ZSCALER AND GOOGLE WORKSPACE DEPLOYMENT GUIDE

OCTOBER 2025, VERSION 1.1

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
XFF	X-Forwarded-For (RFC7239)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see **Zscaler's website**.

Google Overview

Google (NASDAQ: **GOOGL**) is an American multinational corporation and technology company focusing on online advertising, search engine technology, cloud computing, computer software, quantum computing, e-commerce, consumer electronics, and artificial intelligence (AI). Its mission is to organize the world's information and make it universally accessible and useful. It is one of the world's most valuable brands due to its market dominance, data collection, and technological advantages in the field of AI. Google's parent company, Alphabet Inc., is one of the 5 Big Tech companies, alongside Amazon, Apple, Meta, and Microsoft. To learn more, refer to **Google's website**.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- Zscaler Resources
- Google Resources
- Appendix B: Requesting Zscaler Support

Software Versions

This document was authored using the latest version of Zscaler software.

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact **partner-doc-support@zscaler.com** to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact **z-bd-sa@zscaler.com** to reach the team that validated and authored the integrations in this document.

Zscaler and Google Introduction

Overviews of the Zscaler and Google applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

Google Workspace Overview

Google Workspace is a suite of online productivity apps designed for businesses and organizations, offering communication and collaboration tools. It includes familiar apps like Gmail, Google Calendar, Google Meet, Google Drive, Google Docs, Google Sheets, and Google Slides, providing a centralized platform for creating, communicating, and collaborating.

Key features and benefits of Google Workspace:

- Collaboration: Enables real-time document editing, sharing, and feedback within teams.
- Communication: Provides email, video conferencing, and instant messaging for effective communication.
- Storage: Offers cloud-based storage for files and documents through Google Drive.
- Organization: Allows for easy management of users, permissions, and settings through an admin console.
- Integration: Seamlessly integrates various apps for streamlined workflows.
- AI-powered tools: Includes AI-powered features in Gmail and other apps to enhance productivity and efficiency.

Google Resources

The following table contains links to Google support resources.

Name	Definition
Google Workspace Admin Help	Help resources for Google Workspace Administrators.

Zscaler and Google Workspace

Zscaler and Google Workspace are a security partnership that enhances the security and control of data within the Google Workspace suite of applications. Zscaler provides a cloud-based security platform, while Google Workspace offers productivity and collaboration tools like Gmail, Google Drive, and Google Docs. Together, they offer features like zero trust access, data loss prevention (DLP), and security insights, making it easier for businesses to protect sensitive information within their Google Workspace environment.

ZIA provides visibility and security for Google SaaS applications with out-of-band Cloud Access Security Broker (CASB), SaaS Tenant Control, SaaS Security Management, Google Drive Labels, and Google Workspace to third-party application governance. This deployment guide outlines all Zscaler Google Workspace-related integrations and key benefits.

The following diagram shows the Zscaler and Google Workspace integration.

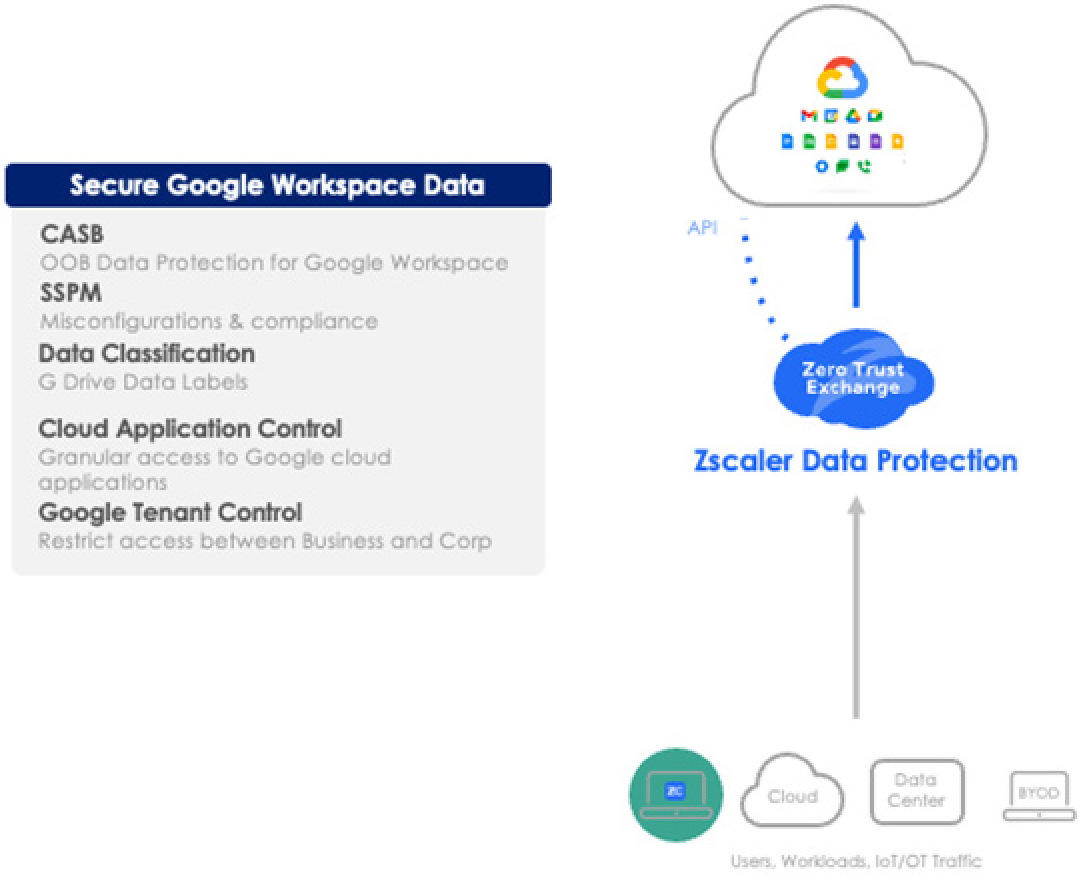

Secure Google Workspace Data
CASB
OOB Data Protection for Google Workspace
SSPM
Misconfigurations & compliance
Data Classification
G Drive Data Labels
Cloud Application Control
Granular access to Google cloud applications
Google Tenant Control
Restrict access between Business and Corp
API
Zero Trust Exchange
Zscaler Data Protection
ZC
Cloud
Data Center
BYOD
Users, Workloads, IoT/OT Traffic

Figure 1. Zscaler and Google Workspace integration

Google Workspace SaaS Security

Zscaler's SaaS Security is an out-of-band CASB security API that protects data and ensures compliance. It scans data repositories and keeps historical data for cloud applications such as Google Workspace.

How Does it Work?

- Scans data: Zscaler's out-of-band CASB scans data repositories and identifies files at rest.
- Remediates threats: Zscaler's out-of-band CASB remediates threats and prevents data exposure.
- Ensures compliance: Zscaler's out-of-band CASB provides deep compliance visibility and assurance across SaaS applications.

Key Benefits

- Threat protection: Zscaler's CASB protects against malware, ransomware, and other threats.
- Data protection: Zscaler's CASB prevents malicious and accidental data leakage.
- Visibility: Zscaler's CASB provides in-depth logging and reporting for cloud data.
- Compliance: Zscaler's CASB provides deep compliance visibility and assurance.

Onboarding Overview

The Zscaler service supports both Zscaler-defined and custom-defined onboarding connectors. Both supported API authorization capabilities are outlined in this deployment guide.

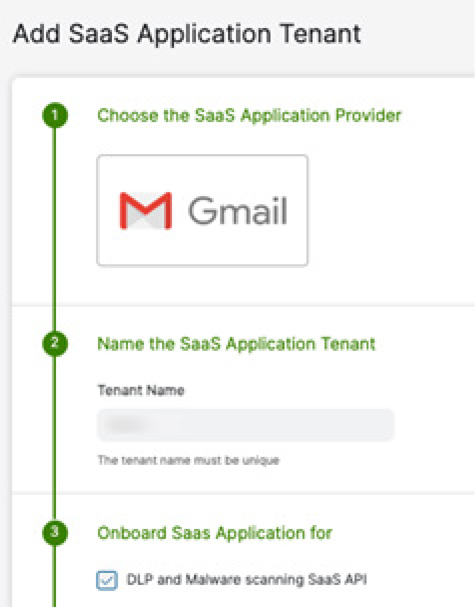
For more information about the Google Workspace Administration, refer to Google Workspace Admin Help.

Onboarding Zscaler-Defined Connectors

The following sections describe onboarding the defined Zscaler connectors.

Gmail

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **SaaS Application Tenants**.
3. Select **Add SaaS Application Tenant**.
4. Select **Gmail**.
5. In **Tenant Name**, enter a unique name.
6. In **Onboard SaaS Application for**, select the **DLP and Malware scanning SaaS API** checkbox.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

2 Name the SaaS Application Tenant

Tenant Name

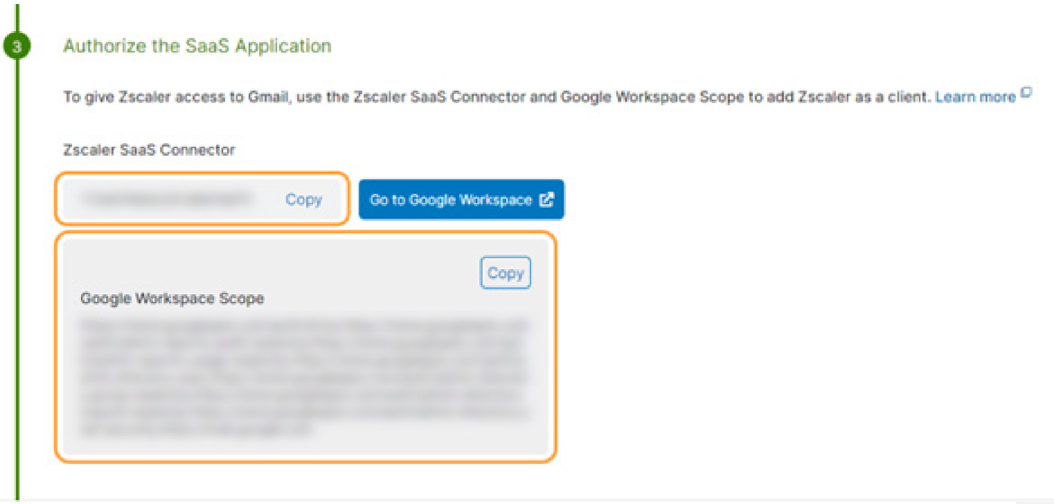
The tenant name must be unique

3 Onboard Saas Application for

☑ DLP and Malware scanning SaaS API

Figure 2. Gmail Zscaler defined

7. Enter your **Google Admin Email ID**.
8. Under **Authorize the SaaS Application**, select **Zscaler Defined**, and copy the **Zscaler SaaS Connector** and **Google Workspace Scope**. You need it for a later step when adding an API client for Google Workspace.



