Data Protection & Data Privacy

WHITEPAPER

Table of Contents

Overview Zscaler Data Protection

The adoption of SaaS and public cloud has rendered data widely distributed and difficult, if not impossible, to secure with legacy protection appliances. As such, it is easy for both careless users and malicious actors to expose enterprise cloud data.

Zscaler Data Protection follows users and the apps they access—protecting anywhere and anytime against data loss. The Zero Trust Exchange™ inspects inline and cloud data to ensure all data everywhere is secure, while delivering a dramatically streamlined approach to protection and operations.

DISCLAIMER: The content of this document is for informational purposes only and doesn't represent any commercial offer nor provides any guarantee of correctness or completeness and does not represent any legal advice or guidance.

Zscaler Data Protection provides protection in the following areas:

Prevent inline data loss to Web and unmanaged devices

When users access the internet and its risky destinations, it is a threat to enterprise data. Legacy appliances can't follow users off-network or secure their web traffic. Zscaler is a cloud-native platform that scales to inspect all traffic, everywhere. A single DLP policy protects data across web, SaaS and private apps, along with advanced classification like EDM, IDM and OCR. Leverage browser isolation to safely stream data as pixels to unmanaged BYOD.

Secure SaaS data with CASB

Securing data at rest in SaaS apps is critical for security – it only takes two clicks to share data with an unauthorized user through apps like Microsoft OneDrive. Zscaler's integrated, multimode CASB secures SaaS apps without the cost and complexity of a point product. Inline functionality delivers full shadow IT discovery and control. Out-of-band DLP and ATP remediate risky file sharing and malware at rest in the cloud, respectively.

Secure endpoint data

Data in use on endpoints can be easily lost across multiple channels. From removable media, to printing to network shares, users often expose sensitive data to unnecessary risks, or maliciously exfiltrate data when leaving for another company. With Endpoint DLP, organizations can enforce consistent DLP policy across endpoints to ensure sensitive data remains protected. Control USB drives, bluetooth, printing or network shares with always-on DLP protection.

Email DLP via Smarthost

Email is one of the most common channels for data loss.Users can easily forward sensitive data out of the organization or to personal email accounts. With Zscaler Email DLP, security administrators get a powerfully simple way to insert DLP inspection into their email architecture.

Implemented as a Smarthost, Zscaler can be added as the next hop after your email service via SMTP relay. Enforce DLP inspection and actions like blocking, encrypt and quarantine, all with minimal changes to your Email or MTA settings.

Unified SaaS Security (SSPM, SaaS Supply Chain, CASB)

Many cloud breaches are caused by dangerous misconfigurations, access or third-party apps connected into SaaS Platforms. Understanding and governing your SaaS posture is an important step to secure the vast amounts of sensitive data in these clouds With Zscaler's Unified SaaS Security, organizations get a unified approach to scan and secure SaaS Platforms like Office 365 or Google. Get in-depth visibility into dangerous misconfigurations and app integrations, with auto remediation, guidance, and control over revoking risky connected apps.

Data Security Posture Management (DSPM)

Sensitive data stored in public clouds like AWS and Azure can be very dynamic. From excess privileges and vulnerabilities to shadow data, IT teams need a better way to discover, catalog and secure public cloud data. Zscaler's DSPM quickly discovers sensitive data, understands risk, and controls access and posture. Best of all, Zscaler's integrated DSPM leverages the same DLP engine as all other channels (Endpoint, Network, SaaS), so alerting is consistent, no matter where your data moves to.

Architecture Components

The Zscaler Digital Experience architecture is built to scale with the monitoring requirements of our clients. The ZIA solution architecture is composed of the following blocks:

Zscaler Client Connector

Now with digital experience monitoring software, new functionality designed to be orthogonal to the forwarding data plane, the Zscaler Client Connector provides device metrics at negligible additional CPU consumption. The Zscaler Client Connector exchanges information with the telemetry and policy gateway to receive configuration from ZIA and reports metrics to the cloud service for consumption. The service also provides latitude and longitude coordinates for geolocation if the operating system location services are enabled.

Zero Trust Exchange

The ZIA cloud connects and authenticates to ZIA/ZPA clouds to retrieve users, departments, and locations and to the Zscaler Client Connector Portal for integrated management of Zscaler Client Connector and ZIA definitions. User-definition infrastructure and integration for ZIA standalone deployments without ZIA/ZPA services is also included.

ZIA User Interface

With administrator access for configuration, reporting, alerting and analysis, the ZIA user interface integrates with ZIA/ZPA management to provide a centralized configuration. ZIA provides very granular role-based access control with SSO in the Zscaler Client Connector Portal for administrators.

Incident Receiver

The Zscaler Incident Receiver is a tool that allows you to receive information about DLP policy violations securely. It can run on an EC2 instance on Amazon Web Services (AWS), on an Azure VM, or on-premises. The Zscaler service sends information about policy violations via ICAP to the Incident Receiver. This tool sends the policy-violating content and a JSON file containing the metadata for the inline web and CASB DLP policy scan (e.g., the URL, Collaborators, DLP dictionaries, DLP engines, etc.)

Workflow Automation

Workflow Automation is an application that enables governance admins to manage and resolve the different Data Protection incidents and ZIA alerts that occur in their organization. Workflow Automation integrates with Zscaler Internet Access (ZIA) to capture the Data Protection incidents generated from the DLP policies defined in ZIA. It also integrates with ZIA to generate enriched tickets for different events that are triggered when the predefined threshold is reached for the alert rules defined in ZIA.

Information Accessed by Zscaler DLP

Generally, the following areas are touched by Zscaler DLP:

ENDPOINT

Zscaler Endpoint DLP operates on the endpoint, classifies files on the endpoint based on a policy, received from the cloud and applies local enforcement, while reporting data is submitted to the Zscaler Cloud.

NETWORK

Zscaler DLP scans data in motion in uploads or downloads and applies detection for sensitive information therein. Reporting and enforcement happen as part of the Zero Trust Exchange in the cloud.

CLOUD

Zscaler DLP scans data inside SaaS apps over their API and determines their sharing level and enforces a collaboration policy. For IaaS and PaaS, Zscaler performs and in-tenant scan and detects sensitive data and permissions to access that data. Reporting and scanning happen as part of the Zero Trust Exchange and enforcement happens over an API inside the 3rd party SaaS, IaaS or PaaS.

EMAIL

Zscaler Email DLP scans emails in transit using redirection from the mail service, Exchange or Gmail. The scanning happens in the Zscaler service while policy enforcement happens in the mail service.

