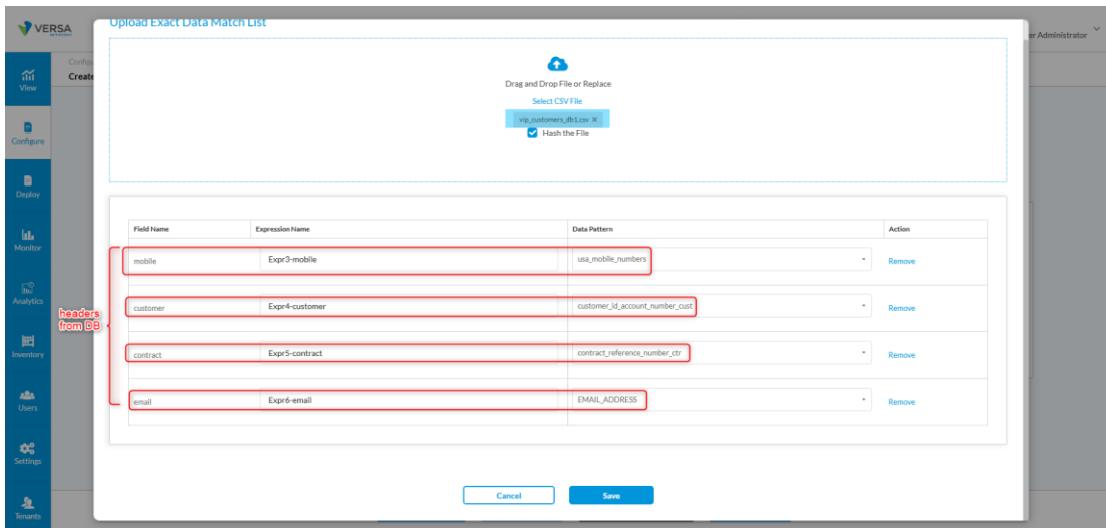
**Upload File:** Allows us to upload our database file, and Versa will automatically display the column headers so the user can decide which ones to use and which data pattern to associate with each of them. For example, if the database has a column with email addresses, that column can be mapped to Versa's predefined data pattern for emails.

**Select File Name:** Allows us to select a file that was previously uploaded to Versa under the *File and Folders* path.

For our case, we will use the option **Upload File**, and the following screen will appear. We can keep the *Hash the File* option enabled, which is selected by default for security reasons. However, if in the future the Administrator wants to download the original database from Concerto, this option must be unchecked; otherwise, the downloaded file will only contain the hashed values.



Next, we either drag and drop the database file or click to select it manually. In our case, we upload the file named *vip\_customers\_db1.csv*. We then proceed to remove the columns that are not relevant to our use case and map each remaining column to the corresponding DLP data pattern created earlier, as shown in the image below.



Click **Save** to continue.

2. **Boolean Operation:** After completing the previous step, we proceed to define the boolean expression that will determine the match condition. For example, in our case, we will use a simple expression that applies an OR to all the expression name headers, as shown in the image below.

ACME-ONE

CONFIGURATION

Edit DLP Rule: DLP-Rule-EDM-CustomersDB

Boolean Operation

Expr3-mobile OR Expr4-customer OR Expr5-contract OR Expr6-email

Click to add data identifier to rule

+ Expr3-mobile + Expr4-customer + Expr5-contract + Expr6-email

Click to add data operator to rule

+ AND + OR + NEAR

Cancel Back Skip to Review Next

3. Click **Next** to continue.

**File Type:** Select the file types you want to inspect. For this use case, select: .csv and .txt.

**NOTE: Supported File Types are CSV, Excel and Text.**

Click on **Next** to continue.

ACME-ONE

CONFIGURATION

Edit DLP Rule: DLP-Rule-EDM-CustomersDB

Exact Data Match

File Type

Configure Activity, Protocol & Context

Exclude

Action

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

CSV

txt

Search for File Type

File Types (37)

CSV

DOC

DOCX

XML

CPP

PHP

CLASS

MSOFFICE

PDF

Cancel Back Skip to Review Next

## Configure Activity, Protocol & Context:

1. **Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**.

2. **Web Protocol:** Select HTTP.
3. **Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments**.

The screenshot shows the VERSA Configuration interface for creating a DLP rule. The left sidebar has buttons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, and Tenants. The main area shows the 'Edit DLP Rule: DLP-Rule-EDM-CustomersDB' screen. The top navigation bar includes 'ACME-ONE', 'CONFIGURATION', 'America/Bogota', 'English', 'Administrator', and 'Service Provider Administrator'. A progress bar at the top indicates the rule is 60% complete. The 'Configure Activity, Protocol & Context' step is currently selected. The configuration screen includes sections for Activity (upload), Protocol (Web Protocol, HTTP selected), and Context (Header, Body, Attachment selected). The 'Next' button at the bottom is highlighted with a red box and a red number 4.

**Exclude:** Specify the file name(s) that should be excluded from DLP inspection. In our case there is no need to exclude any files so we can leave this field blank and click **Next**.

**Action:** Define the action to be executed when the rule is triggered. Several options are available, including:

- Allow
- Alert
- Block
- Reject

In our case, we will select **Block**. For more information on the different actions, refer to **Appendix B: DLP Rule Actions**.

ACME-ONE

CONFIGURATION

Edit DLP Rule: DLP-Rule-EDM-CustomersDB

Exact Data Match File Type Configure Activity, Protocol & Context Exclude Action Review & Submit

Action: Block (1) Logging (2)

Notification Profile: Select

Labels: Select

Threat Type: Exfiltration In Content Analysis (3) Threat Severity: Major (4)

Next (5)

**Review & Submit:** Verify that your rule matches the example shown in the image below, then click **Save**.

Review your DLP Rule configuration below

**General**

|   |   |
|---|---|
| <b>Name *</b> <span style="color: #0070C0;">(i)</span><br><input type="text" value="DLP-Rule-EDM-CustomersDB"/> | <b>Description</b><br><input type="text" value="Enter description name"/> |
| <b>Tags</b><br><input type="text" value="Press Enter to add..."/>   |   |
| <input checked="" type="checkbox"/> <b>Rule is Enabled</b>  |   |

---

**Match Conditions**  
Type of traffic that will be scanned for Data Loss Prevention

|   |  |
|---|--|
| <b>File Type</b> <span style="color: #0070C0;">(i)</span> <span style="float: right;"><a href="#">Edit</a></span> | <input type="checkbox"/> <b>csv</b><br><input type="checkbox"/> <b>txt</b> |
| <b>Protocol</b> <span style="color: #0070C0;">(i)</span> <span style="float: right;"><a href="#">Edit</a></span>  | <input type="checkbox"/> <b>HTTP</b>                                       |
| <b>Context</b> <span style="color: #0070C0;">(i)</span> <span style="float: right;"><a href="#">Edit</a></span>   | <input type="checkbox"/> <b>Attachment</b>                                 |
| <b>Activity</b> <span style="color: #0070C0;">(i)</span> <span style="float: right;"><a href="#">Edit</a></span>  | Upload   |
| <b>Exclude</b> <span style="color: #0070C0;">(i)</span> <span style="float: right;"><a href="#">Edit</a></span>   |  |

---

**Sensitive Data Type & Data Protection Methods** (i) [Edit](#)

**Boolean Operation**  
Expr3-mobile OR Expr4-customer OR Expr5-contract OR Expr6-email

---

**Actions** (i) [Edit](#)

| Action | Set Label | Threat Type                      | Threat Severity |
|--------|-----------|----------------------------------|-----------------|
| block  |           | Exfiltration In Content Analysis | Major           |

## Create the DLP Profile:

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.**

**Click + Add**, as shown in the image below.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

DLP Profiles List

Filtering Profiles Malware Protection & IPS Data Loss Prevention (DLP) Cloud Access Security Broker (CASB - Inline) Remote Browser Isolation (RBI) Advanced Threat Protection (ATP)

DLP Rules DLP Profiles Data Protection Profiles Data Patterns

Add

Then, complete the six configuration steps shown in the following image.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Create DLP Profile

Select DLP Rules

Select an ordered set of rules in which each rule has one or more match conditions and an action.

1 Select DLP Rules Configure Rule Order Applications & Group Reputation Action Review & Submit

Default\_EDM\_Match

Actions: block

Profile

Match Condition: Context Attachment

File Type: docx|pdf|png|jpg|txt|xml|csv|xls|xlsx

Cancel Back Skip to Review Next

**Select DLP Rules:** In the **User Defined Rules** section, search for the rule you created earlier, select it, and click **Next.** It should look like the example shown in the image below.

The screenshot shows the 'Create DLP Profile' configuration page. The 'Select DLP Rules' step is active. A dropdown menu labeled 'User-Defined Rules' is open, with the option 'DLP-Rule-EDM-CustomersDB' selected. To the right, a detailed view of this rule is shown, including its actions (block), profile, and match conditions (Context: Attachment, File Type: csvtxt, Activity: upload). At the bottom of the screen, the 'Next' button is highlighted with a red box and the number 3.

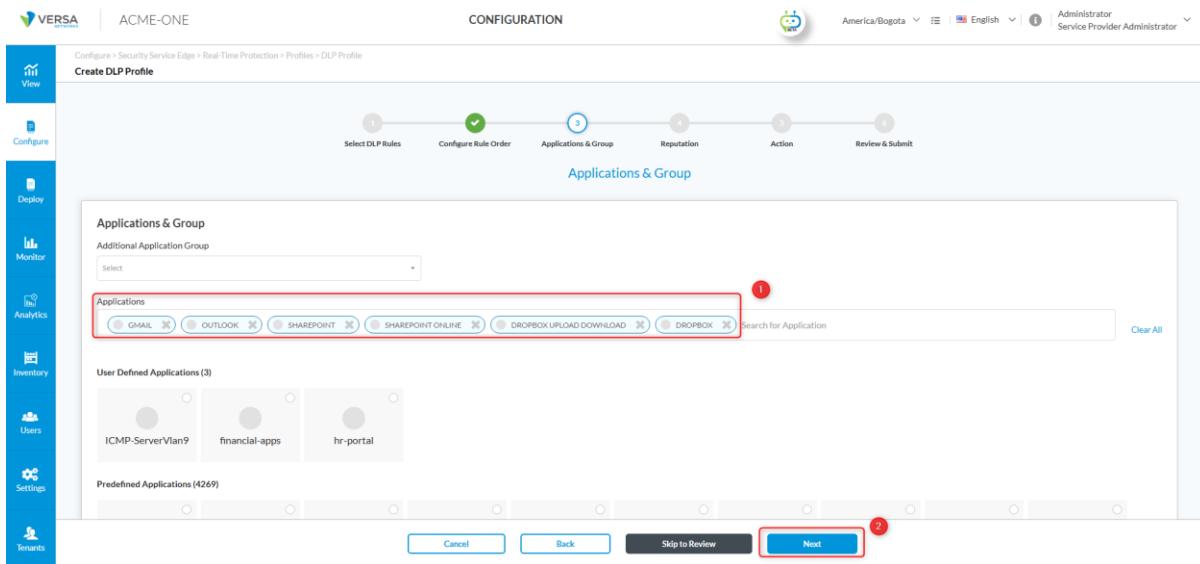
**Configure Rule Order:** Order does not apply for this use case since we have selected only a single rule, so click **Next.**

**Applications & Group:** In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select **Gmail, Outlook, SharePoint** and **Dropbox** then click **Next**, as shown in the image below.