3 Authorize the SaaS Application

To give Zscaler access to Gmail, use the Zscaler SaaS Connector and Google Workspace Scope to add Zscaler as a client. Learn more

Zscaler SaaS Connector

Google Workspace Scope

Figure 3. Authorize SAAS Application

9. Click **Go to Google Workspace**. The **Google Workspace** portal appears.
   a. Log in to Google Workspace.
   b. Go to **Access and data control** > **Security**.
   c. Click **API controls**.
   d. Under **Domain wide delegation**, click **Manage Domain Wide Delegation**.
   e. Click **Add new**. The **Add a new client ID** window appears.
      - **Client ID**: Enter the Zscaler SaaS Connector value.
      - **Overwrite existing client ID**: Deselect.
      - **OAuth scopes (comma-delimited)**: Enter the Google Workspace scope.
      - Click **Authorize**.

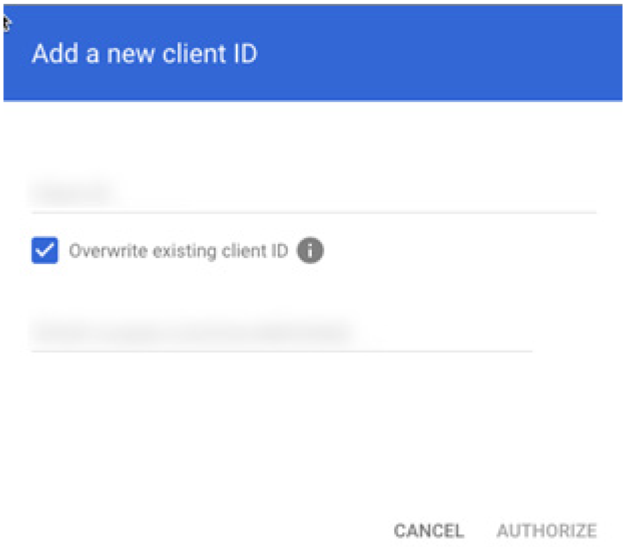


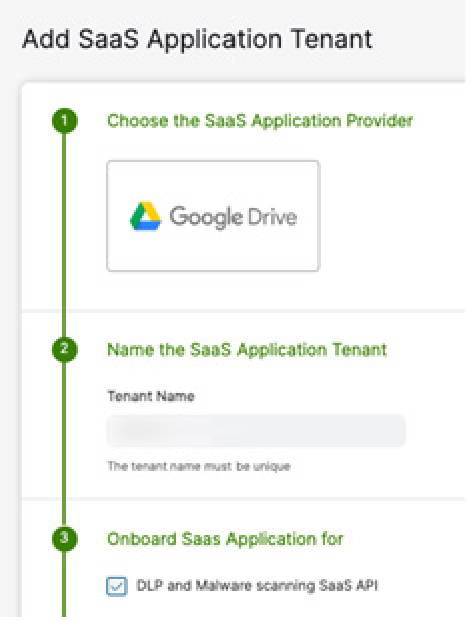
Figure 4. OAuth Scope

The Zscaler Connector App is added as an API client.

10. (Optional) Under **Configure External Trusted Domains & Users for the Tenant**:
    - **External Trusted Domains**: Enter trusted email domains that are outside your organization (i.e., using a different domain). The Zscaler service views any email addresses from the added domains as trusted, internal users for Gmail. For example, if your organization's domain is safemarch.com and your organization recently acquired a company with the domain example.com, you can add example.com to this list, and the service treats any email addresses from example.com (e.g., johnsmith@example.com) as internal users from safemarch.com. You can add up to 1,000 domains.
    - **External Trusted Users**: Enter trusted email addresses that are outside your organization (i.e., using a different email domain). The Zscaler service views the email addresses as trusted, internal users for Gmail. For example, if your organization's email domain is safemarch.com and your organization recently contracted with someone using an external email domain (e.g., johnsmith@example.com), you can add the contractor's email to this list, and the service treats the contractor as an internal user from safemarch.com. You can add up to 1,000 email addresses.

Google Drive

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **SaaS Application Tenants**.
3. Select **Add SaaS Application Tenant**.
4. Select **Google Drive**.
5. In **Tenant Name**, enter a unique name.
6. In **Onboard SaaS Application for**, select the **DLP and Malware scanning SaaS API** checkbox.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

Google Drive

2 Name the SaaS Application Tenant

Tenant Name

[redacted]

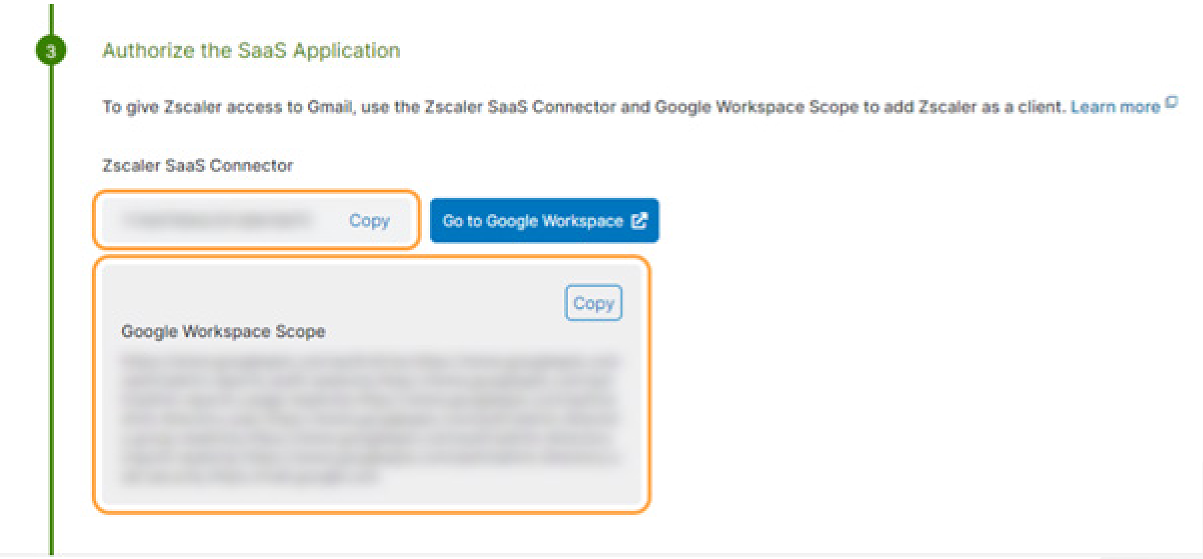
The tenant name must be unique

3 Onboard Saas Application for

☑ DLP and Malware scanning SaaS API

Figure 5. Google Drive Zscaler Defined

7. Enter your **Google Admin Email ID**.
8. Under **Authorize the SaaS Application**, select **Zscaler Defined**, and copy the **Zscaler SaaS Connector** and **Google Workspace Scope**. You need it for a later step when adding an API client for Google Workspace.



3 Authorize the SaaS Application

To give Zscaler access to Gmail, use the Zscaler SaaS Connector and Google Workspace Scope to add Zscaler as a client. Learn more

Zscaler SaaS Connector

[redacted]

Google Workspace Scope

[redacted]

Figure 6. Authorize SaaS App

9. Click **Go to Google Workspace**. The **Google Workspace** portal appears.
10. Log in to Google Workspace.
11. Go to **Access and data control** > **Security**.
12. Click **API controls**.
13. Under **Domain wide delegation**, click **Manage Domain Wide Delegation**.
14. Click **Add new**. The **Add a new client ID** window appears. In the **Add a new client ID** window:
    a. **Client ID**: Enter the Zscaler SaaS Connector value.
    b. **Overwrite existing client ID**: Deselect.
    c. **OAuth scopes (comma-delimited)**: Enter the Google Workspace scope.
    d. Click **Authorize**.

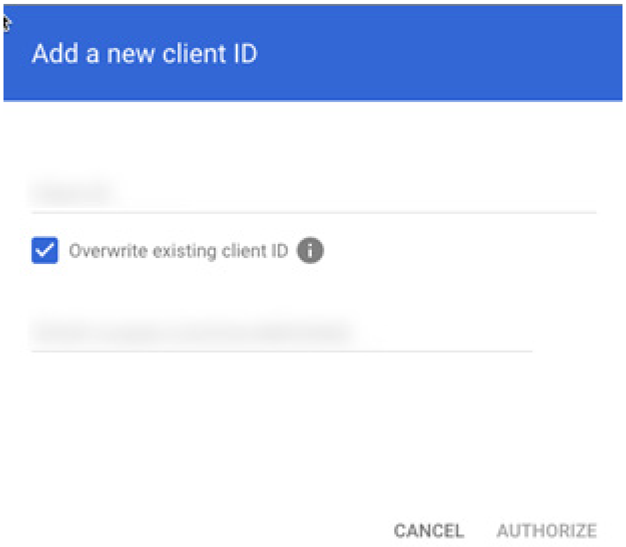


Figure 7. OATH SCOPE

The Zscaler Connector App is added as an API client.