Zscaler can integrate, based on configuration, with 3rd party solutions such as Slack, Teams, Servicenow, Jira or email services for alerting, ticket creation or end user interaction.

Personally Identifiable Information

Zscaler DLP will use the same PII information as ZIA, which is obtained from a customer's IDP. These attributes include, but not limited to:

- Username
- Group
- Department
- IP addresses
- Geo locations

Additionally, other data that is synced from the IDP based on the customer's configuration can be present.

In addition, for cloud services will report to Zscaler:

- Ownership information for data in the form of an email address, which should match the username as obtained from the corporate IDP.
- 3rd party usernames, when collaborators from outside the company are invited to access data in a company's SaaS application.
- Access to 3rd party SaaS applications.

In addition, on the endpoint, Zscaler endpoint DLP will detect and report, but not limited to:

- Ip addresses
- Device names
- Printer names
- Network share names
- USB device IDs
- File Path Names
- Process names

In addition, in Email DLP, Zscaler will detect and report:

- Recipient email addresses
- Sender email addresses

Controlling Access

ZIA offers multiple layers of 1) collecting information and 2) giving access to the collected information.

Define What Information From Whom to Collect

The process of collecting information is to first enable ZIA in ZCC and then configure Application and Probes. To enable ZIA, there is the option to either enable it for the tenant (all users) or for selected user groups. Additionally, the option exists to be selective on data that is collected. Details will follow in the next chapters.

After ZIA is enabled, Applications and Probes are configured. For each probe, it can be defined who the relevant users or user groups, etc. are for whom the probes shall be running.

Beyond the probes, it can be defined if Device Inventory is collected.

Controlled Access to the Collected Information

After the decision and configuration is made for collecting information, the access to that information can be restricted by Role Based Access Control (RBAC). Additionally, obfuscation of certain data points can be enabled.

Define What Information From Whom to Collect

Enabling and Disabling DLP

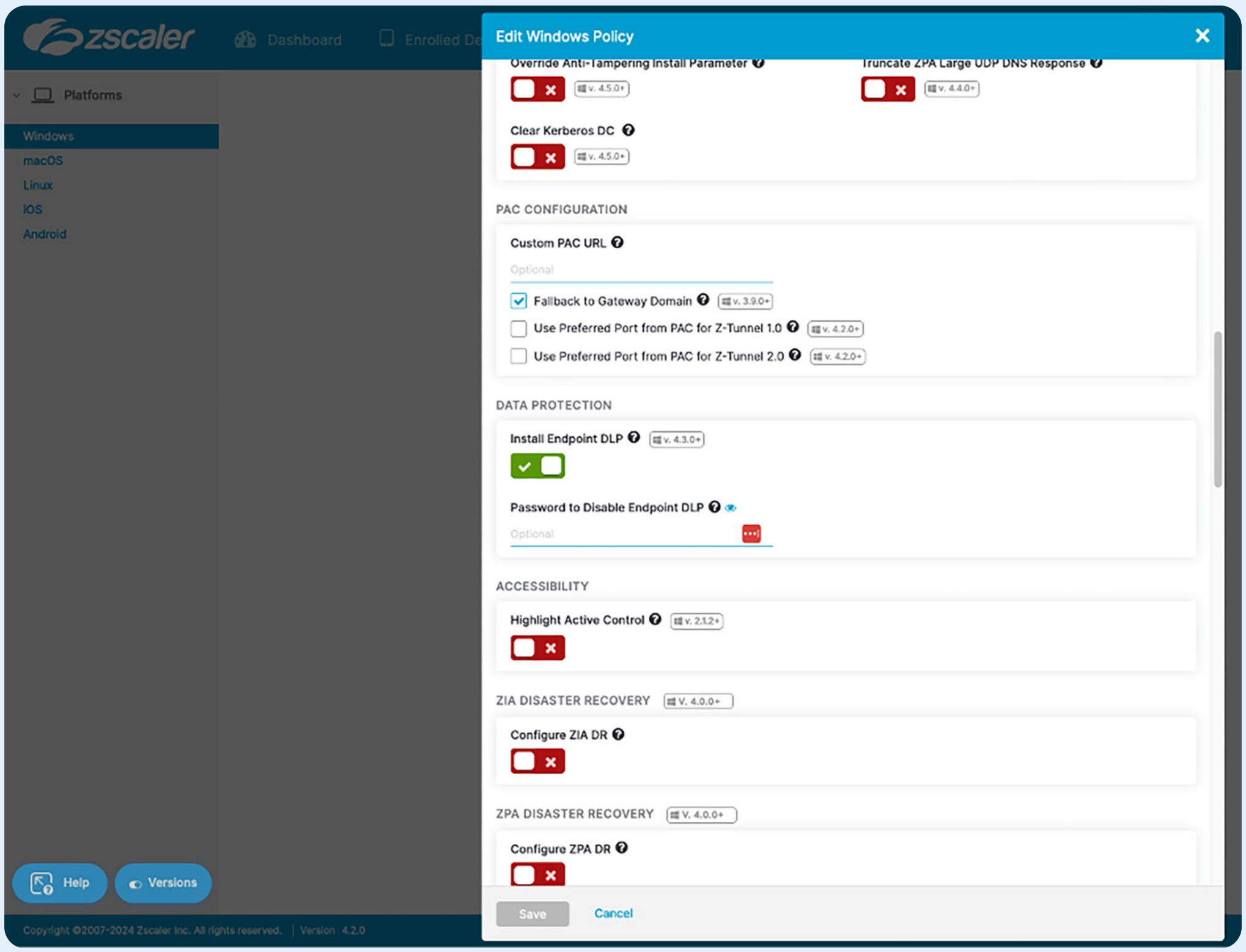
All features depend on purchased licenses and are not generally available for all customers.

Zscaler inline DLP requires DLP policies to be set in the UI. Some policies are default on and can be disabled during the configuration process.

Some DLP reporting capabilities are always on and cannot be disabled.

For Email, SaaS, IaaS and PaaS specific integrations need to be set up for Zscaler to apply DLP scanning to data in thee applications. Additionally, respective policies need to be created before scanning takes place.

Endpoint DLP needs to be enabled specifically in an App Profile in the Client Connector Portal and is only made available to clients using this specific profile.



Collection of Data from DLP Scanning

During scanning files for DLP violations, based on a customer's configuration, using predefined or custom dictionaries, Zscaler will analyze the content of files. This content analysis process is similar to analyzing files for malware or detecting a media type from which files also need to be handled to detect content, embedded information, etc. inside a file.

Zscaler DLP will extract full text from a document and match that against it's DLP engines to detect sensitive content and protect that according to the policy. Protection can mean different things based on vector, i.e.