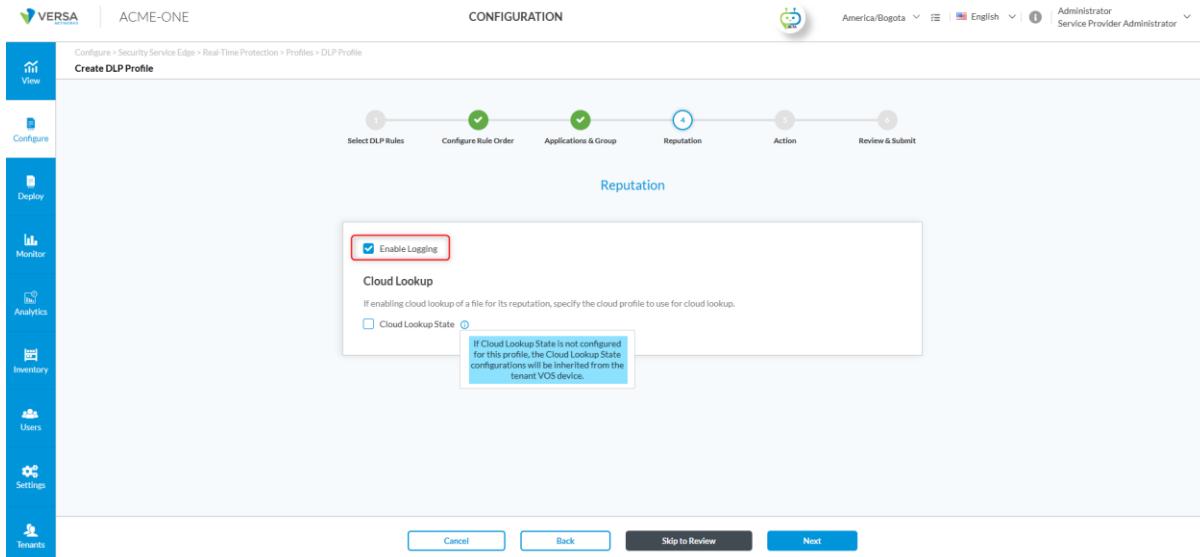
Notes:

- In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.

- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.



**Reputation:** Select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is optional; for more information, you can visit the following link: [How to Configure Cloud Lookup](#).



#### Action:

**Actions:** Set the default action set to **Allow**. The default action is applied if none of the scanned data matches a rule.

**Logging:** Click on the toggle button to enable logging.

**Exit on First Rule Match:** Leave the default action set to **disabled**.

Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.

**Review & Submit:** Assign a name, then review the configuration and click the **Save** button.

## Step 2: Create the TLS decryption rule for the cloud applications we will test (Gmail, Outlook, SharePoint and Dropbox).

To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., Gmail, Outlook, SharePoint and Dropbox).

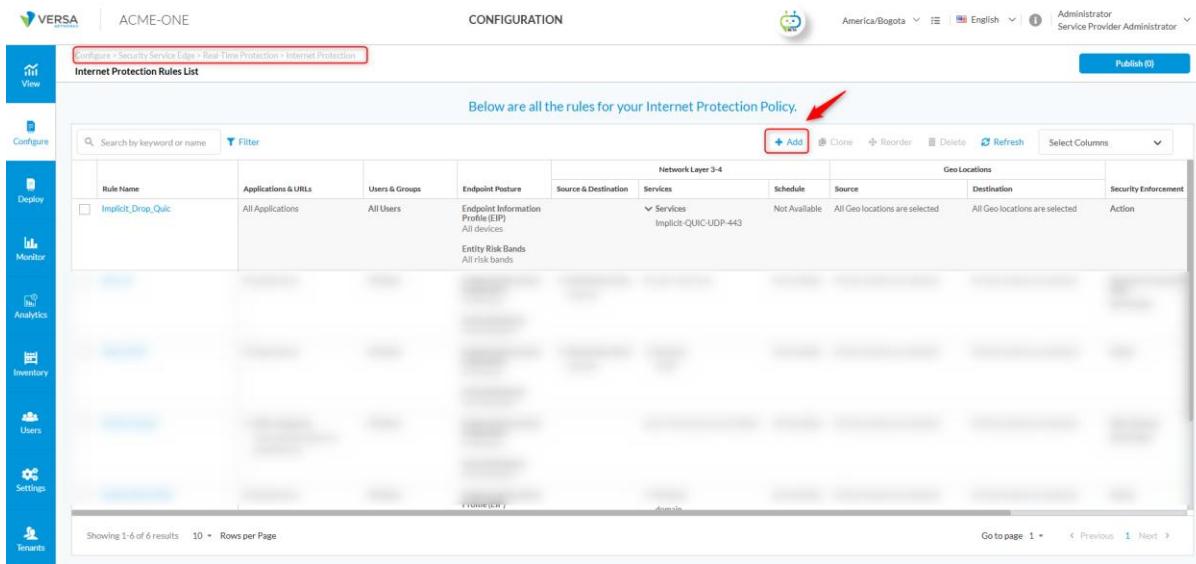
If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

## Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Internet Protection.**

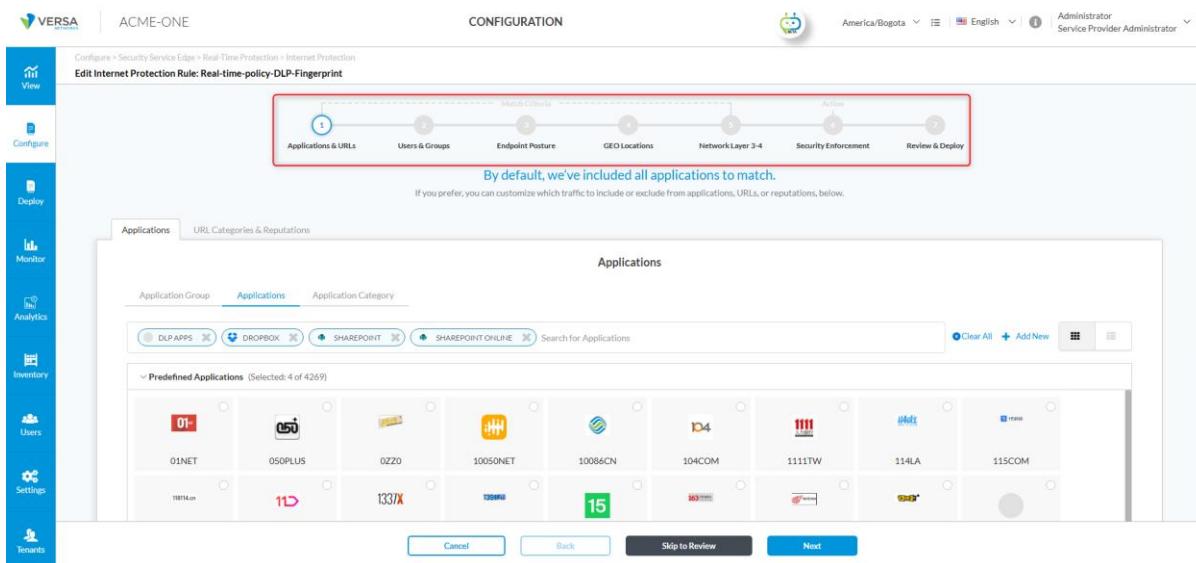
**Click + Add**, as shown in the image below.



Below are all the rules for your Internet Protection Policy.

| Rule Name          | Applications & URLs | Users & Groups | Endpoint Posture                                  | Network Layer 3-4                 | Geo Locations                                   | Security Enforcement                     |
|--------------------|---------------------|----------------|---|-----------------------------------|---|--|
| Implicit_Drop_Quic | All Applications    | All Users      | Endpoint Information Profile (EIP)<br>All devices | Services<br>Implicit-QUIC-UDP-443 | Not Available<br>All Geo locations are selected | All Geo locations are selected<br>Action |

Then, complete the seven configuration steps shown in the following image.



By default, we've included all applications to match.  
If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

Applications

Application Group Applications Application Category

Predefined Applications (Selected: 4 of 4269)

|          |         |       |          |         |         |        |       |        |
|----------|---------|-------|----------|---------|---------|--------|-------|--------|
| 01NET    | 050PLUS | 0ZZO  | 10050NET | 10086CN | 104COM  | 1111TW | 114LA | 115COM |
| 18814.cn | 11D     | 1337X | 123456   | 15      | 103.COM | 1111TW | 114LA | 115COM |

**Applications & URLs:** Select the applications to which we will apply our DLP module. In our case, we choose Gmail, Outlook, SharePoint and Dropbox.

**Users & Groups:** Select our test group and then click Next. In our case, it can be the (VIP) or (Finance) group coming from our LDAP-AD.

**Endpoint Posture:** You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

**Geolocation:** You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

**Network Layer 3-4:** You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

**Security Enforcement:** Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **DLP-Profile-EDM**, which is the one we created. Click **Next**.

**Review & Validate:** Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.

Review your Internet Protection Policy configurations below.  
Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

### General

Name \*  Description

Tags

Rule is Disabled

### Applications & URLs

[Edit](#)

Applications Custom Selection

- Applications | 6
  - Dropbox
  - DROPBOX\_UPLOAD\_DOWNLOAD

### Users & Groups

[Edit](#)

Users & Groups AD-DC1  
User Risk Bands All Risk Bands

Users Device Groups All Device Groups

- User Group | 2
  - Name
    - vip
    - hr

### Endpoint Posture

[Edit](#)

### GEO Locations

[Edit](#)

Source  All source Geo locations are selected  
Destination  All destination Geo locations are selected

### Network Layer 3-4

[Edit](#)

Services  All Services  
destination  
Zones  Internet

### Security Enforcement

[Edit](#)

Enforcements DLP-Profile-EDM

Finally, publish the changes applied in Concerto and proceed with the verifications.

## Step 4. Perform tests and validate the behaviour.

To perform the tests, we only need to upload a test file from Gmail, Outlook, SharePoint, or Dropbox that contains partial information from the original database. For simplicity, we are going to use the same file we used for the database (*vip\_customers\_db1.csv*). Below, you will see a portion of the data contained in the CSV.