15. (Optional) Under **Configure External Trusted Domains & Users for the Tenant**:
    - **External Trusted Domains**: Enter trusted email domains that are outside your organization (i.e., using a different domain). The Zscaler service views any email addresses from the added domains as trusted, internal users for Gmail. For example, if your organization's domain is safemarch.com and your organization recently acquired a company with the domain example.com, you can add example.com to this list, and the service treats any email addresses from example.com (e.g., johnsmith@example.com) as internal users from safemarch.com. You can add up to 1,000 domains.
    - **External Trusted Users**: Enter trusted email addresses that are outside your organization (i.e., using a different email domain). The Zscaler service views the email addresses as trusted, internal users for Gmail. For example, if your organization's email domain is safemarch.com and your organization recently contracted with someone using an external email domain (e.g., johnsmith@example.com), you can add the contractor's email to this list, and the service treats the contractor as an internal user from safemarch.com. You can add up to 1,000 email addresses.

Onboarding Custom Connectors

The Zscaler service supports custom, client-side connector onboarding for access to Gmail, Google Drive, and Google Workspace. With this functionality, instead of requiring full administrator credentials, the Zscaler service can use a minimum set of credentials to access these Google applications.

When creating a custom connector for these applications, you must configure them with the proper settings so that Zscaler can access the application.

For Gmail, Google Drive and Google Workspace custom client-side connector, see Authorizing a Custom Zscaler Connector for Google Applications (government agencies, see Authorizing a Custom Zscaler Connector for Google Applications).

For more information about the APIs or OAuth Scopes, see Appendix A: API/OAuth Permissions for Google Applications.

For SaaS Application validation Error Codes, see SaaS Application Validation Error Codes (government agencies, see SaaS Application Validation Error Codes).

Scanning Data at Rest Policies

The Data at Rest Scanning policy consists of the Data Loss Prevention (DLP) and Malware Detection policies policies (government agencies, see Data Loss Prevention (DLP) and Malware Detection policies). You can configure policies independently of each other for optimized protection.

Configuring Data at Rest Scanning Malware Detection Policy

The SaaS Security Data at Rest Scanning Malware Detection policy (government agencies, see SaaS Security Data at Rest Scanning Malware Detection policy) allows you to create rules to discover threats to data at rest in sanctioned SaaS applications.

To Configure Malware Detection policy

1. Log in to the ZIA Admin Portal.
2. Go to **Policy** > **SaaS Security** > **Data at Rest Scanning**.
3. Click **Malware Detection**.
4. On the **Malware Detection** tab, choose one of the following SaaS application types from the drop-down menu.
   - Email for Gmail.
   - File Sharing for Google Drive.

Email for Gmail

1. Click **Add Malware Detection Rule**. The **Add Malware Detection Rule Window** appears.
2. In the **Add Malware Detection Rule** window, enter the rule attributes:
   a. **Rule Name**: Enter a rule name.
   b. **Status**: Set to **Enabled**.
   c. **Application**: Select an application from the list.
   d. **Saas Application Tenant**: Select the tenant previously created.

   e. **Rule Label**: (Optional) Select rule label to associate with the rule.
   f. **Scan Inbound Email Links**: Select **Enabled** to allow the Zscaler service to inspect links included in inbound emails. If you select **Disabled**, the Zscaler service doesn't inspect the links.
3. For **Action**: Select the action for the rule to take when it detects malware:
   a. **Apply Email Tag**: The Zscaler service reports the incident and adds an unsafe attachment or link label to the email. When you choose this action, the **Label Name** field appears. From this drop-down menu, you can choose an email label you want the rule to apply to the emails. The Zscaler service automatically creates an email category or an email label in the users' email account if it hasn't already been created.
   b. **Report Malware**: The Zscaler service reports the incident but doesn't quarantine or remove the malware.
4. Click **Save** and activate the change.

File Sharing for Google Drive

1. Click **Add Malware Detection Rule**. The **Add Malware Detection Rule Window** appears.
2. In the **Add Malware Detection Rule** window enter the rule attributes:
   a. **Rule Name**: Enter a rule name.
   b. **Status**: Set to **Enabled**.
   c. **Application**: Select an application from the list.
   d. **Saas Application Tenant**: Select the tenant previously created.
   e. **Rule Label**: (Optional) Select rule label to associate with the rule.
   f. **Scan Inbound Email Links**: Select **Enabled** to allow the Zscaler service to inspect links included in inbound emails. If you select **Disabled**, the Zscaler service doesn't inspect the links.
3. **For Action**: Select the action for the rule to take when it detects malware:
   a. **Quarantine Malware**: The Zscaler service quarantines the file.
   b. **Quarantine Location**: This field appears only if you select the **Quarantine Malware** action. This is the location where malicious files are moved for quarantine. The Zscaler service creates a folder or library called Zscaler_Quarantine for the location. To specify the quarantine location for Google Drive, enter the **Google ID** for the user who owns the folder. The service creates the folder on the user's account.
   c. **Remove Malware**: The Zscaler service deletes the file.
   d. **Report Malware**: The Zscaler service reports the incident but doesn't quarantine or remove the malware.
4. Click **Save** and activate the change.

Configuring Data at Rest Scanning DLP Policy

The SaaS Security Data at Rest Scanning Data Loss Prevention (DLP) policy (government agencies, see SaaS Security Data at Rest Scanning Data Loss Prevention (DLP) policy) allows you to create rules to discover and protect sensitive data at rest in sanctioned SaaS applications.

1. Log in to the ZIA Admin Portal.
2. Go to **Policy** > **SaaS Security** > **Data at Rest Scanning**.
3. Click **Data Loss Prevention**.
4. On **Data Loss Prevention** tab, choose one of the following SaaS application types from the drop-down menu.
   - Email for Gmail.
   - File Sharing for Google Drive.

Email for Gmail

1. Click **Add DLP Rule**. The **Add DLP Rule Window** appears.
2. In the **Add DLP Rule** window, enter the rule attributes:
    a. **Rule order**: Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, and so on), and the rule order reflects this rule's place in the order. You can change the value, but if you've enabled **Admin Ranking** (government agencies, see **Admin Ranking**), then the assigned admin rank determines the rule order values you can select.
    b. **Rule Name**: Enter a unique name for the DLP rule.
    c. **Rule Status**: An enabled rule is actively enforced. A disabled rule is not actively enforced but does not lose its place in the rule order, the service skips it and moves to the next rule.
    d. **Rule Label**: (Optional) Select a rule label to associate it with the rule.
3. Define Criteria:
    a. **SaaS Application Tenant**: Select the **SaaS application tenants** (government agencies, see **SaaS application tenants**) to which you want to apply the rule. You can also search for application tenants.
    b. **Components**: The components that the Zscaler service inspects for sensitive data. Preset to inspect all components.
    c. **Senders**: The users who sent the attachments or messages containing sensitive data. Select **Any** to apply the rule to all **users** (government agencies, see **users**), or select up to 4 users under **General Users**. You can search for users or click **Add** to add a new user
    d. **Recipients**: Preset to **External**.
    e. **Groups**: The **groups** (government agencies, see **groups**) of the users who sent the attachments or messages containing sensitive data. Select **Any** to apply the rule to all groups, or select up to 8 groups. You can search for groups or click **Add** to add a new group.
    f. **Departments**: The departments of the users who sent the attachments or messages containing sensitive data. Select **Any** to apply the rule to all **departments** (government agencies, see **departments**) or select up to 8 departments. You can search for departments or click **Add** to add a new department.
    g. **DLP Engines**: Select **Any** to choose all **DLP engines** (government agencies, see **DLP engines**) for this rule, or select up to 4 engines. You can search for DLP engines.
4. (Optional) Define **DLP Incident Receiver**.
    a. If you don't have a third-party DLP solution or don't want to forward content, leave the **Zscaler Incident Receiver** field as **None**.
    b. If you want to forward the transactions captured by this policy rule to an on-premises DLP incident receiver, select the applicable **Zscaler Incident Receiver** from the drop-down menu. You must configure your **Zscaler Incident Receivers** (government agencies, see **Zscaler Incident Receivers**) to complete this step.
5. Define **Action**:
    a. **Apply Email Tag**: The rule reports the incident and applies an email tag to it. When you choose this action, the **Label Name** field appears. From this drop-down menu, you can choose an email label you want the rule to apply to the emails. The Zscaler service automatically creates an email category or an email label in the users' email account if it hasn't already been created.
    b. **Report Incident Only**: The rule reports the incident only.
    c. **Severity**: Select a severity level (i.e., **High**, **Medium**, **Low**, or **Information**) for the incidents that match this rule. The Information level allows you to track low-risk incidents that must be observed.

6. (Optional) Configure the email notification for the rule. If you do not select an auditor and notification template, a notification is not sent for this rule.
   a. For **Auditor Type**, select whether the auditor is from a **Hosted** database or **External** to your organization.
   b. Select the **Auditor**:
      - If the auditor is from a hosted database, select or search for the auditor.
      - If the auditor is external, enter the auditor's email address.
7. Select a **Notification Template**, if you configured one (government agencies, see configured one). You can also search for a notification template or click **Add** to add a new notification template.
8. (Optional) In the **Description** field, enter additional notes or information. The description cannot exceed 10,240 characters.
9. Click **Save** and activate the change.

File Sharing for Google Drive

Google Drive file sharing includes sharing by Google Calendar.