- Block the upload of a file to a website
- Prevent sharing a sensitive file in OneDrive
- Close access to a data base in AWS

During the scanning process, additional data is collected and made available for analysis.

Zscaler will at no point store sensitive files or the content thereof in the Zscaler cloud. An exception applies to the GenAI reporting product, which, after consent, will store the prompts for all users.

Generally, the product documentation, as available on help.zscaler.com, takes precedence over any information in this document, as the help is the only representative source of information, while this document might become outdated while the product progresses.

WEB ACCESS

Additional information captured in the web access logs, **help.zscaler.com/zia/web-insights-logs-columns:**

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for the transactions using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact transaction.

DLP MD5: The MD5 hash for the file that triggered the DLP rule. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing the MD5 hash of the file is sent to your auditors. Use it as a filter to locate the exact transaction.

DLP Severity: The severity of the triggered DLP rule violation (i.e., High, Medium, Low, or Information). These severities are assigned to the DLP rules at the time of DLP rule configuration.

Document Type: The type of document uploaded or downloaded during the transaction.

SAAS SECURITY

When scanning data inside SaaS applications, additional data will be captures in the SaaS Security Insight Logs.

Each application category has its own set of columns.
help.zscaler.com/unified/about-saas-security-insights-logs

Collaboration Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., Slack).

Application Category: The type of application category.

Channel Name: The name of the Slack, Webex Teams, or Microsoft Teams channel.

Collaboration Scope: The collaboration scope and permissions for SaaS application tenant files.

Component: The type of component (e.g., Message, Email).

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

External Recipients: The email recipients outside your organization.

File ID: The ID of a file. For example, if a file was scanned multiple times, an admin can use the file ID to view the scan trail.

File MD5: The MD5 hash for the file.

File Size: The size of the file.

File Type: The type of file that was either uploaded or downloaded.

Internal Recipients: The recipients within your organization.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Message ID: The email message identifier. Every email message has a unique ID. An Exchange or Gmail administrator can log in to their admin portals and search and pull a specific message with this ID if needed.

Number of External Recipients: The number of recipients outside your organization.

Number of Internal Recipients: The number of recipients within your organization.

Policy Type: The type of policy that took action during the record.

Rule Name: The name of the rule that triggered the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

SHA: The secure hash algorithm (SHA).

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Sender Name: The name of the message sender.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

Shared Channel Domain: The shared channel domain in Slack, Webex Teams, or Microsoft Teams.

Tenant: The sanctioned SaaS application that is integrated with the Zscaler service.

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

User: The email address of the user who performed the record. If an internet gateway location is specified and authentication is not required, this field displays the name of the gateway location. You can sort and search through this column.

CRM Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., Salesforce and Dynamic 365).

Application Category: The type of application category.

Collaboration Scope: The collaboration scope and permissions for SaaS application tenant files.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

External Collaborators: The collaborators outside your organization.

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

File MD5: The MD5 hash for the file.

File Message ID

File Message Modification Time

File Name: The name of the suspicious file detected by SaaS Security API policy.

File Size: The size of the file.

File Source Location: The source location of the files containing sensitive data that were detected by the SaaS Security API DLP or Malware Detection policy.

File Type: The type of file that was either uploaded or downloaded.

Internal Collaborators: The internal collaborators within your organization.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Number of External Collaborators: The number of collaborators outside your organization.

Number of Internal Collaborators: The number of collaborators within your organization.

Object Name: The name of an object (e.g., you might have the object type Opportunity with an object name of “Pepsi”.).

Object Type: The type of object (e.g., budget request, campaign, opportunity).

Policy Type: The type of policy that took action during the record.

Public URL: The public URLs used to access a shared file.

Rule Name: The name of the rule that triggered the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

SHA: The secure hash algorithm (SHA).

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

Shared Channel Domain: The shared channel domain in Salesforce or Dynamic 365.

Tenant: The sanctioned SaaS application that is integrated with the Zscaler service.

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

User: The email address of the user who performed the record. If an internet gateway location is specified and authentication is not required, this field displays the name of the gateway location. You can sort and search through this column.

Email Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., Exchange, Gmail, etc.).

Application Category: The type of application category.

Attachments: The attachments within the email message.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

Email Direction: The direction of the email (Inbound or Outbound).

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

External Recipients: The email recipients outside your organization.

Internal Recipients: The email recipients within your organization.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Mail Sent Time: The time the email was sent.

Message ID: The email message identifier. Every email message has a unique ID. An Exchange or Gmail administrator can log in to their admin portals and search and pull a specific message with this ID if needed.

Message Size: The size of the email message.

Number of External Recipients: The number of recipients outside your organization.

Number of Internal Recipients: The number of recipients within your organization.

Owner Name: The owner of the mailbox where the questionable email is located. It can be a sender (DLP) or a recipient (Malware).

Policy Type: The type of policy that took action during the record.

Rule Name: The name of the rule that triggered the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Sender Name: The name of the email sender.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

Shared Channel Domain: The shared channel domain.

Tenant: The sanctioned SaaS application that is integrated with the Zscaler service.

Thread Name: The name of the email thread.

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

File Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., Box, Microsoft OneDrive, SharePoint, etc.).

Application Category: The type of application category.

Collaboration Scope: The collaboration scope and permissions for SaaS application tenant files.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

External Collaborators: The collaborators outside your organization.

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

File ID: The ID of a file. For example, if a file was scanned multiple times, an admin can use the file ID to view the scan trail.

File MD5: The MD5 hash for the file.

File Modification Time: The date and time when a SaaS Security API DLP policy modified the collaboration scope for SaaS application tenant files.

File Name: The name of the suspicious file detected by SaaS Security API policy.

File Size: The size of the file.

File Source Location: The source location of the files containing sensitive data that were detected by the SaaS Security API DLP or Malware Detection policy.

File Type: The type of file that was either uploaded or downloaded.

Internal Collaborators: The internal collaborators within your organization.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Number of External Collaborators: The number of collaborators outside your organization.

Number of Internal Collaborators: The number of collaborators within your organization.

Policy Type: The type of policy that took action during the record.

Public URL: The public URLs used to access a shared file.

Rule Name: The name of the rule that triggered the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

SHA: The secure hash algorithm (SHA).

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

Shared Channel Domain: The shared channel domain.

Tenant: The sanctioned SaaS application that is integrated with the Zscaler service.

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

User: The email address of the user who performed the record. If an internet gateway location is specified and authentication is not required, this field displays the name of the gateway location. You can sort and search through this column.

ITSM Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., ServiceNow).