*vip\_customers\_db1.csv*

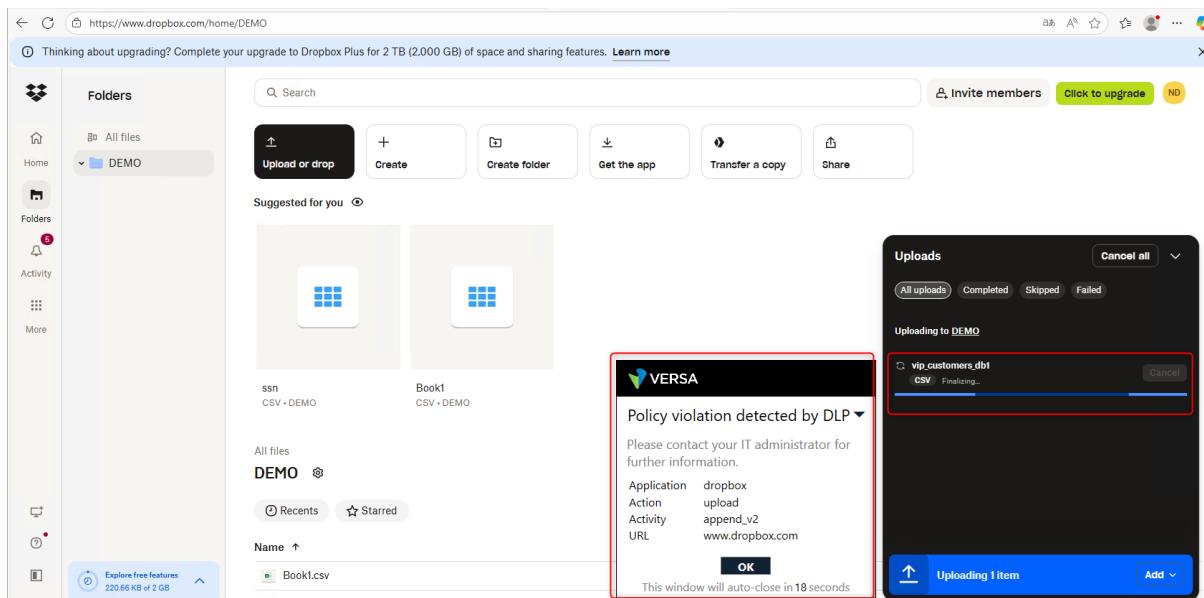
---

*firstname,lastname,gender,mobile,customer,contract,email*  
Ava,Jackson,Male,3140474786,CUST\_000001,CTR\_1001\_0001,ava.jackson@initech.com  
Ava,Harris,Female,7359869480,CUST\_000002,CTR\_1001\_0002,ava.harris@acmeenergy.com  
Lucas,Lee,Female,9411336152,CUST\_000003,CTR\_1001\_0003,luca.lee@hooli.com  
Olivia,Lee,Male,7110163088,CUST\_000004,CTR\_1001\_0004,olivia.lee@wayneenterprises.com  
Daniel,Johnson,Female,2647706560,CUST\_000005,CTR\_1001\_0005,daniel.johnson@wayneenterprises.com  
Emma,Taylor,Male,5041660904,CUST\_000006,CTR\_1001\_0006,emma.taylor@umbrella-corp.com  
Daniel,Martinez,Male,3286054734,CUST\_000007,CTR\_1001\_0007,daniel.martinez@initech.com  
Ethan,Harris,Male,4032561166,CUST\_000008,CTR\_1001\_0008,ethan.harris@aurora-services.com  
Daniel,Diaz,Male,4129341454,CUST\_000009,CTR\_1001\_0009,daniel.diaz@globex.com  
Emma,Allen,Female,4604552725,CUST\_000010,CTR\_1001\_0010,emma.allen@cascadeinc.com

---

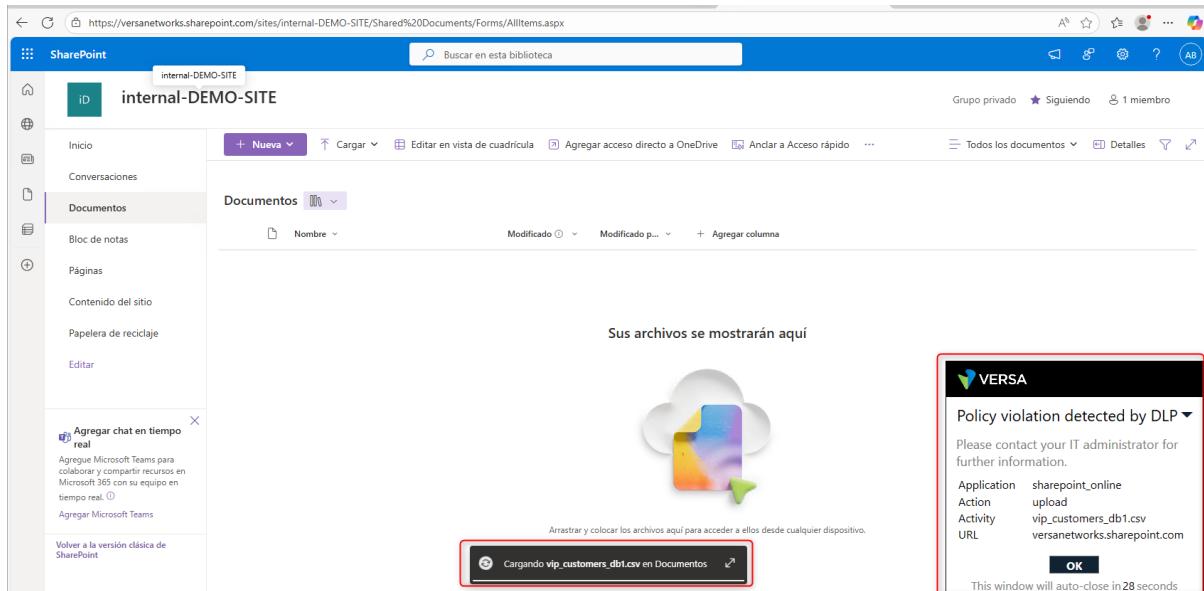
Now, Upload from Gmail, Outlook, SharePoint or Dropbox the file created with the data mentioned before, which should be blocked because the **Block** action was selected. See the images below.

Dropbox test



The screenshot shows a Dropbox interface. At the top, a banner suggests upgrading to Dropbox Plus. The left sidebar shows 'Folders' with a 'DEMO' folder selected. The main area shows 'Suggested for you' with two files: 'ssn CSV - DEMO' and 'Book1 CSV - DEMO'. A central modal window displays a 'Policy violation detected by DLP' message from 'VERSA'. The message states: 'Policy violation detected by DLP', 'Please contact your IT administrator for further information.', and provides details: 'Application: dropbox', 'Action: upload', 'Activity: append\_v2', and 'URL: www.dropbox.com'. An 'OK' button is at the bottom, and a note says 'This window will auto-close in 18 seconds'. To the right, an 'Uploads' dialog shows an item named 'vip\_customers\_db1 CSV - Finalizing...' with a progress bar. The progress bar is highlighted with a red box.

## SharePoint test



The screenshot shows a SharePoint 'Documentos' library. The left sidebar includes 'Documentos' under 'internal-DEMO-SITE'. The main area shows a message: 'Sus archivos se mostrarán aquí' with a cloud icon. Below it, a text box says 'Arrastrar y colocar los archivos aquí para acceder a ellos desde cualquier dispositivo.' A progress bar at the bottom indicates 'Cargando vip\_customers\_db1.csv en Documentos'. A central modal window displays a 'Policy violation detected by DLP' message from 'VERSA'. The message states: 'Policy violation detected by DLP', 'Please contact your IT administrator for further information.', and provides details: 'Application: sharepoint\_online', 'Action: upload', 'Activity: vip\_customers\_db1.csv', and 'URL: versanetworks.sharepoint.com'. An 'OK' button is at the bottom, and a note says 'This window will auto-close in 28 seconds'. The progress bar is highlighted with a red box.

When checking the logs in **Concerto > Analytics > DLP Logs**, you should see something similar to the images below.

| Receive Time                  | Appliance | Application       | User              | Match Type     | Match String  | Match Component | Action | Pattern            | Data Profile | Profile       |
|-------------------------------|-----------|-------------------|-------------------|----------------|---|-----------------|--------|--------------------|--------------|---------------|
| Sep 29th 2025, 9:21:01 AM -05 | demo1     | owa               | vip1@acme-one.com | ExactDataMatch | Expr3-mobile OR Expr4-customer OR Expr5-contract OR Expr6-email | ExactDataMatch  | block  | usa_mobile_numbers | EDM Profile  | dlp-profile-1 |
| Sep 29th 2025, 9:19:42 AM -05 | demo1     | sharepoint_online | vip1@acme-one.com | ExactDataMatch | Expr3-mobile OR Expr4-customer OR Expr5-contract OR Expr6-email | ExactDataMatch  | block  | usa_mobile_numbers | EDM Profile  | dlp-profile-1 |
| Sep 29th 2025, 9:06:21 AM -05 | demo1     | dropbox           | vip1@acme-one.com | ExactDataMatch | Expr3-mobile OR Expr4-customer OR Expr5-contract OR Expr6-email | ExactDataMatch  | block  | usa_mobile_numbers | EDM Profile  | dlp-profile-1 |
| Sep 29th 2025, 9:02:47 AM -05 | demo1     | gmail             | vip1@acme-one.com | ExactDataMatch | Expr3-mobile OR Expr4-customer OR Expr5-contract OR Expr6-email | ExactDataMatch  | block  | usa_mobile_numbers | EDM Profile  | dlp-profile-1 |

## Use Case 4: Collaboration Chat Monitoring with DLP for Bad Words

This case demonstrates how **ACME-ONE** leverages **DLP profiles in Versa Networks** to detect and flag inappropriate or non-compliant language in collaboration tools, specifically **Slack** chats. The objective is to monitor communication channels for the use of prohibited terms, ensuring compliance with corporate policies and maintaining a professional environment.

The **Collaboration and HR departments** at ACME-ONE are responsible for monitoring employee chat activity for the following categories of concern:

- Use of offensive, discriminatory, or profane language (bad words).
- Custom-defined terms that reflect ACME-ONE's internal compliance policies (e.g., code words, sensitive project names, or restricted topics).

Versa's DLP engine allows combining **predefined bad words dictionaries** with **custom keyword lists**, ensuring that both general profanity and organization-specific terms are detected in Slack chat messages.

To reduce the risk of misconduct or policy violations in internal collaboration, Versa's DLP engine is configured to **inspect chat content from Slack (web and desktop app)** and apply DLP actions when matches are detected.

Using Versa's integrated DLP engine, ACME-ONE defines a DLP policy named "**Bad Words and Inappropriate Language Monitoring**" with the following conditions:

| Policy Name  | Conditions   | Details   |
|--|--|---|
| <b>Bad Words and Inappropriate Language Monitoring</b> | Match on predefined Bad Words dictionary <b>OR</b> custom keyword list | 1) Enable Versa's predefined dictionary for profanity/offensive language. 2) Create a custom keyword list with terms specific to ACME-ONE's compliance rules (e.g., project code names, restricted slang). 3) Apply the policy to outbound and internal chat traffic within <b>Slack</b> . 4) Actions include Alerting, Logging, and optional Blocking. |

## Configuration steps

The DLP configuration consists of the following steps, which are described in detail below:

1. Create DLP objects
  - Create a **DLP Pattern for custom Badwords**.
  - Create a **DLP Rule** (conditions that trigger DLP checks).
  - Create and assign a **DLP Profile / Policy** (the policy that ties the data profile and rules to enforcement actions).
2. **Create TLS decryption rule** for the cloud apps you will test (**Slack**).
3. **Create real-time protection rule** that applies the DLP profile to the cloud apps defined in Step 2.
4. **Perform tests and validate the behaviour**. Execute test cases, verify detection and enforcement, and record results.

### Step 1: Create DLP objects

For this use case (Content Analysis), we will use the predefined Bad Words data pattern and create an additional custom pattern if needed. These patterns will be referenced in the DLP rule, where a Boolean expression (e.g., *Predefined\_BadWords OR Custom\_BadWords*) defines the match condition.