1. In the **Add DLP Rule** window, enter the rule attributes:
   a. **Rule order**: Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, and so on), and the rule order reflects this rule's place in the order. You can change the value, but if you've enabled Admin Ranking (government agencies, see Admin Ranking), then the assigned admin rank determines the rule order values you can select.
   b. **Rule Name**: Enter a unique name for the DLP rule.
   c. **Rule Status**: An enabled rule is actively enforced. A disabled rule is not actively enforced but does not lose its place in the rule order, the service skips it and moves to the next rule.
   d. **Rule Label**: (Optional) Select a rule label to associate it with the rule
2. Define **Criteria**:
   a. **SaaS Application Tenant**: Select the SaaS application tenants (government agencies, see SaaS application tenants) to which you want to apply the rule. You can also search for application tenants.
   b. **Site**: Select the sites to which you want to apply the rule. You can search for a site or select all sites.
   c. **Owners**: The users (government agencies, see users) who own the files containing sensitive data. Select **Any** to apply the rule to all users, or select up to 4 users under **General Users**. You can search for users or click **Add** to add a new user.
   d. **Groups**: The groups (government agencies, see groups) of the users who sent the attachments or messages containing sensitive data. Select **Any** to apply the rule to all groups, or select up to 8 groups. You can search for groups or click **Add** to add a new group.
   e. **Departments**: The departments (government agencies, see departments) of the users who sent the attachments or messages containing sensitive data. Select **Any** to apply the rule to all departments, or select up to 8 departments. You can search for departments or click **Add** to add a new department.
   f. **DLP Engines**: Select **Any** to choose all DLP engines for this rule, or select up to 4 engines. You can search for DLP engines.
   g. **File Type**: Select file types to which you want to apply the rule. You can select any number of file types and also search for file types.

h. **Collaboration Scope**: The collaboration scopes and permissions for SaaS tenant files that contain sensitive data. Select **Any** to apply the rule to files with all collaboration levels, or select any number of the following collaboration scopes and specify the permissions (**View**, **Edit**) for each scope:

   i. **External Collaborators**: Files that are shared with specific collaborators outside of your organization.

   ii. **External Link**: Files with shareable links that allow anyone outside your organization to find the files and have access.

   iii. **Internal Collaborators**: Files that are shared with specific collaborators or are discoverable within your organization

   iv. **Internal Link**: Files with shareable links that allow anyone within your organization to find the files and have access

   v. **Private**: Files that are only accessible to the owner.

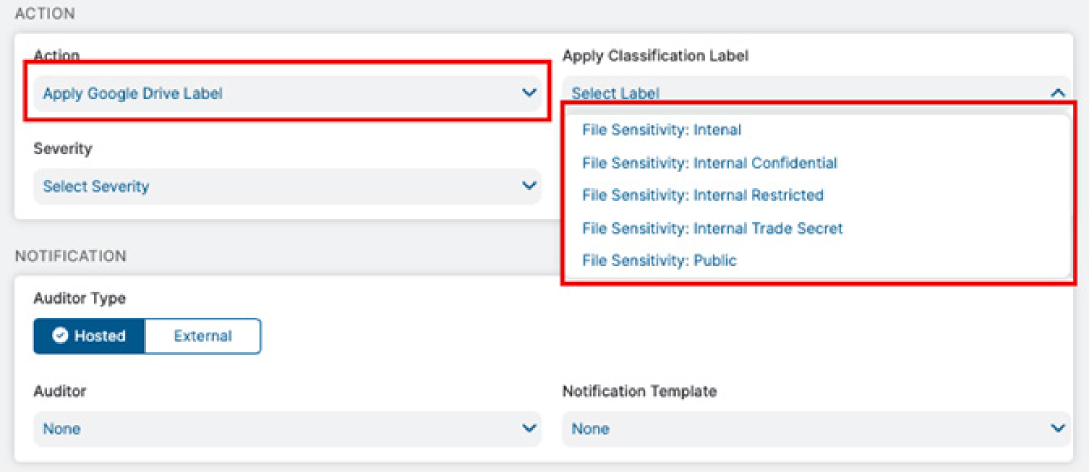
3. (Optional) Define **DLP Incident Receiver**.

   - If you don't have a third-party DLP solution or don't want to forward content, leave the **Zscaler Incident Receiver** field as **None**.
   - If you want to forward the transactions captured by this policy rule to an on-premises DLP incident receiver, select the applicable Zscaler Incident Receiver (government agencies, see Zscaler Incident Receiver) from the drop-down menu. You must configure your Zscaler Incident Receivers to complete this step.

4. Define **Action**:

   a. **Apply Google Drive Label**: This action is only applicable for Google Drive tenants. The rule reports the incident and applies the chosen Google Drive label to the file. When you choose this action, the **Apply Classification Label** field appears. From this drop-down menu, you can choose the Google Drive classification label you want the rule to apply to files. The Zscaler service collects these labels when you onboard the Google Drive tenant (government agencies, see onboard the Google Drive tenant). Deleted labels appear with a strikethrough line in the drop-down menu and cannot be applied to a rule.

   To see this action, you must choose a single Google Drive tenant with defined labels from the **SaaS Application Tenant** drop-down menu. This action is unavailable if you choose a tenant without defined labels or select multiple Google Drive tenants.



ACTION

Action: Apply Google Drive Label

Severity: Select Severity

Apply Classification Label: Select Label

- File Sensitivity: Intenal
- File Sensitivity: Internal Confidential
- File Sensitivity: Internal Restricted
- File Sensitivity: Internal Trade Secret
- File Sensitivity: Public

NOTIFICATION

Auditor Type: Hosted | External

Auditor: None

Notification Template: None

Figure 8. Drive labels

Before you can use labels in a Google Drive tenant that you have already onboarded, you must reauthorize the tenant so that Zscaler can identify all available labels. To learn more, see About SaaS Application Tenants (government agencies, see About SaaS Application Tenants).

b. **Quarantine to Root User Root Folder**: The rule reports the incident and quarantines sensitive content to a user's root folder. When you select this option, the **Tombstone Template** drop-down menu appears.

c. **Remove External Collaborators**: The rule reports the incident and removes all of the file's external collaborators.

d. **Remove External Collaborators and Sharable Link**: The rule reports the incident and removes all of the file's external collaborators and any shareable links.

e. **Remove Internal Collaborators and Sharable Link**: The rule reports the incident and removes all internal collaborators and any shareable links.

f. **Remove Internal Sharable Link**: The rule reports the incident and removes the file's internal shareable link. Existing collaborators are unaffected.

g. **Remove Public Sharable link**: The rule reports the incident and removes the file's public shareable link. Existing collaborators are unaffected.

h. **Remove Sharing**: The rule reports the incident and removes all of the file's collaborators and any shareable links.

i. **Report Incident Only**: The rule reports the incident only and makes no changes to the file's collaboration scope.

j. **Update to Not Discoverable to All**: The rule reports the incident and changes the file's collaboration scope to prevent it from being discoverable through public search engines or within your organization.

For more information about the DLP engines, see About DLP Engines (government agencies, see About DLP Engines).

5. (Optional) Define **DLP Incident Receiver**.

   a. If you don't have a third-party DLP solution or don't want to forward content, leave the **Zscaler Incident Receiver** field as **None**.

   b. If you want to forward the transactions captured by this policy rule to an on-premises DLP incident receiver, select the applicable Zscaler Incident Receiver (government agencies, see Zscaler Incident Receiver) from the drop-down menu. You must configure your Zscaler Incident Receivers to complete this step.

6. (Optional) Configure the email notification for the rule. If you do not select an auditor and notification template, a notification is not sent for this rule.

   a. For **Auditor Type**, select whether the auditor is from a **Hosted** database or **External** to your organization.

   b. Select the Auditor:

      - If the auditor is from a hosted database, select or search for the auditor.
      - If the auditor is external, enter the auditor's email address.

7. Select a **Notification Template**, if you configured one (government agencies, see configured one). You can also search for a notification template or click **Add** to add a new notification template.

8. (Optional) In the **Description** field, enter including additional notes or information. The description cannot exceed 10,240 characters.

9. Click **Save** and activate changes.

Configuring SaaS Scan Schedule

To configure a Scan Schedule:

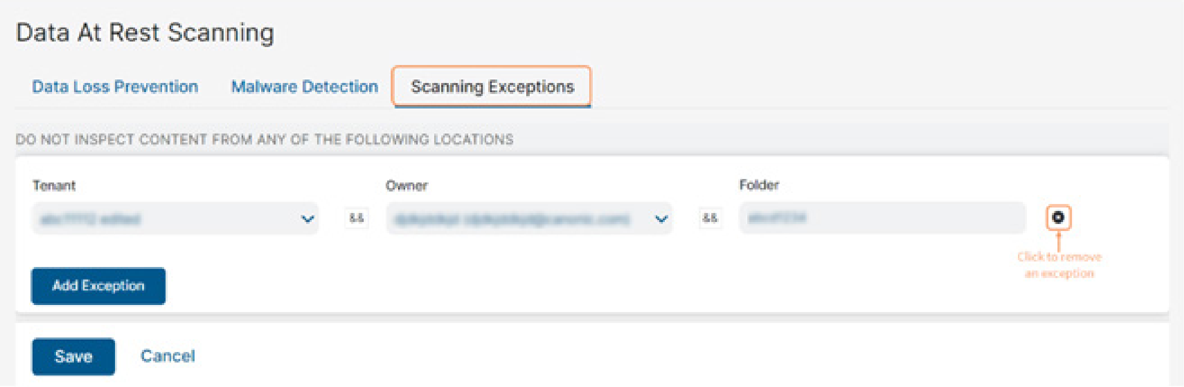
1. Log in to the ZIA Admin Portal.
2. Go to **Policy** > **SaaS Security** > **Scan Configuration**.
3. Click **Add Scan Schedule**.
4. The **Add Scan Schedule** window appears. In the **Add Scan Schedule** window:
    a. **SaaS Application Tenant**: Select the SaaS application tenant (government agencies, see SaaS application tenant) to which you want to apply the scan.
    b. **Policy**: Select the SaaS Security API policies you want the scan to use when inspecting content. You must choose at least one policy to schedule a scan.
    c. **Data to Scan**: Specify the amount of historical data for the scan to inspect. When the scan processes historical content, it continuously inspects active data at the same time. To learn more, see Configuring a Scan to Inspect Historical Data (government agencies, see Configuring a Scan to Inspect Historical Data).
        i. **All Data**: The scan inspects all historical data. The time it takes to complete the scan depends on the amount of data you have.
        ii. **Data Created or Modified After**: The scan inspects historical data within a specific time frame. Use the Calendar menu to choose the starting date for the time frame.
        iii. **New Data Only**: The scan ignores all historical data.
5. (Optional) In the **Description** field, enter additional notes or information. The description cannot exceed 10,240 characters.
6. Click **Save** and activate the change.