Application Category: The type of application category.

Collaboration Scope: The collaboration scope and permissions for SaaS application tenant files.

Component: The type of component (e.g., Message, Email).

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

External Collaborators: The collaborators outside your organization.

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

File MD5: The MD5 hash for the file.

File Message: The message of the file.

File Message Modification Time: The date and time when a file message was modified.

File Name: The name of the suspicious file detected by SaaS Security API policy.

File Source Location: The source location of the files containing sensitive data that were detected by the SaaS Security API DLP or Malware Detection policy.

Internal Collaborators: The internal collaborators within your organization.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Number of External Collaborators: The number of collaborators outside your organization.

Number of Internal Collaborators: The number of collaborators within your organization.

Object Name: The name of an object (e.g., you might have the object type Opportunity with an object name of “Pepsi”.)

Object Type: The type of object (e.g., budget request, campaign, opportunity).

Policy Type: The type of policy that took action during the record.

Rule Name: The name of the rule that triggered the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

SHA: The secure hash algorithm (SHA).

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

Shared Channel Domain: The shared channel domain.

Tenant: The sanctioned SaaS application that is integrated with the Zscaler service.

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

User: The email address of the user who performed the record. If an internet gateway location is specified and authentication is not required, this field displays the name of the gateway location. You can sort and search through this column.

Public Cloud Storage Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., Amazon S3).

Application Category: The type of application category.

Bucket Name: The name of the bucket.

Collaboration Scope: The collaboration scope and permissions for SaaS application tenant files.

Collaborators: The collaborators of the files.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for the records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

File ID: The ID of a file. For example, if a file was scanned multiple times, an admin can use the file ID to view the scan trail.

File MD5: The MD5 hash for the file.

File Modification Time: The date and time for when a SaaS Security API DLP policy modified the collaboration scope for SaaS application tenant files.

File Name: The name of the suspicious file detected by SaaS Security API policy.

File Size: The size of the file.

File Source Location: The source location of the files containing sensitive data that were detected by the SaaS Security API DLP or Malware Detection policy.

File Type: The type of file that was either uploaded or downloaded.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Number of Collaborators: The number of collaborators for the file.

Object Type: The type of object.

Policy Type: The type of the policy that took action during the record.

Public URL: The public URLs used to access a shared file.

Rule Name: The name of the rule that triggered on the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

SHA: The secure hash algorithm (SHA).

Tenant: The sanctioned SaaS application that is integrated with the Zscaler service.

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

User: The email address of the user who performed the record. If an internet gateway location was specified and authentication is not required, this field displays the name of the gateway location. You can sort and search through this column.

Repository Columns

Action: The SaaS Security API DLP policy rule action.

- No SaaS Security API DLP / Malware policy rule action is performed if a SaaS application detects the malware. If SaaS application detects the malware, the Zscaler service does not run its anti-virus.

Advanced Threat Category: If the service detected a threat in the record, it displays the virus or spyware type, if applicable.

Application: The type of sanctioned SaaS application (e.g., GitHub and GitLab).

Application Category: The type of application category.

Collaboration Scope: The collaboration scope and permissions for SaaS application tenant files.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a Data Loss Prevention (DLP) engine.

DLP Identifier: Used to search for records using this DLP identifier. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors. Use it as a filter to locate the exact record.

Data Center: The name of the data center.

Department: The department to which the user belongs. As with the User field, if authentication is not required and the traffic comes from a location specified in the service, this field displays the name of the gateway location. You can sort and search through this column.

Document Type: The type of document uploaded or downloaded during the transaction.

Download Time: The download time of the suspicious file detected by SaaS Security API.

External Collaborators: The collaborators outside your organization.

Non-Provisioned Owner: The file owners (inside or outside your organization) that are not provisioned to the ZIA services.

- When a non-provisioned file owner within your organization is later provisioned to the ZIA services, the service begins to log the file owner under the User column.

File ID: The ID of a file. For example, if a file was scanned multiple times, an admin can use the file ID to view the scan trail.

File MD5: The MD5 hash for the file.

File Name: The name of the suspicious file detected by SaaS Security API policy.

File Size: The size of the file.

File Source Location: The source location of the files containing sensitive data that were detected by the SaaS Security API DLP or Malware Detection policy.

Last Modified Time: The last time (date and time) the file was modified. You can sort by ascending or descending order.

Logged Time: The incident logged time, which is when we perform a scan and evaluate policies and log results. You can sort by ascending or descending order.

Number of External Collaborators: The number of collaborators outside your organization.

Policy Type: The type of policy that took action during the record.

Project Name: The name of the project.

Repository Name: The name of the repository.

Rule Name: The name of the rule that triggered the session or aggregated sessions.

Run ID: A run is when a scan is stopped and started. Every run is identified and tracked with a run ID.

SHA: The secure hash algorithm (SHA).

Scan ID: Every scan that is defined in the Historic Scan Configuration has a unique identifier associated with it.

Scan Time: The amount of time, in milliseconds, the SaaS Security API policy took to scan content within the tenant.

Severity: The severity level of the incidents detected by the SaaS Security API DLP policy.

Shared Channel Name

Threat Name: If the service detected a threat in the record, it displays the name of the threat. Click to read more information about the threat in the Zscaler Threat Library.

Threat Super Category: If the service detected a threat in the record, it displays the Virus and Spyware super category, if applicable.

User: The email address of the user who performed the record. If an internet gateway location is specified and authentication is not required, this field displays the name of the gateway location. You can sort and search through this column.

ENDPOINT DLP (Source)

Action Taken: The action taken on the user activity per the configured rule.

Activity Type: The type of activity performed by the user (e.g., copy, print, upload, download, etc.).

Channel: The channel through which the activity takes place.

Confirm Action: The action taken by the user when the user is prompted with a confirmation dialog box for the activity, if applicable.

Confirm Justification: The justification provided by the user for the activity.

Data Center: The data center associated with the activity.

Department: The department to which the user belongs. You can sort and search this column.

Destination Type: The destination type for the item associated with the activity (e.g., application, local drive, printer, etc.).

Destination Name: The name of the destination for the item associated with the activity.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a DLP engine.

DLP Identifier: A unique identifier used to search for the activity. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors.

Document Type: The type of document uploaded or downloaded during the activity.

Event Time: The date and time of the activity. You can sort this column.

File Destination Location: The source location of the item for the activity.

File MD5: The MD5 hash for the file that triggered the DLP rule. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing the MD5 hash of the file is sent to your auditors.

File SHA256: Displays the hash of identical files.

File Size: The size of the file associated with the activity.

File Source Location: The source location of the item for the activity.