#### Creating a Data Pattern for Bad Words

Navigate to

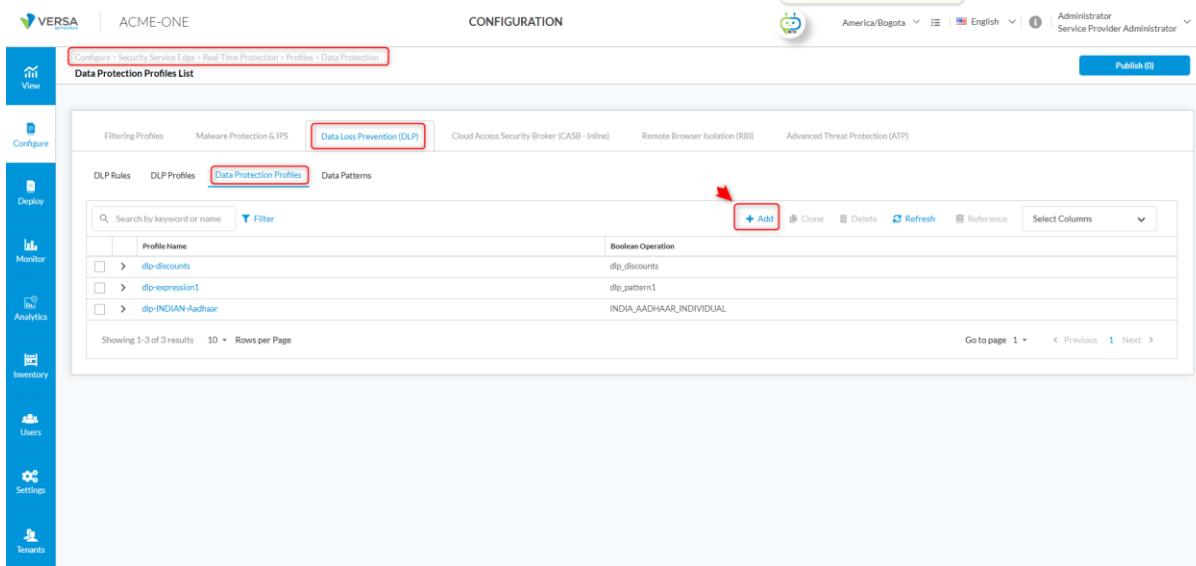
**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Patterns.** Click **+ Add**, as shown in the image below.

Next, we define the values with a simple regex for Bad Words, making sure the keywords are included and related to the content, just as shown in the image below. Finally, click on Save.

## Creating a Data Protection Profile

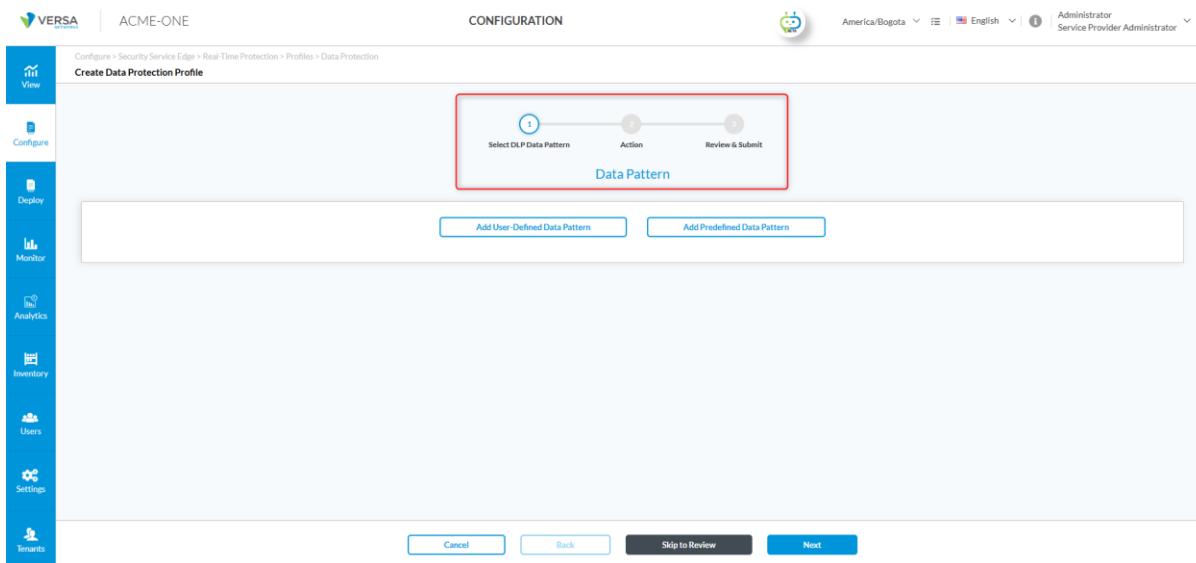
Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > Data Protection.** Click **+ Add**, as shown in the image below.



The screenshot shows the VERSA Configuration interface for the 'ACME-ONE' tenant. The left sidebar contains icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, and Tenants. The main header is 'CONFIGURATION' with sub-links for Filtering Profiles, Malware Protection & IPS, Data Loss Prevention (DLP), Cloud Access Security Broker (CASB - Inline), Remote Browser Isolation (RBI), and Advanced Threat Protection (ATP). The 'Data Protection Profiles' tab is selected. A red box highlights the 'Add' button in the top right corner of the list table. The table lists existing profiles: 'dip-discounts', 'dip-expression1', and 'INDIA\_AADHAAR\_INDIVIDUAL'. The bottom of the table shows 'Showing 1-3 of 3 results' and 'Rows per Page' dropdown.

Next, complete the three configuration steps shown in the image below.



The screenshot shows the 'Create Data Protection Profile' wizard. The left sidebar is identical to the previous screenshot. The main header is 'CONFIGURATION' with the sub-link 'Create Data Protection Profile'. The wizard steps are: 'Select DLP Data Pattern' (highlighted with a red box), 'Action', and 'Review & Submit'. At the bottom, there are buttons for 'Add User-Defined Data Pattern' and 'Add Predefined Data Pattern'. Below these are 'Cancel', 'Back', 'Skip to Review', and 'Next' buttons.

**Select DLP Data Pattern:** Select Add Predefined Data Pattern and search for the one you need. In this example, enable **GLOBAL\_BAD\_WORDS**, then click Save and then click on User-Defined Data Pattern and enable **ProhibitedWords** (created in the last step) Next click on Save

**Action:** Click the + icon next to the data identifier **GLOBAL\_BAD\_WORDS** to add it to your Boolean expression. Then, insert the OR operator and click the + icon again to add **ProhibitedWords**. See the image below.

See the image below.

ACME-ONE

CONFIGURATION

Select DLP Data Pattern

Action

Review & Submit

Configure Action

Boolean Operation

ProhibitedWords OR GLOBAL\_BAD\_WORDS

Click to add data identifier to rule

Click to add data operator to rule

1 + GLOBAL\_BAD\_WORDS

2 + ProhibitedWords

3 AND OR NEAR NOT

Cancel Back Skip to Review Next

Once the data identifier has been added, click **Next** to continue.

**Review & Submit:** Assign a name to your Data Protection profile and click **Save**.

ACME-ONE

CONFIGURATION

Name\*

Description

Tags

Data Patterns

User-Defined

Predefined

Action

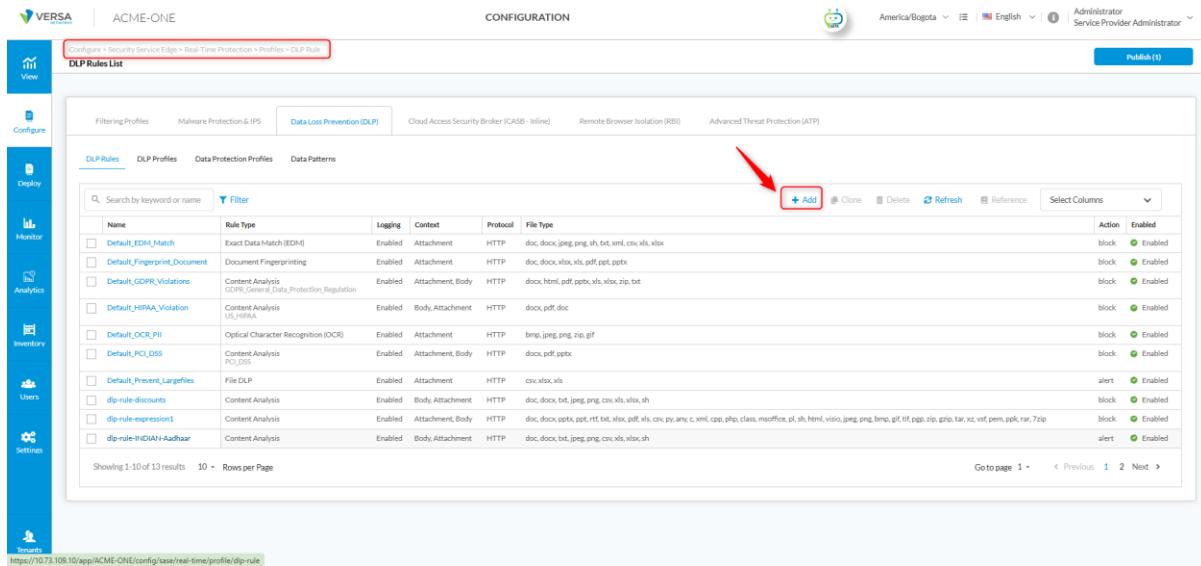
Boolean Operation

Cancel Back Save

### Create DLP Rule:

Navigate to **Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule**.

Click **+ Add**, as shown in the image below.



The screenshot shows the VERSA Configuration interface for the 'ACME-ONE' service. The left sidebar has icons for View, Configure, Deploy, Monitor, Analytics, Inventory, Users, and Settings. The main area is titled 'CONFIGURATION' and shows the 'DLP Rules List' under 'Data Loss Prevention (DLP)'. The table header includes columns for Name, Rule Type, Logging, Content, Protocol, File Type, Action, and Enabled. The 'Action' column contains icons for Block, Alert, and Reference. The 'Enabled' column shows green checkmarks. A red arrow points to the 'Add' button in the top right corner of the table header. The URL in the browser is <https://10.73.108.10/app/ACME-ONE/config/sase/real-time/profile/dlp-rule>.

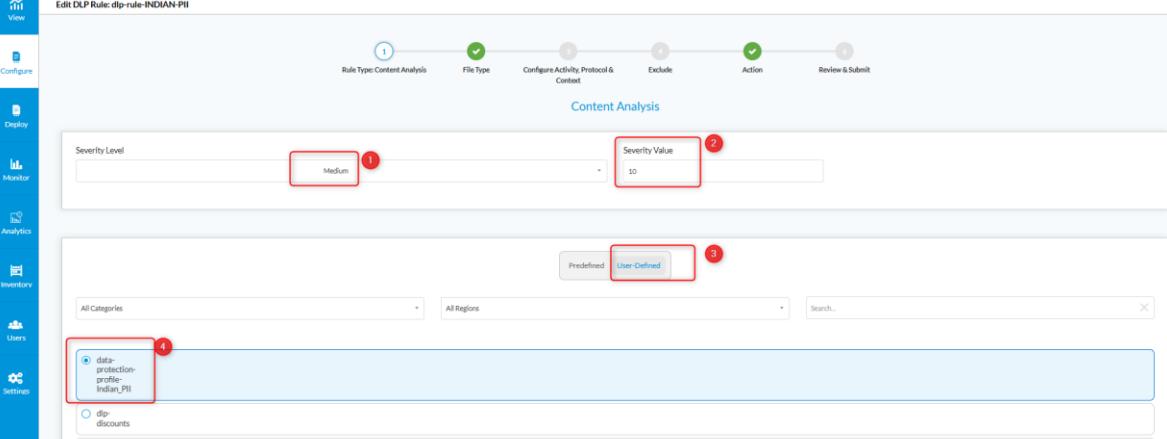
You will now see a menu to select the type of DLP rule. In our case, select **Content Analysis**. For details on the different types of DLP rules, refer to **Appendix A (DLP Rule Types)**.