Configuring SaaS Scan Exceptions

Configuring a scanning exception allows you to exempt specific folders or users from the Understanding the Data at Rest Scanning Policy (government agencies, see Understanding the Data at Rest Scanning Policy), which consists of the Data Loss Prevention (DLP) and Malware Detection policies (goverment agencies, see Data Loss Prevention (DLP) and Malware Detection policies). When you configure a scanning exception for a folder, the Zscaler service completely ignores the files within the folder (i.e., its files aren't evaluated with the Data at Rest Scanning policy). Likewise, the Zscaler service ignores an exempted user and the user isn't evaluated with the policy.

1. Log in to the ZIA Admin Portal.
2. Go to **Policy** > **SaaS Security** > **Data at Rest Scanning** > **Scanning Exceptions**.
3. Under **Do Not Inspect Content From Any of the Following Locations**, to add an exception for a folder:
    a. Click **Add Exception**. A row with the **Tenant**, **Owner**, and **Folder** fields appears. In the row:
        i. **Tenant**: From the drop-down menu, choose the SaaS application tenant (government agencies, see SaaS application tenant) that the folder belongs to.
        ii. **Owner**: From the drop-down menu, choose the user (government agencies, see user) who owns the folder.
        iii. **Folder**: Enter the full path for the folder you want to exempt from inspection.

4. To **Add Exception** for a user:
   a. Click **Add Exception**. A row with the **Tenant**, **Owner**, and **Folder** fields appears.
   b. From the **Owner** drop-down menu, choose the user you want to exempt from inspection.
5. Click **Add Exceptions** to exempt more folders or users from inspection. You can add up to 64 exceptions for folders and users. To remove an exception, click the **Remove** icon for the row.
6. Click **Save** and activate changes.



Data At Rest Scanning

DO NOT INSPECT CONTENT FROM ANY OF THE FOLLOWING LOCATIONS

Tenant		Owner		Folder
[redacted]	&&	[redacted]	&&	[redacted]

Figure 9. Exceptions

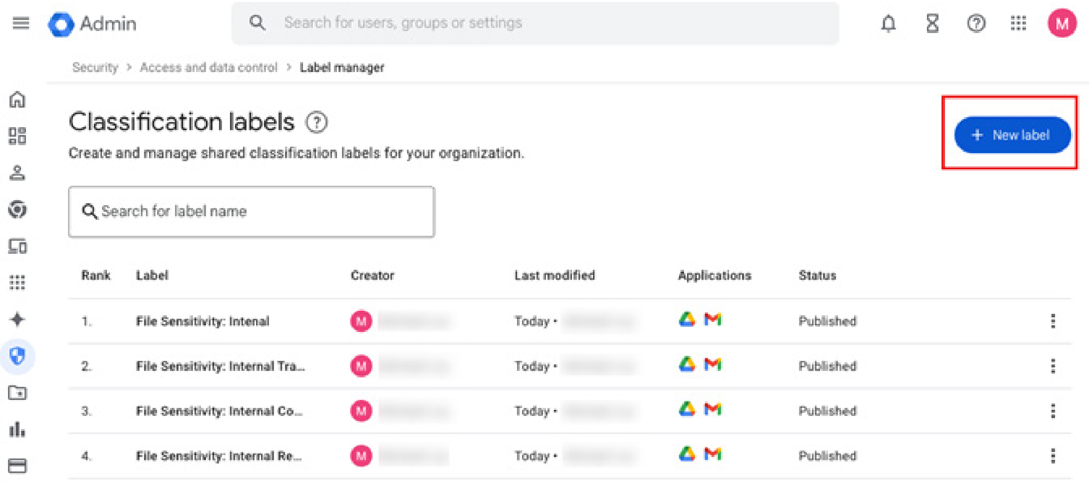
Google Drive Labels

When creating SaaS Security API policy rules for your Google Drive tenants, you can apply classification labels defined in Google Drive.

Zscaler can integrate with Google Drive Labels to add labels to files for classification, audit, and data protection purposes. To enable this integration, Drive labels must be predefined in Google Workspace classification labels. Zscaler by DLP scan policy then scans and assigns appropriate labels based on the defined DLP scan policy.

To enable classification labels:

1. Log in to the Google Admin console.
2. Go to **Security** > **Access and data control** > **Label manager**.
3. Select **New label**.



Admin
Search for users, groups or settings
M
Security > Access and data control > Label manager
+ New label
Search for label name

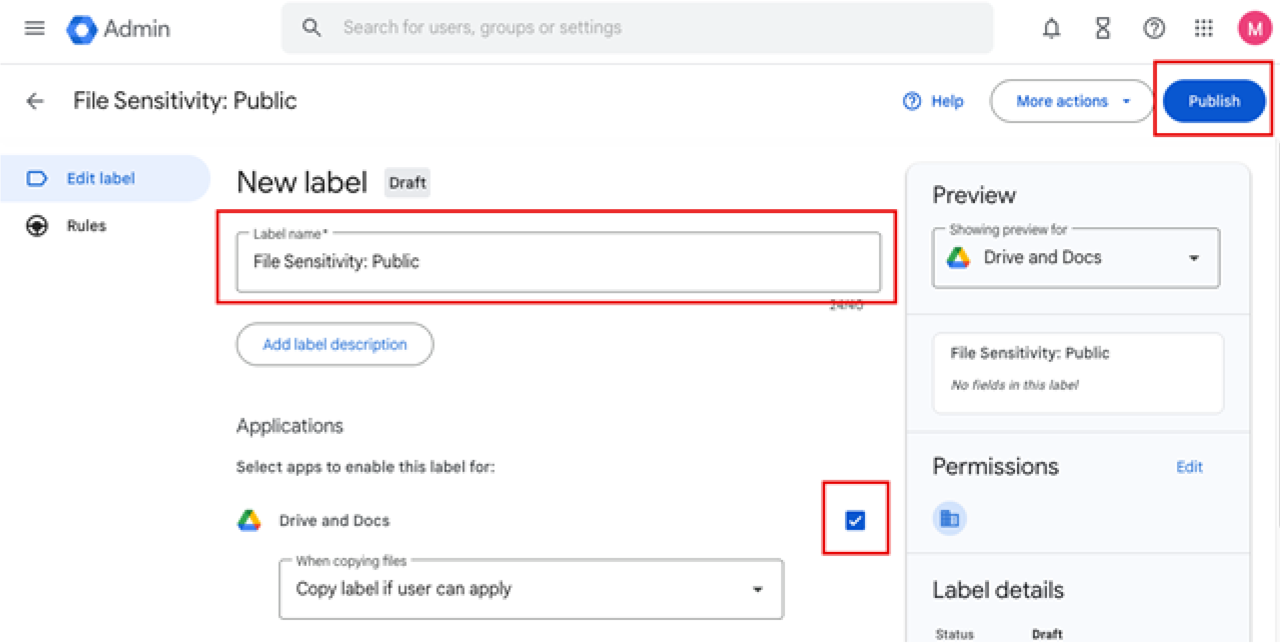
Classification labels

Create and manage shared classification labels for your organization.

Rank	Label	Creator	Last modified	Applications	Status
1.	File Sensitivity: Intenal	M [redacted]	Today • [redacted]		Published
2.	File Sensitivity: Internal Tra...	M [redacted]	Today • [redacted]		Published
3.	File Sensitivity: Internal Co...	M [redacted]	Today • [redacted]		Published
4.	File Sensitivity: Internal Re...	M [redacted]	Today • [redacted]		Published

Figure 10. Google Classification Label

4. A new window appears for **New label**. In the **New label**, define the following:
   a. **Label name**: Enter a label name. This is the label for applying the Zscaler DLP policy.
   b. **Add label description**: (Optional) Add a label description up to 255 characters.
   c. **Applications**: Select the **Drive and Docs** checkbox.
5. Click **Publish**.



File Sensitivity: Public

New label Draft

Label name*: File Sensitivity: Public

24/40

Add label description

Applications

Select apps to enable this label for:

Drive and Docs ☑

When copying files: Copy label if user can apply

Showing preview for: Drive and Docs

File Sensitivity: Public
No fields in this label

Status Draft

Figure 11. New label define and publish

To enable Google Drive labels, follow the steps in **Google Drive** and **File Sharing for Google Drive** under File Sharing.

Google Cloud Application Control

Zscaler Cloud Application Control is a feature within the Zscaler security platform that allows administrators to granularly manage and control access to specific cloud applications used by employees within an organization, enabling them to define rules to allow or block access to certain apps based on categories, usage limits, and other criteria, essentially providing a way to monitor and regulate which cloud applications users can access and how much they can use them.

Zscaler Cloud App Control enables granular control over popular Google websites and SaaS applications. Zscaler provides granular control for over 50 Google applications and services across 13 categories.

The following table shows the supported Google Cloud Applications.