File Type Category: The category of the file associated with the activity.

File Type: The file type associated with the activity.

Item Name: The name of the item associated with the activity.

Item Type: The type of item associated with the activity (e.g., file, email, email attachment, etc.).

Logged Time: The date and time the activity was logged.

Other Rules: The name of any other policy rule that was also triggered by the user activity.

Record Type: The type of activity (i.e., DLP Incident or Sensitive Activity).

Rule Name: The name of the Endpoint DLP rule triggered by the activity performed by the user.

Scan Time: The total time taken to perform the scan on the activity.

Severity: The severity of the activity as per the triggered rule (e.g., Information, Medium, etc.).

Source Name: The name of the source for the item associated with the activity.

Source Type: The source type for the item associated with the activity (e.g., application, local drive, web, etc.).

User: The email address of the user who performed the activity. You can sort and search this column.

ZDP Mode: The Endpoint DLP mode for the activity. When a user enables the exemption mode from the Zscaler Client Connector to bypass the Endpoint DLP policy rules to successfully perform an activity (e.g., copy a file), the ZDP Mode column displays Exemption Mode. When the exemption mode is disabled, the column displays Block Mode.

EMAIL DLP (Source)

Application: The name of the email application.

User: The user who sent the email and is provisioned to ZIA.

Triggered Recipients: The users who received email and a policy action was taken.

Other Recipients: The users who received emails, but no policy was triggered.

Rule Name: The name of the DLP rule that triggered by the activity performed by the user.

Tenant: The name of the email tenant.

Subject: The subject of the email.

DLP Identifier: A unique identifier used to search for the activity. Whenever a DLP rule is hit, and the appropriate alert is configured, an email containing this ID is sent to your auditors.

DLP Dictionaries: Indicates if data leakage was detected by a DLP dictionary.

DLP Engine: Indicates if data leakage was detected by a DLP engine.

Severity: The severity of the activity as per the triggered rule (e.g., Information, Medium, etc.).

Action Taken: The action taken on the user activity per the configured rule.

File Name: The name of the file that was attached with the email. You can click the file name to view attachments that have details such as file name, document type, file size, file type category, and MD5.

Mail Sent Time: The date and time when the email was sent.

Scan Time: The total time taken to perform the scan on the activity in milliseconds..

Department: The department to which the user belongs.

Message ID: The unique email message identifier. Click this field to view details of the recipient, action, rule name, and severity.

External User: The user who sent the email but is not provisioned to ZIA.

Record Type: The event type that was triggered.

INCIDENTS

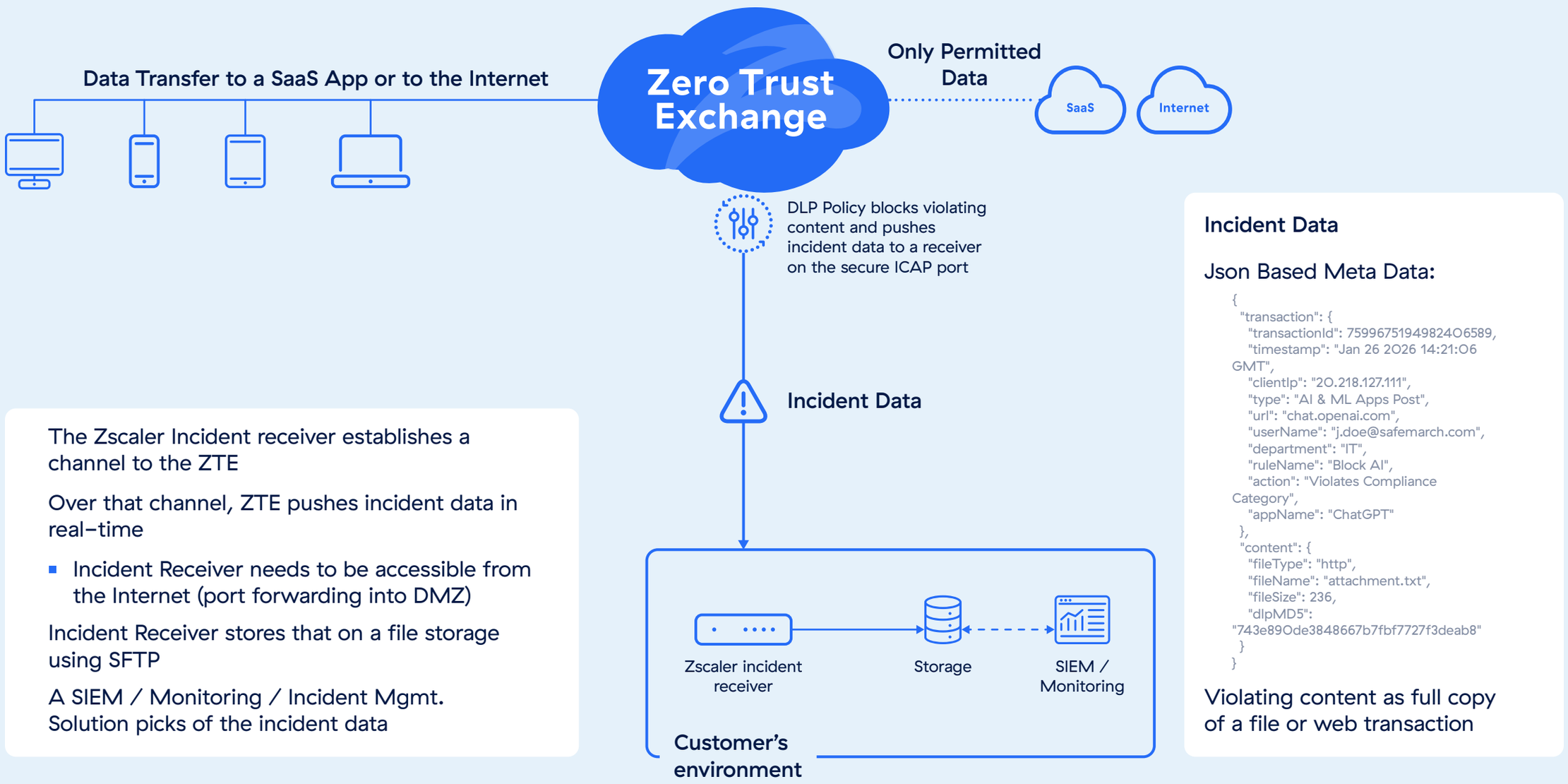
As mentioned above, Zscaler will not store any files or content of file as part of its ecosystem. However, to make violating files available to a DLP investigator or analyst, violating files can be sent via emails, depending on policy.