After selecting **Content Analysis**, six steps will appear. We will describe them below:

Rule Type: Content Analysis

5. **Severity Level:** Select the severity assigned to the DLP event. Each level has a default match threshold: Low = 1, Medium = 10, High = 20, Critical = 30. For this example, choose **Medium**.
6. **Severity Value:** Define a custom number of occurrences required to trigger the rule. The counter starts from 0. For example, if you set the value to 10, the rule will trigger starting from the 11th DLP event. In this case, set the value to **10**.
7. **Predefined/User Defined:** Select **User Defined** and then choose the **Data Protection Profile** we created earlier, named data-protection-profile-AADHAAR.
8. Click **Next** to continue.

*Note: In DLP, the Severity Level defines the default number of matches required to trigger a rule (Low=1, Medium=10, High=20, Critical=30). If a custom Severity Value is set, it overrides the default threshold (e.g., High=20 but Value=5 → triggers after 5 occurrences).*



VERSACONNECT

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule

Edit DLP Rule dlp-rule-INDIAN-PII

Rule Type: Content Analysis

File Type

Configure Activity, Protocol & Context

Exclude

Action

Review & Submit

Content Analysis

Severity Level

Medium

Severity Value

10

Predefined

User-Defined

All Categories

All Regions

Search...

4

5

data-protector-profile-INDIAN PII

dip-discounts

dip-expression1

Cancel

Back

Skip to Review

Next

**File Type:** Select the file types you want to inspect. For this use case select: **.txt**, **.doc**, **.docx**, **.csv**, etc.

Click on **Next** to continue.

**Note: In the image below, you will see the file types supported for DLP.**

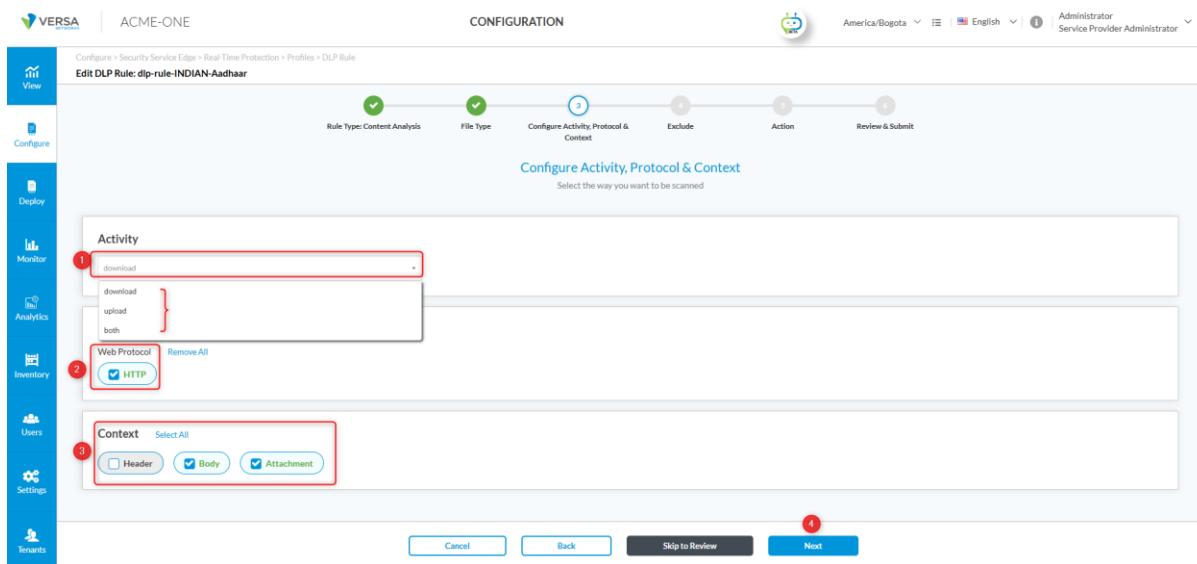
| File Types (37)   |  |  |  |  |   |   |  |  |   |   |  |   |
|---|--|--|--|--|---|---|--|--|---|---|--|---|
|  c   |  doc  |  docx |  xml  |  cpp  |  php   |  class |  msoffice |  pdf  |  pl  |  ppt |  pptx |  rtf |
|  sh  |  xls  |  txt  |  xlsx |  html |  visio |  jpeg  |  png      |  bmp  |  gif |  tif |  pgp  |  csv |
|  zip |  gzip |  tar  |  xz   |  vsf  |  pem   |  ppk   |  rar      |  7zip |  py  |  any |  |   |

## Configure Activity, Protocol & Context:

4. **Activity:** Select the activity to which the DLP module will be applied. In our case, select **Upload**.

5. **Web Protocol:** Select HTTP.

6. **Context:** Defines which part of the packet or message will be inspected. For this example, select **Attachments** and **Body**.



Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule  
Edit DLP Rule: dlp-rule-INDIAN-Aadhaar

Rule Type: Content Analysis      File Type      Configure Activity, Protocol & Context      Exclude      Action      Review & Submit

Configure Activity, Protocol & Context  
Select the way you want to be scanned

Activity

1 download

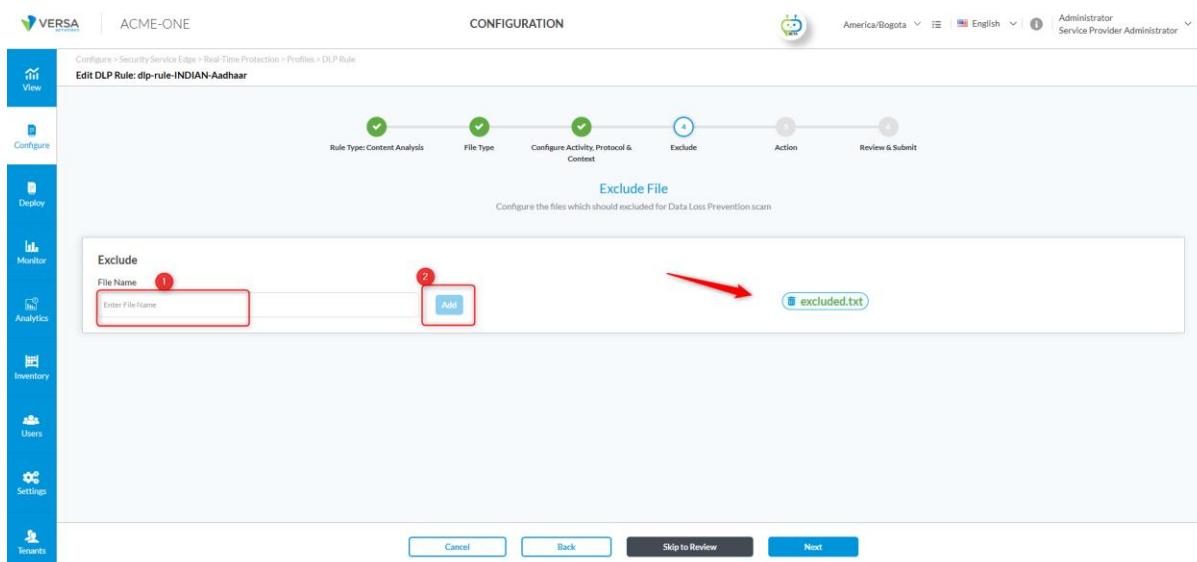
2 download  
upload  
both

3 Web Protocol      Remove All  
HTTP

4 Context      Select All  
Header      Body      Attachment

Cancel      Back      Skip to Review      Next

**Exclude:** Specify the file name(s) that should be excluded from DLP inspection.



Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule  
Edit DLP Rule: dlp-rule-INDIAN-Aadhaar

Rule Type: Content Analysis      File Type      Configure Activity, Protocol & Context      Exclude      Action      Review & Submit

Exclude File  
Configure the files which should excluded for Data Loss Prevention scan

Exclude

1 File Name  
Enter File Name

2 Add  
excluded.txt

3 excluded.txt

4 Cancel      Back      Skip to Review      Next

**Action:** Define the action to be executed when the rule is triggered.

Several options are available, such as:

- Allow

- Alert
- Block
- Reject
- Reject

In our case, we will select **Alert** because we only want a log to be generated in the platform without blocking the user or displaying any pop-up messages. This option is commonly used when tuning DLP rules. For more information on the different actions, refer to **Appendix B: DLP Rule Actions**.

The screenshot shows the VERSA Configuration interface for editing a DLP rule. The main window is titled 'Edit DLP Rule: dlp-rule-INDIAN-Aadhaar'. The 'Action' section is highlighted with a red box, showing 'Alert' selected. Other options like 'Logging' and 'File Dlp' are also visible. The 'Threat Severity' is set to 'Normal'. The interface includes a sidebar with 'View', 'Configure', 'Deploy', 'Monitor', 'Analytics', 'Inventory', 'Users', 'Settings', and 'Tenants' options.

**Review & Submit:** Verify that your rule matches the example shown in the image below, then click **Save**.

Review your DLP Rule configuration below

**General**

|  |  |
|--|--|
| <p>Name* <a href="#">?</a></p> <input type="text" value="dip-rule-11IDIAN-Aadhaar"/> | <p>Description</p> <input type="text" value="Enter description name"/> |
| <p>Tags</p> <input type="text" value="Press Enter to add"/>                          |  |
| <input checked="" type="checkbox"/> Rule Is Enabled                                  |  |

**Match Conditions**

Type of traffic that will be scanned for Data Loss Prevention

|                                       |   |
|---------------------------------------|---|
| <b>File Type</b> <a href="#">Edit</a> | <input type="checkbox"/> doc <input type="checkbox"/> docx <input type="checkbox"/> txt <input type="checkbox"/> jpg <input type="checkbox"/> png <input type="checkbox"/> csv <input type="checkbox"/> xls <input type="checkbox"/> xlsx <input type="checkbox"/> sh |
| <b>Protocol</b> <a href="#">Edit</a>  | <input type="checkbox"/> HTTP   |
| <b>Context</b> <a href="#">Edit</a>   | <input type="checkbox"/> Body <input type="checkbox"/> Attachment   |
| <b>Activity</b> <a href="#">Edit</a>  |   |
| <b>Exclude</b> <a href="#">Edit</a>   | <input type="checkbox"/> excluded.txt   |

**Sensitive Data Type & Data Protection Methods** [Edit](#)

Content Analysis

|                                 |                |                |
|---------------------------------|----------------|----------------|
| User-Defined Data Profile       | Severity Level | Severity Value |
| data-protection-profile-AADHAAR | Critical       | 2              |

**Actions** [Edit](#)

| Action | Set Label | Threat Type | Threat Severity |
|--------|-----------|-------------|-----------------|
| alert  |           | File Dlp    | Normal          |

## Create the DLP Profile:

Navigate to

**Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Profile.**

**Click + Add**, as shown in the image below.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

DLP Profiles List

Filtering Profiles Malware Protection & IPS Data Loss Prevention (DLP)

DLP Rules DLP Profiles Data Protection Profiles Data Patterns

Add

Then, complete the six steps shown in the following image.

ACME-ONE

CONFIGURATION

America/Bogota | English | Administrator | Service Provider Administrator

Create DLP Profile

Select DLP Rules

Select an ordered set of rules in which each rule has one or more match conditions and an action.

User-Defined Rules

Default\_EDM\_Match

Default\_Fingerprint\_Document

Default\_GDPR\_Violations

Default\_HIPAA\_Violation

Default\_OCR\_PII

Default\_PCI\_DSS

Default\_EDM\_Match

Actions

Profile

Match Condition

Context Attachment

File Type docdocx|jpg|png|pdf|txt|xml|csv|xls|xlsx

Cancel Back Skip to Review Next

**Select DLP Rules:** In the **User Defined Rules** section, search for the rule you created earlier, select it, and click **Next**. It should look like the example shown in the image below.