Category	Application
AI & ML Applications	Gemini
Collaboration and Online Meeting Applications	Google Calendar Google Keep Google Sites Google Alerts Google Jamboard Google Cloud Print Google Workspace Google Duo Google Remote Desktop
Consumer Applications	Google Earth Google Doodle Games
DNS over HTTP Services	Google DNS
File Sharing Applications	Google Drive Google Photos
Hosting Provider	Google Cloud Compute Google App Engine Google Cloud Platform
Instance Messaging	Google Hangouts Google Chat
IT Services	Google Login Service Google Domains Google Apps Back Up
Sales and Marketing	Google Wallet Google Ads Google Ad Manager Google Business Review Link Generator Google Marketing Platform Google Search Console

Category	Application
CRM and Productivity Tools	Google Analytics Google App for Business Google Classroom Google Data Studio Google Analytics 360 studio Google Contacts Google Enterprise support Google Feed burner Google Translate Google Books Google opensource
Social Networking	Google Groups Google +
Streaming Media	Google Video You Tube
System and Development	Google Developers Google App Maker Google Maps Google Web Toolkit (GWT) Google Fonts Google DeepMind
Web Mail	Gmail

To configure Cloud Application Control for a Google Cloud Application:

1. Log in to the ZIA Admin Portal.
2. Go to **Policy** > **URL & Cloud App Control**.
3. From the **Cloud App Control Policy** tab, click **Add** and select applicable category from the previous table.
4. Select one of the following **View by** options to see the **Cloud App Control** rules accordingly
   a. **Rule Order**: Policy rules are evaluated in ascending numerical order (Rule 1 before Rule 2, and so on), and the Rule Order reflects this rule's place in the order. You can change the value, but if you've enabled **Admin Rank** (government agencies, see **Admin Rank**), your assigned admin rank determines the Rule Order values you can select.
   b. **Admin Rank**: If **Enabled**, enter a value from 0–7 (0 is the highest rank). Your assigned admin rank determines the values you can select. You cannot select a rank that is higher than your own. The rule's admin rank determines the value you can select in Rule Order, so that a rule with a higher admin rank always precedes a rule with a lower admin rank
   c. **Rule Name**: Enter a unique name for the rule or use the default name
   d. **Rule Status**: An enabled rule is actively enforced. A disabled rule is not actively enforced but does not lose its place in the Rule Order. The service skips it and moves to the next rule.
   e. **Rule Label**: elect a rule label to associate it with the rule. To learn more, see **About Rule Labels** (government agencies, see **About Rule Labels**).

5. From **Criteria**:

   a. Cloud Application: Select **Any** to apply the rule to all cloud applications in this category, or select any number of cloud applications. You can also search for applications. By default, this field displays the first 100 cloud applications. The subsequent 100 cloud applications are displayed when you click the **Click to see more** link at the bottom of the list. You can repeat this process to view the remaining cloud applications.

   b. **Cloud Application Instances**: Select the cloud application instances to which the rule applies. You can select a maximum of 8 instances per rule.

The cloud application instance appears only if its parent application is selected as the cloud application.

   c. **Cloud Application Risk Profile**: Select a profile to which the rule applies.

You can either select the Cloud Application Risk Profile or the Cloud Applications field for the rule.

   d. **Users**: Select **Any** to apply the rule to all users (government agencies, see users), or select up to 4 users under **General Users**. If you've enabled the Policy for Unauthenticated Traffic (government agencies, see Policy for Unauthenticated Traffic), you can select **Special Users** to apply this rule to all unauthenticated users, or select specific types of unauthenticated users. You can search for users or click **Add** to add a new user.

   e. **Groups**: elect **Any** to apply the rule to all groups (government agencies, see groups), or select up to 8 groups. You can search for groups or click **Add** to add a new group.

   f. **Departments**: Select **Any** to apply the rule to all departments (government agencies, see departments), or select up to 8 departments. If you've enabled the Policy for Unauthenticated Traffic (government agencies, see Policy for Unauthenticated Traffic), you can select **Special Departments** to apply this rule to all unauthenticated transactions. You can search for departments or click **Add** to add a new department.

Any rule that applies to unauthenticated traffic (government agencies, see unauthenticated traffic) must apply to all Groups and Departments. So, if you have chosen to apply this rule to unauthenticated traffic for either Users or Departments, select **Any** from the drop-down menus for Groups and Departments.

   g. **Location**: Select **Any** to apply the rule to all locations (government agencies, see locations), or select up to 8 locations. You can also search for a location or click Add to add a new location.

   h. **Location Groups**: Select **Any** to apply the rule to all location groups (government agencies, see location groups), or select up to 32 location groups. You can also search for a location group.

   i. **Time**: Select **Always** to apply this rule to all time intervals (government agencies, see time intervals), or select up to two time intervals. You can also search for a time interval or click **Add** to add a new time interval.

   j. **Devices**: Select the devices (government agencies, see devices) to which the rule applies. You can also search for a device. Selecting no value ignores this criterion in the policy evaluation.

   k. **Device Groups**: Select the device groups (government agencies, see device groups) for which you want to apply the rule. For Zscaler Client Connector traffic, select the appropriate group based on the device platform. Select **Cloud Browser Isolation**, **IoT**, or **No Client Connector** to apply the rule to Isolation traffic, IoT traffic, or traffic that is not tunneled through Zscaler Client Connector, respectively. You can also search for a device group. Selecting no value ignores this criterion in the policy evaluation.

The Cloud Browser Isolation group is available only if Isolation is enabled for your organization.

l. **Device Trust Level**: Select the device trust level values (**High Trust**, **Medium Trust**, **Low Trust**, or **Unknown**) to which the rule applies. While the High Trust, Medium Trust, or Low Trust evaluation is applicable only to Zscaler Client Connector traffic, Unknown evaluation applies to all traffic. Selecting no value ignores the criterion in the policy evaluation.

The trust levels assigned to the devices are based on your posture configurations (government agencies, see posture configurations) in the Zscaler Client Connector Portal.

m. **User Agent**: Select **Any** to apply the rule to all user agents, or select any number of user agents. You can also search for an agent.

n. **User Risk Profile**: Select the user risk score levels to which the rule applies. Selecting no value ignores this criterion in the policy evaluation. Users are assigned a risk score based on their browsing activities. A range of risk scores is grouped as a risk score level. By default, the following user risk score levels are available:

- **Low**: Level with user risk scores ranging from 0 to 29
- **Medium**: Level with user risk scores ranging from 30 to 59
- **High**: Level with user risk scores ranging from 60 to 79
- **Critical**: Level with user risk scores ranging from 80 to 100

6. Define R**ule Expiration**:

a. **Enable Rule Expiration**: Enable this option to set a validity period for the rule.

b. **Start Date and Time**: Select a start date and time. The rule is valid starting on this date and time.

c. **End Date and Time**: Select an end date and time. The rule ceases to be valid on this date and time.

d. **Time Zone**: Select the time zone in which the rule should be valid.

7. Specify the **Action** for the Rule.

Policy Actions for Google Cloud Applications varies depending on the Cloud Application Category.

Allow:

- **Daily Bandwidth Quota**: (Optional) The bandwidth quota includes data uploaded to and downloaded from the cloud application. To enforce the quota on each location, do not select specific users, groups, or departments. To enforce the quota on specific users, groups, or departments, SSL inspection and authentication (government agencies, see SSL inspection and authentication) must be enabled. If a user comes from a known location (government agencies, see), the quota is reset at midnight based on the location time zone; for remote users, the quota is reset based on the organization's time zone. The minimum value you can enter is 10 MB and the maximum value is 100,000 MB.
- **Daily Time Quota**: (Optional) The time quota is based on the amount of time elapsed in a session while uploading and downloading data. The session idle times are ignored. The minimum value you can enter is 15 minutes and the maximum value is 600 minutes.
- **Uploading**: (Optional) Allow or block users from uploading files to the selected applications.
- **Creating**: (Optional) Allow or Block users from creating items on the selected applications
- **Deleting**: (Optional) Allow or Block users from deleting items on the selected applications.
- **Downloading**: (Optional) Allow or Block users from downloading files to the selected applications.
- **Editing**: (Optional) Allow or Block users from editing files on the selected application.
- **Form Sharing**: (Optional) Allow or Block users from sharing forms from the selected applications.
- **Renaming**: (Optional) Allow or Block users from renaming items on the selected applications.
- **Sharing**: (Optional) Allow or Block users from sharing files from the selected applications.

- **Tenant Profiles**: Appears only when Google Workspace Gmail or Google Drive is selected as the cloud application. You can select the tenant profiles for which you want to apply the rule. To learn more, see About Tenant Profiles (government agencies, see About Tenant Profiles).
- **SSL Inspection** is required for Tenant Profiles.

Caution:

- **Daily Bandwidth Quota**: (Optional) The bandwidth quota includes data uploaded to and downloaded from the cloud application. To enforce the quota on each location, do not select specific users, groups, or departments. To enforce the quota on specific users, groups, or departments, SSL inspection and authentication (government agencies, see SSL inspection and authentication) must be enabled. If a user comes from a known location, the quota is reset at midnight based on the location time zone; for remote users, the quota is reset based on the organization's time zone. The minimum value you can enter is 10 MB and the maximum value is 100,000 MB.
- **Daily Time Quota**: (Optional) The time quota is based on the amount of time elapsed in a session while uploading and downloading data. The session idle times are ignored. The minimum value you can enter is 15 minutes and the maximum value is 600 minutes.

Block:

- Choose to block the users from viewing and/or uploading content to the selected applications.