As primary option, Zscaler offers the creation of incidents within customer's premises by leveraging IaaS to store incidents using the cloud-to-cloud incident forwarding. As part of that flow Zscaler will forward incident data to a customer's public cloud storage, which enables Workflows Automation to pick up that data for incident management. Workflow Automation will be explained in the next section.

Additionally, Zscaler introduced the incident receiver, which allows Zscaler to hand back violating files and information about the violation in real-time. This is best suited if incident data needs to retained purely on premise and feed to tools other than Workflow Automation.

In both scenarios, in addition to transactional information, these will include details from inside the file and display matching content and include the violating file itself. This enabled the company to follow up on a DLP violation and investigate the occurrence. As this data is always stored within a customer's environment, Zscaler is not responsible for managing access to this information and a customer can establish their own RBAC to that data.

Zscaler Incident Receiver



The Zscaler Incident receiver establishes a channel to the ZTE

Over that channel, ZTE pushes incident data in real-time

- Incident Receiver needs to be accessible from the Internet (port forwarding into DMZ)

Incident Receiver stores that on a file storage using SFTP

A SIEM / Monitoring / Incident Mgmt. Solution picks of the incident data

More details: help.zscaler.com/zia/about-zscaler-incident-receiver

WORKFLOW AUTOMATION

Workflow Automation is a solution built on top of the previously mentioned concept of the incident receiver. As cloud service it will work on the data stored in the possession of a customer. For that purpose, the customer will need to install an incident receiver in their public cloud and make data available to Zscaler's Workflow Automation service using data or event pipelines in that public cloud environment. Zscaler then will visualize that data in Workflow automation and will buffer the transactional data of the incidents, which is not different than the data in the logs. Every sensitive information, such as files and violating content, will remain in custody of the customer and access to that can be limited or fully disabled.

AI PROMPTS

Zscaler provides a feature in which Prompts sent to AI applications can be captured based on policy. This feature is not enabled by default and enabling is up to the customer's decision. If enabled, the logfiles will include the prompt itself for supported services as listed on Zscaler's online-help.
help.zscaler.com/zia/about-generative-ai-security-report

The service includes RBAC to save guard access to this information and on a per admin role it can be decided to choose access to this information:

- **Visible:** Gen AI prompts are visible.
- **Obfuscated:** Gen AI prompts are obfuscated.

Controlled Access to the Collected Information

Operational Use and Role Based Access Control (RBAC) in the ZIA UI

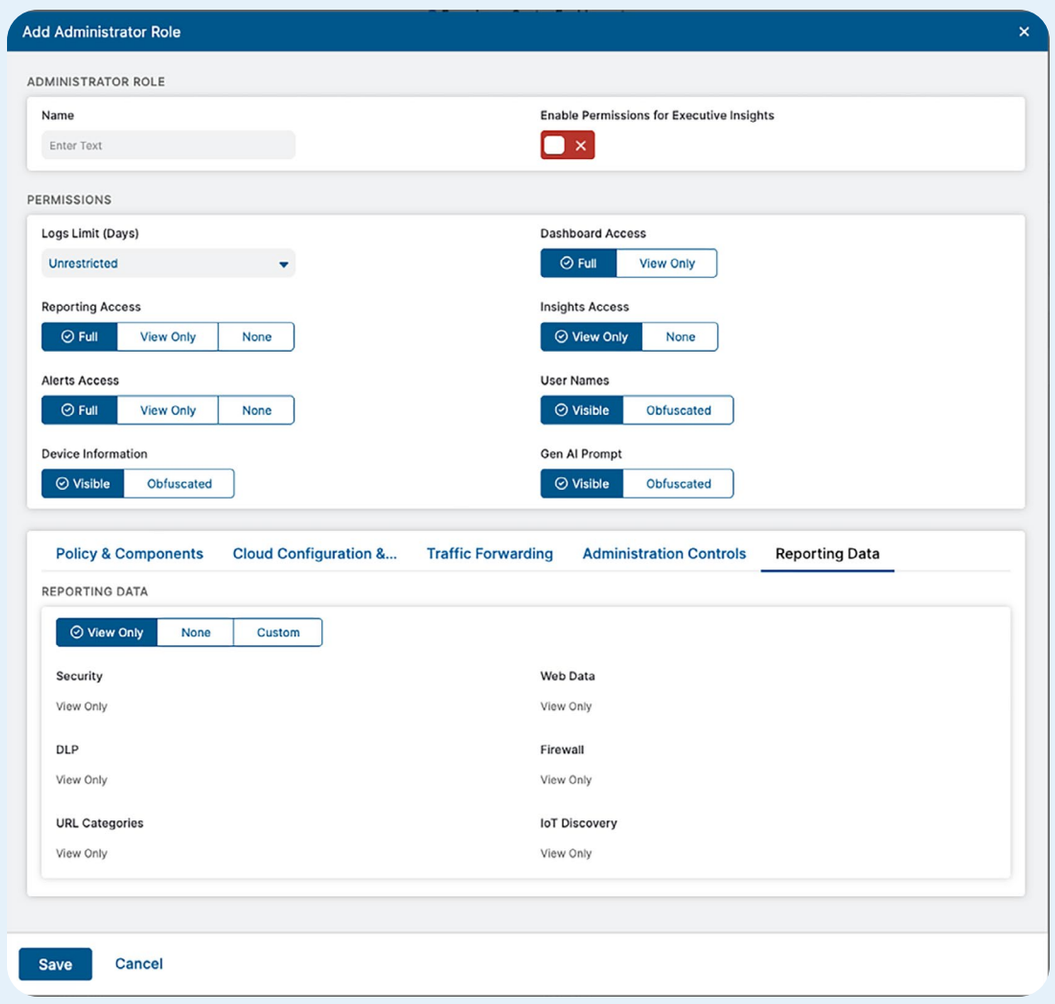
As the DLP UI is fully embedded into the ZIA UI, apart from workflow automation, which will be handled separately, it follows the same approach to allowing access to the policy and logging sections. Additionally, the same method of username obfuscation is applied for displaying the log's data.