ACME-ONE

CONFIGURATION

Edit DLP Profile: DLP-Profile-BADWORDS

Select DLP Rules

Configure Rule Order

Applications & Group

Reputation

Action

Review & Submit

Select DLP Rules

User-Defined Rules

All Categories

All Regions

badword

Default\_Fingerprint\_Document

Actions

Actions block

Profile

Match Condition

Context Attachment

File Type docx/docx/pdf/pptx

Activity both

Selected DLP-Rule-BADWORDS

Cancel Back Skip to Review Next

**Configure Rule Order:** Order does not apply since we have selected only a single rule.

**Applications & Group:** In the **Applications** search field, search for each application to which the DLP profile will be applied. In our case, select **Slack**, then click **Next**, as shown in the image below.

*Notes: - In cases where not all dependent applications are known, adding the generic applications **HTTPS** or **HTTP** to the DLP profile may help. However, this approach is not technically guaranteed to work and could impact unrelated traffic. Therefore, rules applied in real-time protection should remain as specific as possible.*

*- In some cases, you may also need to add dependent applications when dealing with SaaS apps. For example, Gmail relies on additional services such as **gstatic.com** to load resources like icons, scripts, or image previews (e.g., when sending or viewing image attachments). Without allowing these dependencies, the SaaS application may not function correctly.*

ACME-ONE

CONFIGURATION

Edit DLP Profile: DLP-Profile-BADWORDS

Select DLP Rules

Configure Rule Order

Applications & Group

Reputation

Action

Review & Submit

Applications & Group

Additional Application Group

Select

Applications

SLACK

Search for Application

User Defined Applications (2)

ICMP-ServerVlan9 financial-apps hr-portal

Predefined Applications (4269)

01NET 050PLUS 0ZZO 10050NET 104 1111TW 114LA 115COM 118114CN 11ST

Cancel Back Skip to Review Next

**Reputation:** In Versa, *Reputation* refers to a local URL database used to categorize websites and assign reputation scores for web filtering. This local database allows quick lookups for the most common and popular websites.

Additionally, Versa offers the option to enable **Cloud Lookup** to complement the local database.

For our use case, select the **Enable Logging** option to store website reputation events, as shown in the image below. **Cloud Lookup** is optional; for more information, you can visit the following link: [How to Configure Cloud Lookup](#).

The screenshot shows the Versa Configuration interface for creating a DLP profile. The top navigation bar includes 'ACME-ONE', 'CONFIGURATION', and 'Administrator'. The left sidebar lists 'View', 'Configure', 'Deploy', 'Monitor', 'Analytics', 'Inventory', 'Users', 'Settings', and 'Tenants'. The main content area shows a step-by-step wizard: 'Select DLP Rules' (step 1), 'Configure Rule Order' (step 2, marked with a green checkmark), 'Applications & Group' (step 3, marked with a green checkmark), 'Reputation' (step 4, marked with a blue circle), 'Action' (step 5), and 'Review & Submit' (step 6). The 'Reputation' step is currently active. A sub-section titled 'Cloud Lookup' contains an 'Enable Logging' checkbox (which is checked) and a 'Cloud Lookup State' checkbox. A tooltip for 'Cloud Lookup State' states: 'If Cloud Lookup State is not configured for this profile, the Cloud Lookup State configurations will be inherited from the tenant VOS device.' At the bottom of the wizard are buttons for 'Cancel', 'Back', 'Skip to Review', and 'Next'.

### Action:

Actions: Set the default action set to **Allow**. The default action is applied if none of the scanned data matches a rule.

Logging: Click on the toggle button to enable logging.

Exit on First Rule Match: Leave the default action set to **disabled**.

*Note: if multiple DLP rules are configured, this option should be disabled to ensure that all rules are applied to the same session.*

**Review & Submit:** Assign a name, then review the configuration and click the **Save** button.

## Step 2: Create the TLS decryption rule for the cloud applications we will test (Slack).

To ensure that payloads can be inspected and DLP policies applied, a TLS decryption rule must exist for the cloud applications being tested (e.g., Slack).

If you need the detailed step-by-step configuration for creating this rule, refer to **Appendix C: TLS Decryption Rule Configuration**.

## Step 3. Create the real-time protection rule using the DLP profile on the cloud apps defined earlier.

Navigate to **Configure > Security Service Edge > Real-Time Protection > Internet Protection**.

**Click + Add**, as shown in the image below.

VERSÀ | ACME-ONE | CONFIGURATION | America/Bogota | English | Administrator | Service Provider Administrator

Internet Protection Rules List

Below are all the rules for your Internet Protection Policy.

**Add**

| Rule Name          | Applications & URLs | Users & Groups | Endpoint Posture                                  | Source & Destination                | Services                          | Schedule      | Source                         | Destination                    | Security Enforcement |
|--------------------|---------------------|----------------|---|-------------------------------------|-----------------------------------|---------------|--------------------------------|--------------------------------|----------------------|
| Implicit_Drop_Quic | All Applications    | All Users      | Endpoint Information Profile (EIP)<br>All devices | Entity Risk Bands<br>All risk bands | Services<br>Implicit-QUIC-UDP-443 | Not Available | All Geo locations are selected | All Geo locations are selected | Action               |

Showing 1-6 of 6 results 10 Rows per Page Go to page 1 < Previous 1 Next >

Then, complete the seven steps shown in the following image.

VERSABRIDGE | ACME-ONE | CONFIGURATION | America/Bogota | English | Administrator | Service Provider Administrator

Configure > Security Service Editor > Real-Time Protection > Internet Protection

Create Internet Protection Rule

Match Criteria

Action

1 Applications & URLs 2 Users & Groups 3 Endpoint Posture 4 GEO Locations 5 Network Layer 3-4 6 Security Enforcement 7 Review & Deploy

By default, we've included all applications to match.

If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

Applications URL Categories & Reputations

Applications

Application Group Applications Application Category

GMAIL OUTLOOK Search for Applications Clear All Add New

Predefined Applications (Selected: 2 of 4269)

| Icon      | Application Name | Icon  | Application Name | Icon | Application Name | Icon     | Application Name | Icon  | Application Name |
|-----------|------------------|-------|------------------|------|------------------|----------|------------------|-------|------------------|
| 01        | 01NET            | 050   | 050PLUS          | 0220 | 0220             | 10050NET | 10086CN          | 104   | 104COM           |
| 11814.com | 11D              | 1337X | 1337X            | 15   | 15               | 162      | 162              | 114LA | 115COM           |

Cancel Back Skip to Review Next

**Applications & URLs:** Select the applications to which we will apply our DLP module. In our case, we choose Slack.

**Users & Groups:** Select our test group and then click Next. In our case, it can be the (VIP and HR) group coming from our LDAP-AD.

**Endpoint Posture:** You can apply Endpoint Information Profiles and Entity Risk Bands; however, in our case, leave the default settings to apply none and click **Next**.

**Geolocation:** You can filter by Source or Destination Geo Location. In our case, we leave the default setting to **All** and click **Next**.

**Network Layer 3-4:** You can filter by services (Layer 4) such as HTTP, HTTPS, DNS, ICMP, etc. You can also filter by Source & Destination (Layer 3). However, leave the default values and click **Next**.

**Security Enforcement:** Click on the **Security Profiles** option, then select **Data Loss Prevention**. Toggle the switch to enable it, then choose the profile named **DLP-Profile-BADWORDS**, which is the one we created. Click **Next**.

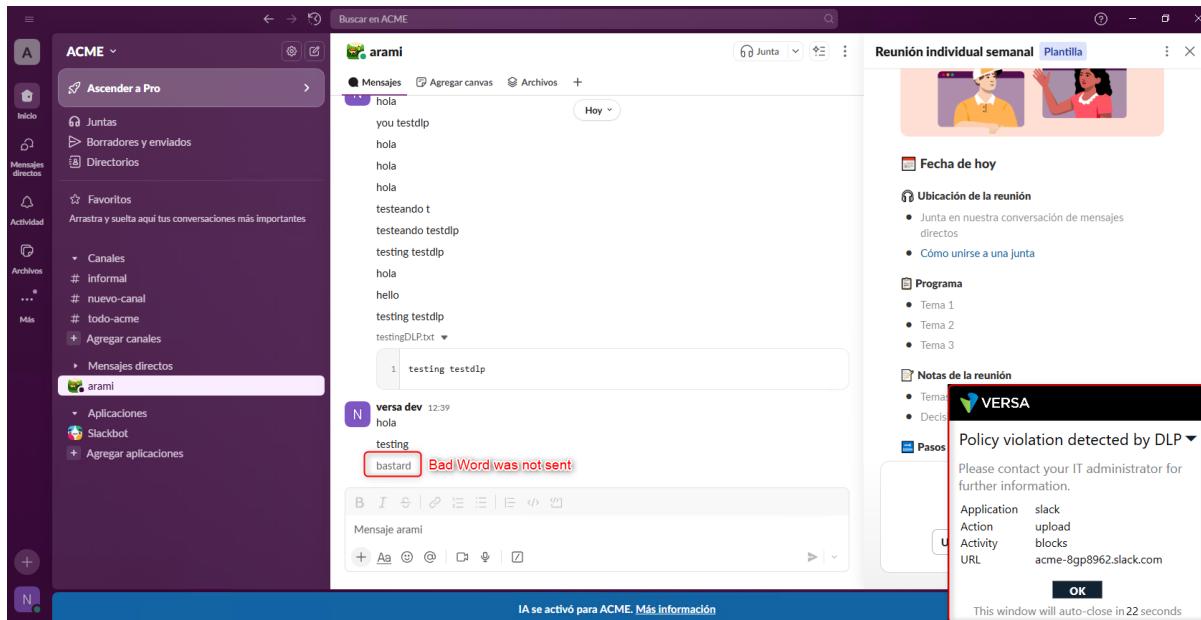
**Review & Validate:** Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.

Finally, publish the changes applied in Concerto and proceed with the verifications.

#### Step 4. Perform tests and validate the behaviour.

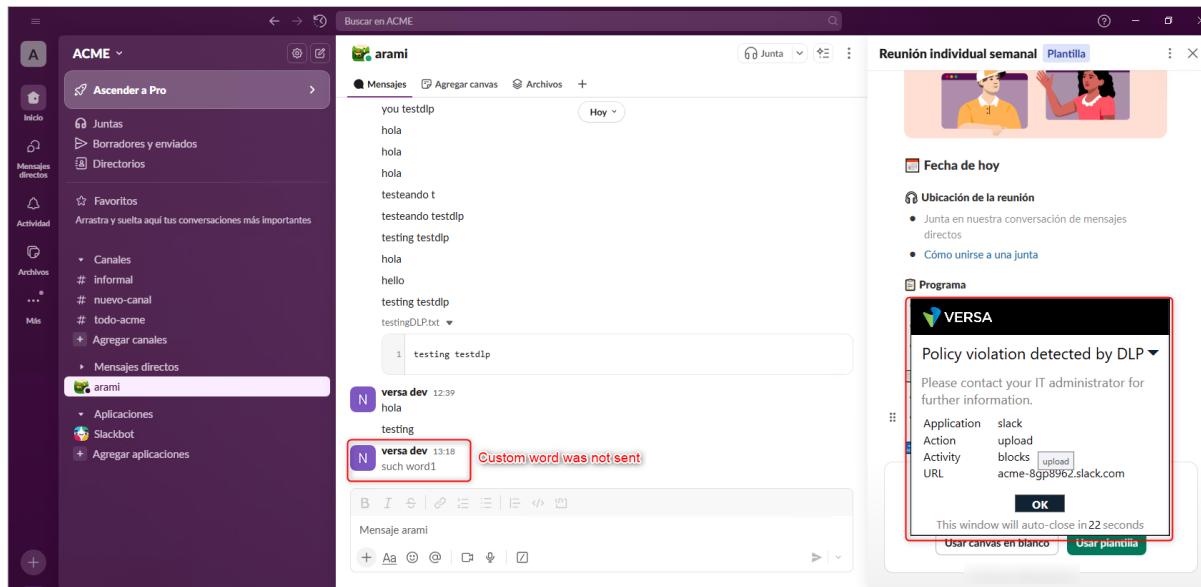
To perform the tests, we only need to send via Slack with the Versa SASE client enabled.