Isolate:

- Choose to isolate viewing the content on cloud applications through a remote browser for all the traffic that matches the cloud app control rule. To learn more, see What Is Isolation? (government agencies, see What Is Isolation?).
- **Isolation Profile**: Appears when you select Isolate. You can choose the isolation profiles to which the rule applies. to learn more about how to create isolation profiles (government agencies, see create isolation profiles).
- **Daily Bandwidth Quota**: (Optional) The bandwidth quota includes data uploaded to and downloaded from the cloud application. To enforce the quota on each location, do not select specific users, groups, or departments. To enforce the quota on specific users, groups, or departments, SSL inspection and authentication (government agencies, see SSL inspection and authentication) must be enabled. If a user comes from a known location, the quota is reset at midnight based on the location time zone; for remote users, the quota is reset based on the organization's time zone. The minimum value you can enter is 10 MB and the maximum value is 100,000 MB.
- **Daily Time Quota**: (Optional) The time quota is based on the amount of time elapsed in a session while uploading and downloading data. The session idle times are ignored. The minimum value you can enter is 15 minutes and the maximum value is 600 minutes.
- **Tenant Profiles**: Appears only when Gmail, Google Drive, or Google Photos is selected as the cloud application. You can select the tenant profiles for which you want to apply the rule. To learn more, see About Tenant Profiles (government agencies, see About Tenant Profiles).
- **Cascade to URL Filtering**: Enable if you want to enforce the URL Filtering policy on a transaction, even after it's explicitly allowed by the Cloud App Control policy. However, the URL Filtering policy doesn't apply if the Cloud App Control policy blocks the transaction. This field appears only when the Allow Cascading to URL Filtering option is disabled on the **Advanced Settings** page (**Administration** > **Advanced Settings**).

Send Attachments

- **Chatting**: Allow users to chat on the selected cloud applications, caution users with a notification before they can proceed, or block users.

8. (Optional) Define the notification settings:
   a. **Browser Notification Template**: Select a browser-based End User Notification (EUN) message from the drop-down menu to display the message on the browser when the user activity triggers the Cloud App Control Policy rule.
   b. **End User Notification**: Appears only when a tenant profile is selected. Select **Show** to show the Zscaler Client Connector-based EUN message on endpoints when the user activity triggers the Cloud App Control policy rule, or select **Hide** if you don't want an EUN message to appear. This field is set to **Show** by default.
      - Custom Message: Select a custom notification message that you want to show as the Zscaler Client Connector-based EUN. This field is set to the Default notification message if no message is selected from the drop-down menu.
9. (Optional) In the **Description** field, enter additional notes or information. The description cannot exceed 10,240 characters.
10. Click **Save** and activate the change.

Google Tenant Profiles

Zscaler's tenancy restriction feature allows you to restrict access either to personal accounts, business accounts, or both for certain cloud applications such as Google Workspace. It consists of two parts, creating tenant profiles and associating them with the Cloud App Control policy rules.

You can provide restricted access to the cloud applications that support tenancy restrictions by creating tenant profiles for these apps and associating them with the respective Cloud App Control policy rules. For example, you can restrict access to content specific to your organization on YouTube by creating a tenant profile, corporate YouTube channel with your organization's YouTube channel ID, and associating it to a YouTube Cloud App Control policy rule with Allow action.

To add a tenant profile:

1. Go to **Administration** > **Tenant Profiles**.
2. Click **Add Tenant Profile**. The **Add Tenant Profile** page appears.
3. In the **Applications** field, select one of the following Google applications and configure it accordingly:
   a. **YouTube**: To configure the tenant profile for YouTube, in the **YouTube Configuration** field, select one of the following configuration types:
      i. **YouTube Category ID**: Select the required categories from the following list of categories:
         - Action/Adventure
         - Anime/Animation
         - Autos & Vehicles
         - Classics
         - Comedy
         - Documentary
         - Drama
         - Education
         - Entertainment
         - Family
         - Film & Animation
         - Foreign

- Gaming
- Horror
- How to & Style
- Movies
- Music
- News & Politics
- Nonprofits & Activism
- People & blogs
- Pets & Animals
- Science & Technology
- Sci-fi/Fantasy
- Shorts
- Short Movies
- Shows
- Sports
- Thriller
- Trailers
- Travel & Events
- Videoblogging

ii. **YouTube Channel ID**: Enter the YouTube channel IDs (e.g., **UCSylwuqCXM_W13ARfzASm3Q**) you want to add to this tenant profile, and click **Add** Items.

- To enter multiple entries, press `Enter` after each entry, then click **Add** Items. You can add up to 200 YouTube channel IDs. To learn more, see **Ranges & Limitations** (government agencies, see **Ranges & Limitations**). For item lists, you can filter the list by searching for a word, phrase, or number contained in an item, and you can remove all items from the list (**Remove All**) or only items from a specific page (**Remove Page**). If you select **Remove All** or **Remove Page,** a confirmation window appears.

iii. **YouTube School ID**: Enter the IDs YouTube assigned to your school network (e.g., `UC1xagwHTcYzlpIriGARvPig`), which you want to add to this tenant profile, and click **Add Items**.

- To enter multiple entries, press `Enter` after each entry, then click **Add** Items. You can add up to 100 YouTube school IDs. To learn more, see **Ranges & Limitations** (government agencies, see **Ranges & Limitations**). For item lists, you can filter the list by searching for a word, phrase, or number contained in an item, and you can remove all items from the list (**Remove All**) or only items from a specific page (**Remove Page**). If you select **Remove All** or **Remove Page**, a confirmation window appears.

To learn more about associating tenant profiles of YouTube with the Cloud App Control policy rule, see **Adding a Streaming Media Rule for Cloud App Control** (government agencies, see **Adding a Streaming Media Rule for Cloud App Control**).

b. Google Apps: To configure the tenant profile for Google apps:

   i. In the **Domains** field, enter the domains (e.g., `www.zscaler.com`) you want to add to this tenant profile and click **Add Items**. To enter multiple entries, press `Enter` after each entry, then click **Add** Items. You can add up to 100 domains. To learn more, see **Ranges & Limitations** (government agencies, see **Ranges & Limitations**). For item lists, you can filter the list by searching for a word, phrase, or number contained in an item, and you can remove all items from the list (**Remove All**) or only items from a specific page (**Remove Page**). If you select Remove All or **Remove Page**, a confirmation window appears.

   ii. For the **Allow Consumer Access** field, select **Yes** to allow consumer access to the domains in the tenant profile. This field is set to **No** by default.

   iii. For the **Allow Visitor Access** field, select **Yes** to allow visitors access to the domains in the tenant profile. This field is set to **No** by default.

The service intercepts any google.com (or associated Google app) request and adds the HTTP header X-Google Apps-Allowed-Domains (values of the Domains field), which identifies the domains from which users can access Google services. This prevents users from accessing Gmail and other Google apps from other domains.

This feature does not affect Google apps that do not require users to sign in, such as Google search. But a user who signs in from Google search with an account that is not placed on the allowlist is blocked.

To learn more, refer to the Google documentation **here** and **here**.

To learn more about associating tenant profiles of Google apps with the Cloud App Control policy rule, see **Adding Rules to the Cloud App Control Policy** (government agencies, see **Adding Rules to the Cloud App Control Policy**).

Ensure to select these cloud applications as a criterion in an SSL Inspection rule if their tenant profiles are associated with a cloud application rule.

In the SSL Inspection rule, for the following cloud applications, select **Google Login Services** as the cloud application in **Google Apps**.

4. In the **Tenant Profile Name** field, enter a unique name for the tenant profile. This name is displayed while configuring the respective Cloud App Control policy rules.
5. **Description**: (Optional) Enter any additional comments or information. The description cannot exceed 10,240 characters.
6. Click **Save** and activate the change.

SaaS Security Posture Management (SSPM)

Zscaler SSPM Essentials and Advanced offer different levels of features and capabilities for securing SaaS applications. Essentials provides core security features like cyberthreat protection, data protection, and zero trust connectivity. Advanced goes further with a comprehensive approach, including data visibility, posture control, data governance, and the ability to identify and mitigate risky misconfigurations.

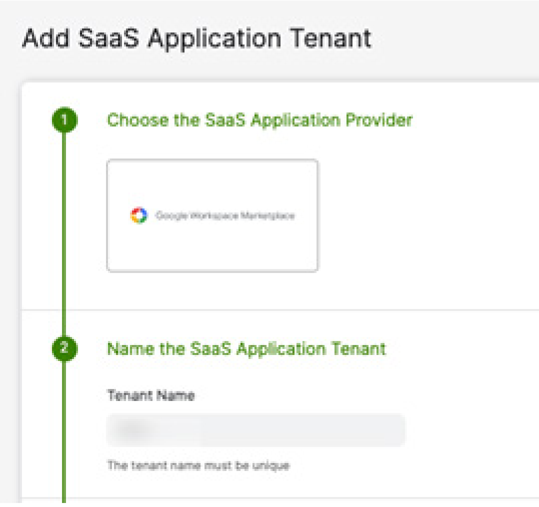
Zscaler SSPM Essentials Onboarding

The Zscaler service supports both Zscaler-defined and custom-defined onboarding connectors. Both supported API authorization capabilities are outlined in this deployment guide.

For more information about the Google Workspace Administration, see Google Workspace Admin Help.