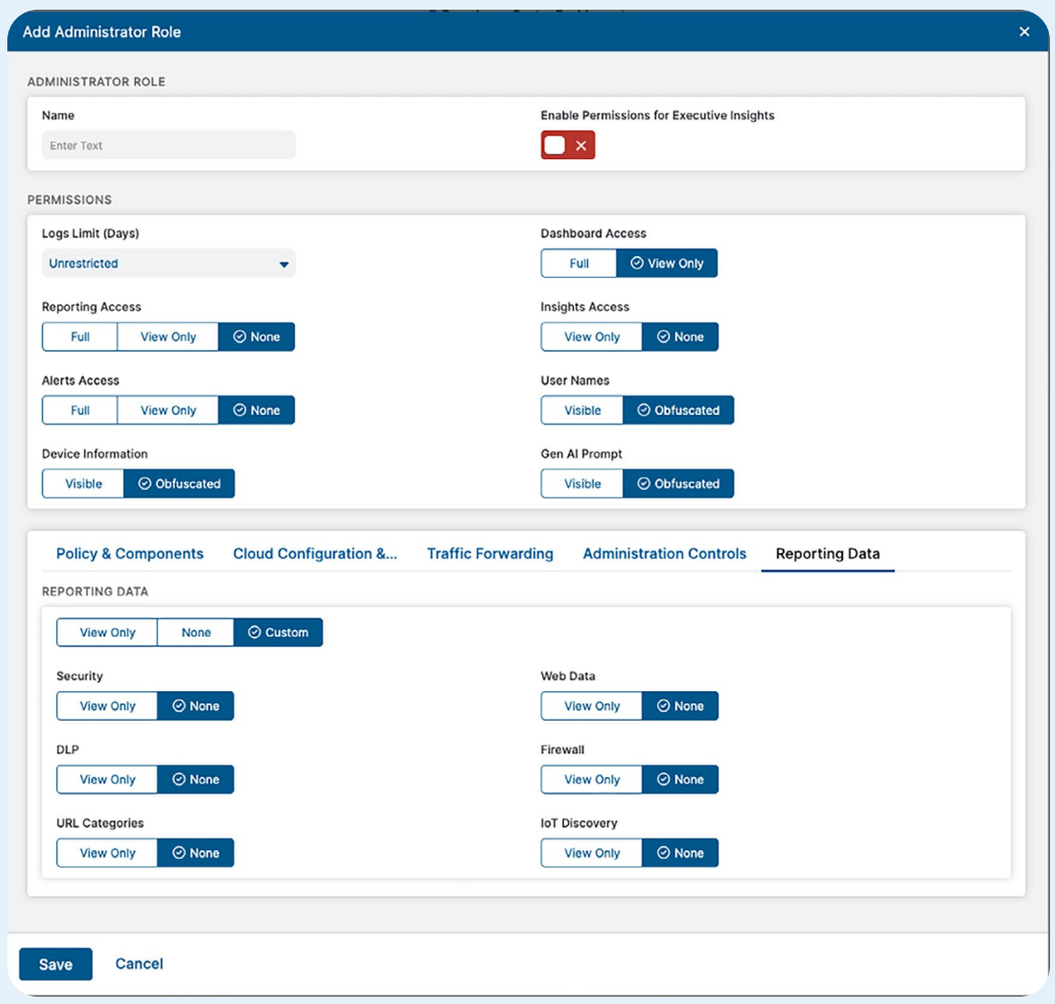
These RBAC controls will specify access to just Data Loss Prevention data inside the console, while non-DLP specific fields are hidden. This applies to data in dashboards as well.

Additionally, using the options to obfuscate usernames and device info, customers can specify whether real user names are visible or obfuscated for an admin when they view dashboards, reports, or insights. This data can also be obfuscated in NSS feeds.

These controls assure that access to data is only permitted to people in need to know.

Configuring Role Based Access for Zscaler Data Security





Operational Use and Role Based Access Control (RBAC) in the Workflow Automation UI

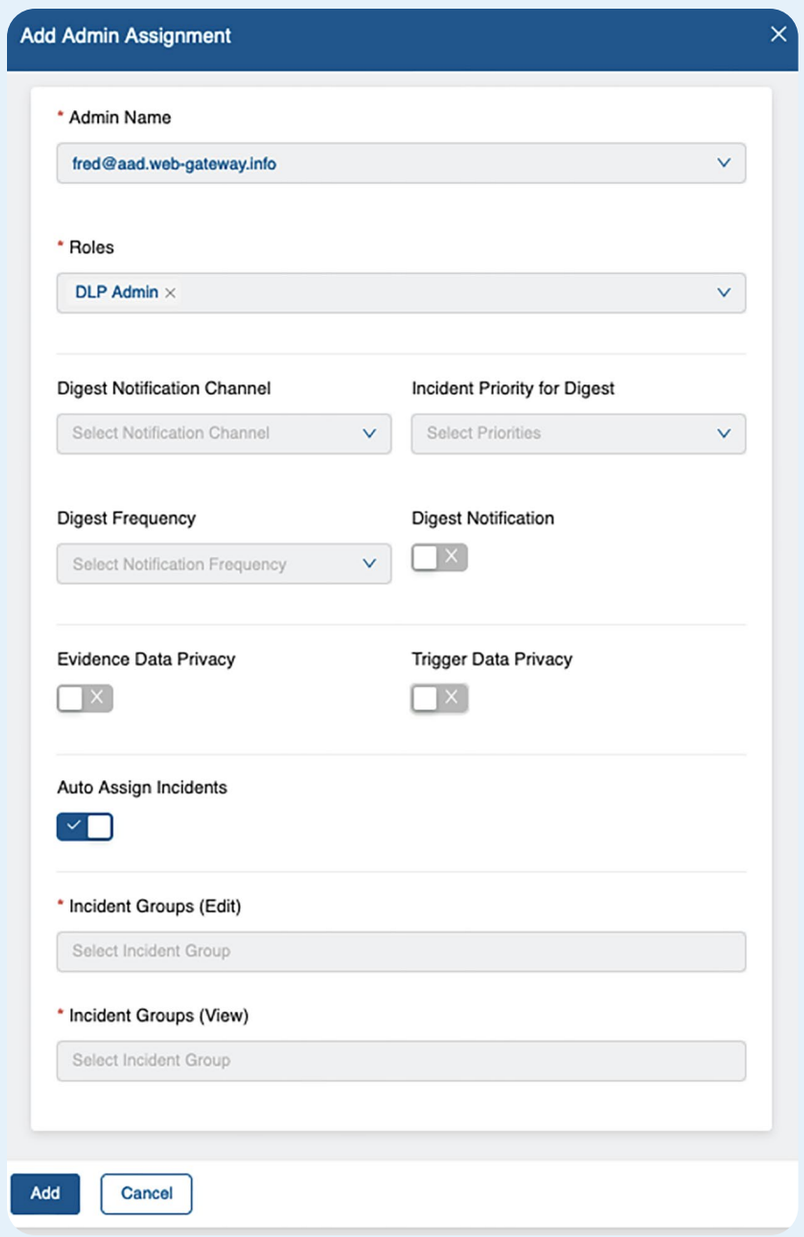
Similar, to the previously explained ZIA UI, Workflow Automation has it's own concept of RBAC, which is important as Workflow Automation provides direct access to sensitive data.