## Slack Test using global bad word sample



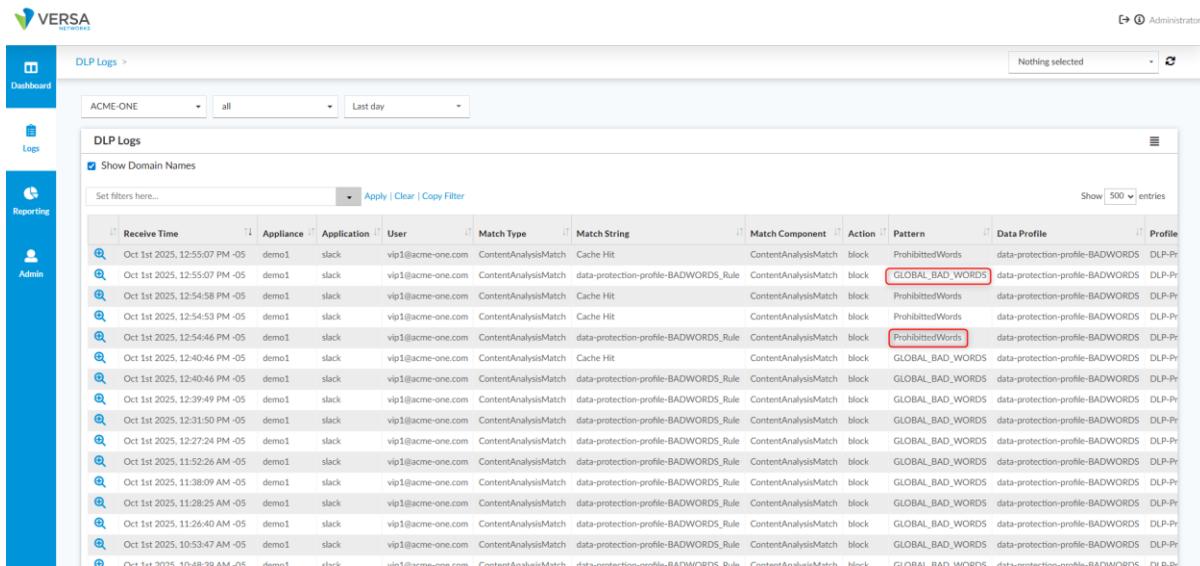
The screenshot shows a Slack workspace for 'ACME'. In the 'Mensajes directos' (Direct Messages) section, a message from 'versa dev' at 12:39 contains the word 'bastard'. A red box highlights this word, and a tooltip 'Bad Word was not sent' appears. A policy violation alert window from 'VERSA' is displayed, stating: 'Policy violation detected by DLP'. It provides details: Application: slack, Action: upload, Activity: blocks, URL: acme-8gp8962.slack.com. The alert includes an 'OK' button and a note: 'This window will auto-close in 22 seconds'.

## Slack test using custom bad word sample.



The screenshot shows a Slack workspace for 'ACME'. In the 'Mensajes directos' (Direct Messages) section, a message from 'versa dev' at 13:18 contains the word 'such word1'. A red box highlights this word, and a tooltip 'Custom word was not sent' appears. A policy violation alert window from 'VERSA' is displayed, stating: 'Policy violation detected by DLP'. It provides details: Application: slack, Action: upload, Activity: blocks, URL: acme-8gp8962.slack.com. The alert includes an 'OK' button and a note: 'This window will auto-close in 22 seconds'. Below the alert, there are buttons for 'Usar canvas en blanco' and 'Usar plantilla'.

## Logs from Analytics



DLP Logs >

ACME-ONE all Last day

Nothing selected

DLP Logs

Show Domain Names

Set filters here... Apply | Clear | Copy Filter

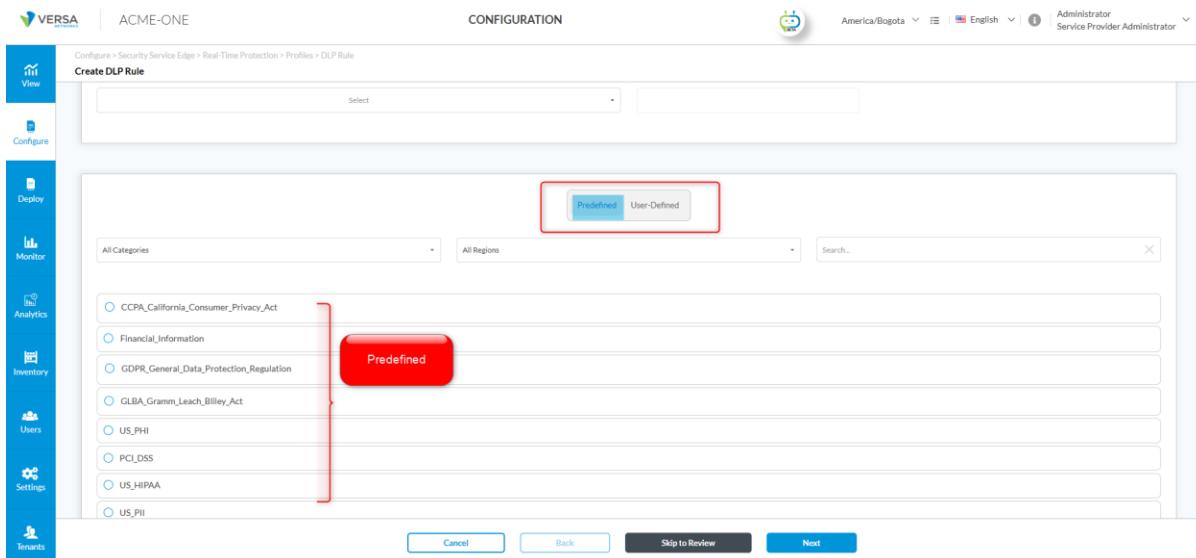
Show 500 entries

| Receive Time                  | Appliance | Application | User              | Match Type           | Match String                          | Match Component      | Action | Pattern          | Data Profile                     | Profile |
|-------------------------------|-----------|-------------|-------------------|----------------------|---------------------------------------|----------------------|--------|------------------|----------------------------------|---------|
| Oct 1st 2025, 12:55:07 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit                             | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:55:07 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | ProhibitedWords  | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:54:58 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit                             | ContentAnalysisMatch | block  | ProhibitedWords  | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:54:53 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit                             | ContentAnalysisMatch | block  | ProhibitedWords  | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:54:46 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | ProhibitedWords  | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:40:46 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | Cache Hit                             | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:40:46 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:39:49 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:31:50 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 12:27:24 PM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 11:52:26 AM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 11:38:09 AM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 11:28:25 AM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 11:26:40 AM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 10:53:47 AM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-protection-profile-BADWORDS_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-protection-profile-BADWORDS | DLP-Pr  |
| Oct 1st 2025, 10:48:09 AM -05 | demo1     | slack       | vip1@acme-one.com | ContentAnalysisMatch | data-numbering-profile-R&N/3R/YK_Rule | ContentAnalysisMatch | block  | GLOBAL_BAD_WORDS | data-numbering-profile-R&N/3R/YK | DLP-Pr  |

## Appendix A – DLP Rule Types

### Content Analysis

Use many prefilters before actual data is scanned and analyzed. It helps to apply DLP policies on 'data in motion' effectively. Additionally, it can leverage either predefined or user-defined Data Protection Profiles, as shown in the image below.



ACME-ONE

CONFIGURATION

Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule

Create DLP Rule

Select

Predefined User-Defined

All Categories All Regions Search...

Predefined

CCPA\_California\_Consumer\_Privacy\_Act  
Financial\_Information  
GDPR\_General\_Data\_Protection\_Regulation  
GLBA\_Gramm\_Leach\_Billey\_Act  
US\_PHI  
PCI\_DSS  
US\_HIPAA  
US\_PII

Cancel Back Skip to Review Next

### File DLP

File-based DLP provides protection based on the configured file attributes, as shown in the image below. Administrators can define rules such as file name (using specific patterns or values), file size (by setting minimum and maximum thresholds with actions applied outside the allowed range), and SHA256 hashes (to explicitly allow or block specific files). When multiple attributes are configured, they are evaluated using AND conditions, meaning that all specified criteria must be met simultaneously for the rule to apply. Alternatively, a single attribute can be used on its own—for example, configuring only the file size range, or only the SHA256 hash—by leaving the other fields blank. This flexibility allows organizations to fine-tune protection by combining general attributes with precise identifiers, or by focusing on a single attribute when needed.

## Optical Character Recognition (OCR)

OCR technology converts images into text and applies DLP policies on the extracted text data. It requires connectivity to the Versa OCR Cloud Instance, which should be reviewed with the support team. Similar to Content Analysis, it can leverage either predefined or user-defined Data Protection Profiles, as shown in the image below.

The screenshot shows the Versa Configuration interface with the following details:

- Header:** ACME-ONE, CONFIGURATION, America/Bogota, English, Administrator, Service Provider Administrator.
- Left Sidebar:** View, Configure, Deploy, Monitor, Analytics, Inventory, Users, Settings, Tenants.
- Current Path:** Configure > Security Service Edge > Real-Time Protection > Profiles > DLP Rule.
- Process Step:** Create DLP Rule, Step 1: OCR: Data Protection Methods (highlighted with a red circle).
- Content:** Optical Character Recognition (OCR) Data Protection screen. It shows tabs for 'Predefined' (highlighted with a red box) and 'User-Defined'. A list of categories is shown, each with an 'Unselected' radio button:
  - CCPA\_California\_Consumer\_Privacy\_Act
  - Financial\_Information
  - GDPR\_General\_Data\_Protection\_Regulation
  - GLBA\_Gramm\_Leach\_Billey\_Act
- Buttons:** Cancel, Back, Skip to Review, Next.

## Exact Data Match (EDM)

Versa's Data Loss Prevention (DLP) Exact Data Match (EDM) is an advanced security feature that detects and prevents data breaches by matching specific, sensitive data records against predefined datasets. Unlike traditional pattern-based detection, EDM allows organizations to upload structured data (such as customer records, financial information, or employee details) into a secure, hashed database. Versa DLP then scans network traffic for exact matches to these datasets, ensuring highly accurate data protection with minimal false positives.

A financial institution needs to prevent unauthorized transmission of customer account numbers and Social Security Numbers (SSNs). By using Versa's DLP EDM, they upload a securely hashed database of customer records. If an employee attempts to send an email or upload a file containing an exact match to this data, the system detects the violation and enforces security policies, such as blocking the transmission, alerting administrators, or requiring additional authorization.

This ensures compliance with regulations (e.g., PCI DSS, GDPR, HIPAA) and protects sensitive business and customer information from leaks or theft.

## Document Fingerprinting

It converts a standard form into a sensitive information type, which you can use to define transport rules and DLP policies.