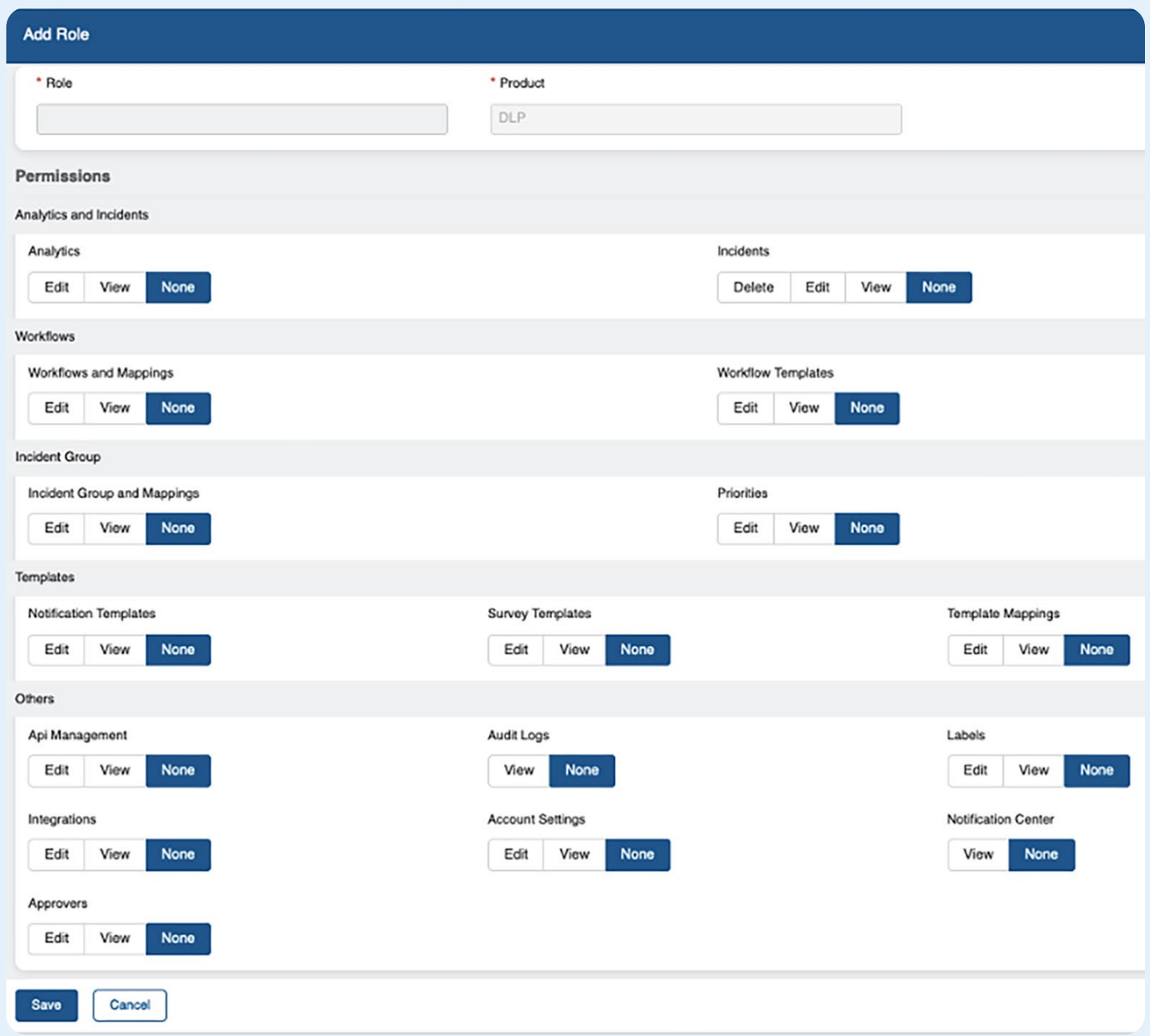
Conceptually, Workflow Automation can segment data, i.e. by group or department a user belongs to. This enabled use cases where a certain DLP analyst is deemed trust worthy to look at incidents for executives, while others are not. Access to specific incident groups of data can be set. Equally, access to trigger data (content that matches inside a document for example) and access to the evidence data (i.e. a file that was uploaded) can be controlled on a per account basis.

- Evidence Data Privacy Controls access to original files
- Trigger Data Privacy controls access to violating content
- Incident Groups (read/write) control what incidents in which group an admin has access to

Additionally, general UI-based RBAC is available to control access to feature and functions of the product.

Configuring Role Based Access for Workflow Automation





Zscaler Compliance

For ZIA, as for all Zscaler offerings, we have strict compliance and data privacy measures in place and are certified on a number of industry recognized standards.

For more information, consult our privacy website, which is the binding source for any official statements or compliance information: **zscaler.com/privacy-compliance/compliance-and-standards.**

Compliance Partnership

As a security-as-a-service provider, data privacy and security are the core of Zscaler's business and something Zscaler takes very seriously. We are committed to helping you successfully comply with Data Provacy and compliance requirements through a strong partnership between Zscaler (data processor) and your organization (data controller).

Zscaler teams have thoroughly analyzed the GDPR to ensure that our services and agreements align with the new regulations. Our tool, the Controller vs Processor Responsibility Chart helps customers better understand compliance requirements with your organization and partners as the data controller, and what they can expect from Zscaler as the data processor.

Data Protection

Zscaler ensures confidentiality and availability by storing a limited amount of personal data, such as IP addresses, URLs, and user IDs, and does not process or store any special categories or sensitive data. The Zscaler cloud platform has been architected to do all inspection in memory; transactional content is never stored or written to disk.

Security Safeguards

Because Zscaler operates a multi-tenant cloud, it is certified to the ISO 27001 framework to maintain consistent and robust security controls. Zscaler encrypts all traffic communication within its cloud, and implements strict security controls such as antivirus, firewalls, vulnerability scanning, penetration testing, and security code peer reviews.

RESOURCES

Information on internet protocol (IP) addresses to access the service.
config.zscaler.com

Data Protection and Privacy
zscaler.com/privacy-compliance/compliance-and-standards

Zscaler Sub-processors
zscaler.com/privacy-compliance/subprocessors

Company > Compliance
zscaler.com/privacy-compliance/compliance

About Zscaler

Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world's largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across more than 160 data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.