## Appendix B – DLP Rule Actions

Allow: The content transfer is permitted without restriction. No enforcement action is taken.

Alert: The action is allowed, but an alert/notification is generated for visibility, monitoring, or further investigation.

Block: The content transfer is prevented. The user may receive a notification that the action was blocked depending on policy configuration.

Reject: The content transfer is actively denied, and the session is forcefully terminated. The browser typically shows a “connection reset” or similar error, and at the same time the endpoint client displays a popup notifying the user of the DLP violation.

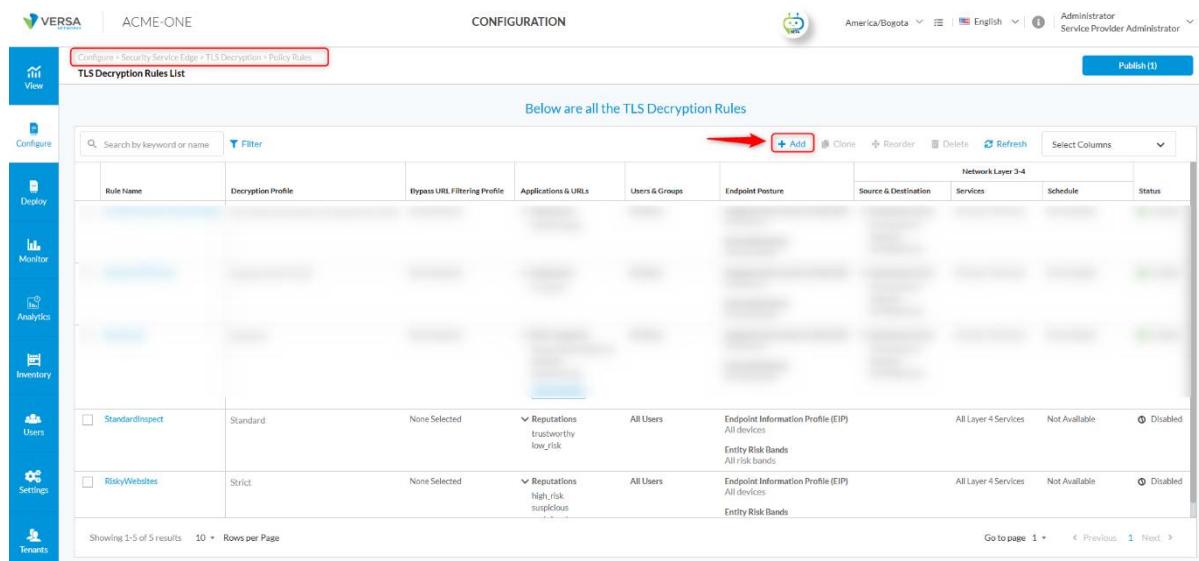
Quarantine: API-DP still in roadmap for 2025

Encrypt: API-DP still in roadmap for 2025

Legal Hold: API-DP still in roadmap for 2025

## Appendix C – TLS Decryption Rule Configuration

Navigate to **Configure > Security Service Edge > TLS Decryption > Policy Rules**. Click **+ Add**, as shown in the image below.



The screenshot shows the VERSA Configuration interface for the 'TLS Decryption Rules List'. The top navigation bar includes 'ACME-ONE', 'CONFIGURATION', 'Administrator', and 'Service Provider Administrator'. The left sidebar has icons for 'View', 'Configure', 'Deploy', 'Monitor', 'Analytics', 'Inventory', 'Users', 'Settings', and 'Tenants'. The main content area has a header 'TLS Decryption Rules List' with a search bar and filter options. A red arrow points to the '+ Add' button in the top right of the header. Below the header is a table with columns: Rule Name, Decryption Profile, Bypass URL Filtering Profile, Applications & URLs, Users & Groups, Endpoint Posture, Network Layer 3-4, Source & Destination, Services, Schedule, and Status. Two rows are visible: 'StandardInspect' (Standard profile, None Selected, Reputations: trustworthy low\_risk, All Users, Endpoint Information Profile (EIP), All Layer 4 Services, Not Available, Disabled) and 'RiskyWebsites' (Strict profile, None Selected, Reputations: high\_risk suspicious, All Users, Endpoint Information Profile (EIP), All Layer 4 Services, Not Available, Disabled). At the bottom, there are buttons for 'Go to page 1 > < Previous 1 Next >'.

Then complete the 6 steps shown in the following image.

**Decryption Enforcement:** Select the green checkmark (Decrypt traffic and inspect the server certificate) and under Use the following decryption profile, select Standard, then click Next.

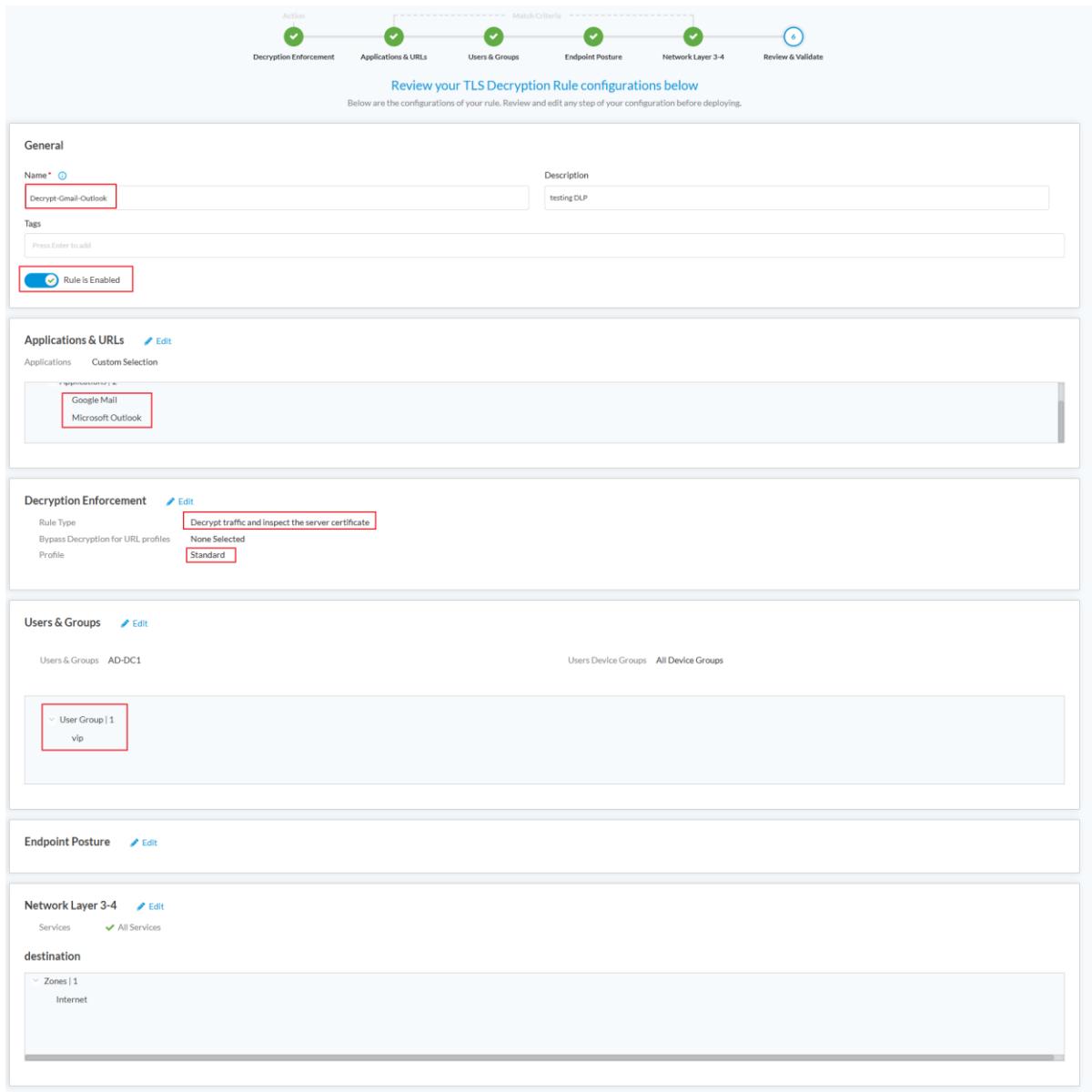
**Applications & URLs:** Click the Applications tab and in the search field add Gmail and Outlook, then click Next.

**Users & Groups:** Select your test group, then click Next. In our case, it can be the VIP group coming from our LDAP-AD.

**Endpoint Posture:** Leave the default values and click Next.

**Network Layer 3-4:** You can filter by services like **http**, **https**, **dns**, **icmp**, etc. However, leave the default values and click Next.

**Review & Validate:** Review the configuration (see image below), click **Save**, and select **add this rule at the top of the rule list**.



Review your TLS Decryption Rule configurations below

Below are the configurations of your rule. Review and edit any step of your configuration before deploying.

**General**

Name \*  Description

Tags

Rule is Enabled

**Applications & URLs** [Edit](#)

Applications Custom Selection

Google Mail Microsoft Outlook

**Decryption Enforcement** [Edit](#)

Rule Type  Bypass Decryption for URL profiles  Profile

**Users & Groups** [Edit](#)

Users & Groups AD-DC1 Users Device Groups All Device Groups

User Group | 1  vip

**Endpoint Posture** [Edit](#)

**Network Layer 3-4** [Edit](#)

Services  All Services

destination

Zones | 1 Internet

## Appendix D – Incident\_Report\_Form\_Filled.docx.

This section lists the sample data used in the testing of use case 2

### Confidential Employee Incident Report Form

This form is intended for the reporting of workplace incidents and policy violations. All submissions are confidential and will be reviewed by the HR Compliance Department. Please complete all required sections. Additional evidence or extended narratives should be attached as separate documents. Do not exceed the provided space in each section.

### Section 1 – Employee Information

Employee Name: John Doe

Department: IT Security

Position: Senior Security Analyst

Date of Incident: 09 / 12 / 2025

## Section 2 – Type of Violation

Please check one or more categories that best describe the violation (mandatory selection):

Confidentiality Breach  
 Code of Conduct  
 Workplace Harassment  
 Safety Violation  
 Other (please specify) \_\_\_\_\_

## Section 3 – Description of Violation

Provide a concise summary of the violation in 3–4 sentences maximum. If additional details are needed, attach a supporting document.

Description:

On September 12th, 2025, an employee was observed uploading a confidential HR policy document to a personal Dropbox account. The file contained sensitive disciplinary procedures. The incident was detected by the DLP monitoring system and reported for investigation.

## Section 4 – Witnesses

List up to 2 witnesses with name and department. Additional names must be attached separately.

1. Jane Smith – HR Department
2. Michael Brown – IT Department

## Section 5 – Co-Workers Involved

List any co-workers directly involved in the incident. Specify their role or relation to the case.

1. Alice Johnson – Co-worker who shared the document link internally.
2. N/A

## Section 6 – Acknowledgement

By signing this form, the reporting employee confirms that the information provided is accurate to the best of their knowledge. The HR Compliance Department will review the case and take the appropriate action as outlined in company policy.

Employee Signature: John Doe Date: 09 / 12 / 2025

Confidential – Internal Use Only

This document is property of ACME Corporation. Unauthorized distribution is strictly prohibited. All reports will be handled according to HR and Compliance policies in effect as of the date of submission.

## About Versa

Versa, the global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the [VersaONE Universal SASE Platform](#) delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit <https://www.versa-networks.com> and follow Versa on [LinkedIn](#) and X (Twitter) [@versanetworks](#).