Zscaler-Defined Connectors for SSPM Essentials

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **SaaS Application Tenants**.
3. Click **Add SaaS Application Tenant**.
4. Click **Google Market Place**.
5. In **Tenant Name**, enter a unique name.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

Google Workspace Marketplace

2 Name the SaaS Application Tenant

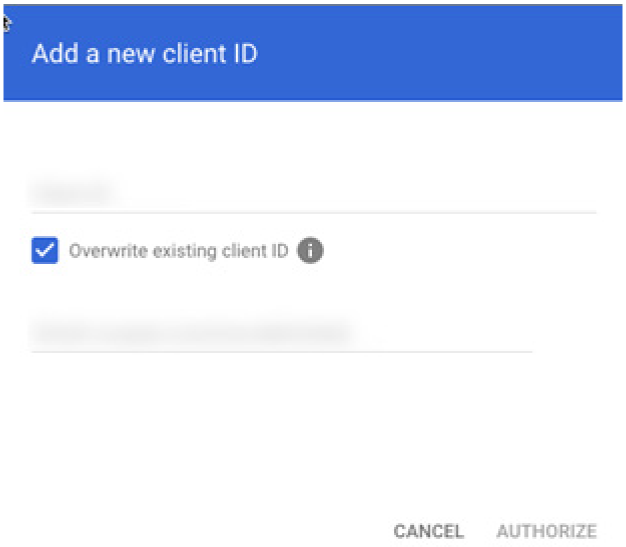
Tenant Name

The tenant name must be unique

Figure 12. Google Marketplace Tenant Configuration

6. Enter your **Google Admin Email ID**.
7. Under **Authorize the SaaS Application**, select **Zscaler Defined**, and copy the **Zscaler SaaS Connector** and **Google Workspace Scope**. You need it for a later step when adding an API client for Google Workspace.
8. Click **Go to Google Workspace**. The **Google Workspace** portal appears.
9. Log in to **Google Workspace**.
10. Go to **Access and data control** > **Security**.
11. Click **API controls**.
12. Under **Domain wide delegation**, click **Manage Domain Wide Delegation**.
13. Click **Add new**. The **Add a new client ID** window appears.

14. In the **Add a new client ID** window:
    - **Client ID**: Enter the Zscaler SaaS Connector value.
    - **Overwrite existing client ID**: Deselect.
    - **OAuth scopes (comma-delimited)**: Enter the Google Workspace scope.
    - Click **Authorize**. The Zscaler Connector App is added as an API client.



Add a new client ID

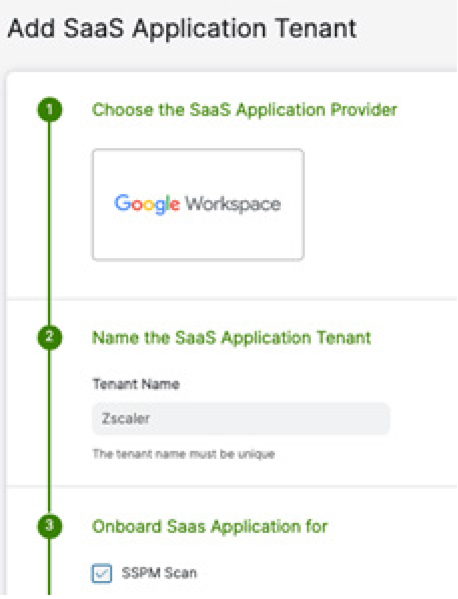
☑ Overwrite existing client ID

Figure 13. Authorize

15. (Optional) Under **Configure External Trusted Domains & Users for the Tenant**:
    - **External Trusted Domains**: Enter trusted email domains that are outside your organization (i.e., using a different domain). The Zscaler service views any email addresses from the added domains as trusted, internal users for Gmail. For example, if your organization's domain is safemarch.com and your organization recently acquired a company with the domain example.com, you can add example.com to this list, and the service treats any email addresses from example.com (e.g., johnsmith@example.com) as internal users from safemarch.com. You can add up to 1,000 domains.
    - **External Trusted Users**: Enter trusted email addresses that are outside your organization (i.e., using a different email domain). The Zscaler service views the email addresses as trusted, internal users for Gmail. For example, if your organization's email domain is safemarch.com and your organization recently contracted with someone using an external email domain (e.g., johnsmith@example.com), you can add the contractor's email to this list, and the service treats the contractor as an internal user from safemarch.com. You can add up to 1,000 email addresses.

Google Workspace

1. Log in to the ZIA Admin Portal.
2. Go to **Administration** > **SaaS Application Tenants**.
3. Click **Add SaaS Application Tenant**.
4. Click **Google Workspace**.
5. In **Tenant Name**, enter a unique name.
6. In **Onboard SaaS Application for**, select the **SSPM Scan** checkbox.



Add SaaS Application Tenant

1 Choose the SaaS Application Provider

Google Workspace

2 Name the SaaS Application Tenant

Tenant Name

Zscaler

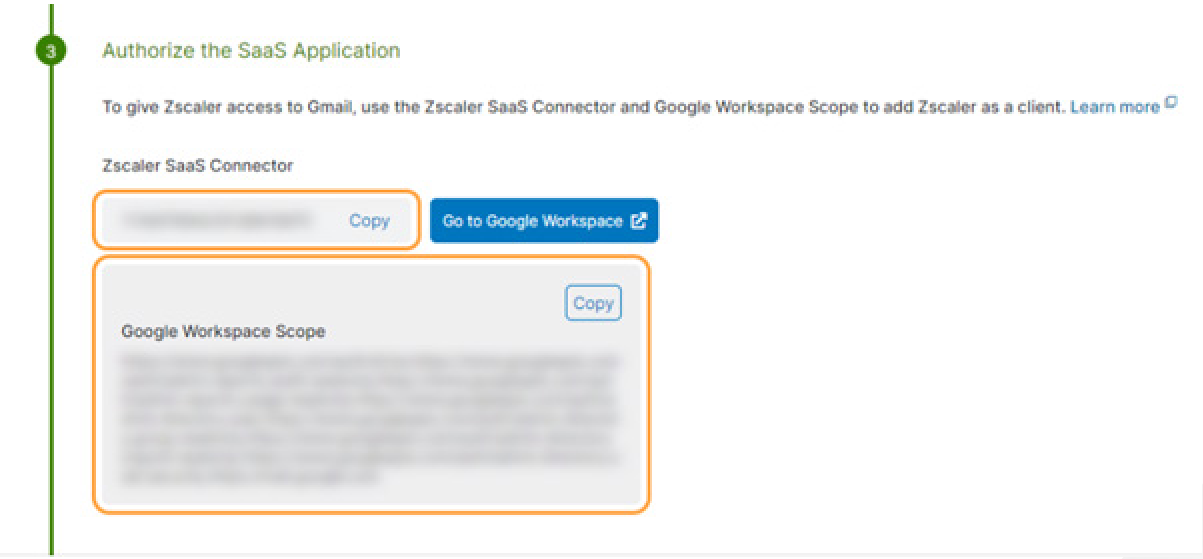
The tenant name must be unique

3 Onboard Saas Application for

☑ SSPM Scan

Figure 14. Zscaler Google Workspace Defined

7. Enter your **Google Admin Email ID**.
8. Under **Authorize the SaaS Application**, select **Zscaler Defined**, copy the **Zscaler SaaS Connector** and **Google Workspace Scope**. You need it for a later step when adding an API client for Google Workspace.



3 Authorize the SaaS Application

To give Zscaler access to Gmail, use the Zscaler SaaS Connector and Google Workspace Scope to add Zscaler as a client. Learn more

Zscaler SaaS Connector

[redacted] Copy

Go to Google Workspace

Google Workspace Scope

Copy

[redacted]

Figure 15. Authorize SaaS APP

9. Click **Go to Google Workspace**. The **Google Workspace** portal appears.
10. Log in to **Google Workspace**.
    a. Go to **Access and data control** > **Security**.
    b. Click **API controls**.
    c. Under **Domain wide delegation**, click **Manage Domain Wide Delegation**.
    d. Click **Add new**.

To learn more about SSPM Essentials, see [Viewing and Managing the Supported SSPM Policies]() (government agencies, see [Viewing and Managing the Supported SSPM Policies]()).

11. In the **Add a new client ID** window:
    - **Client ID**: Enter the Zscaler SaaS Connector value.
    - **Overwrite existing client ID**: Deselect.
    - **OAuth scopes (comma-delimited)**: Enter the Google Workspace scope.
    - Click **Authorize**. The Zscaler Connector App is added as an API client.

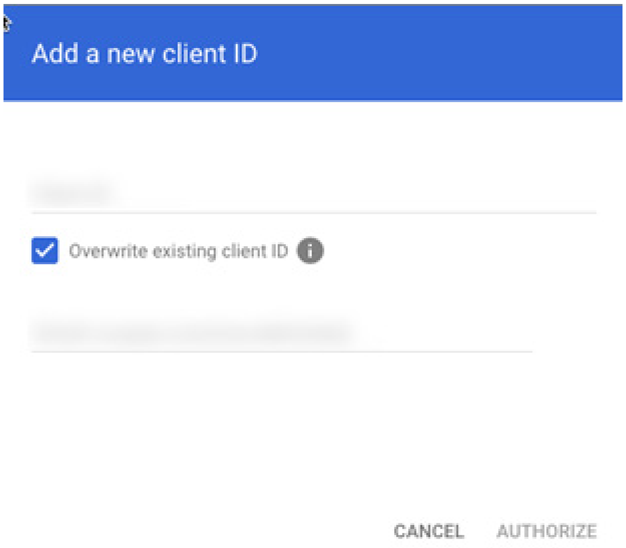


Figure 16. Authorize

Zscaler SSPM Advanced Onboarding for Google Workspace

If you subscribed to the Advanced SSPM service, you can access Advanced SSPM from the ZIA Admin Portal using single sign-on (SSO). To access Advanced SSPM from the ZIA Admin Portal, go to **Analytics** > **SaaS Security** > **Posture Management**, or **Policy** > **SaaS Security** > **Posture Management**.

1. Log in to the ZIA Admin Portal, go to **Analytics** > **Posture Management or Policy** > **SaaS Security** > **Posture Management**.
2. Click **Connect** in the left-side navigation. The **Integrations** window appears.
3. In the **Integrations** window, click **Add** next to **Google Workspace**. You are prompted to sign in if you haven't already done so.
4. A consent window appears, displaying all privileges as read-only, and you can view a detailed list of permissions and data here.

This consent step only allows reading of the apps in your workspace. Additional consent steps are required for the revocation and banning of apps. By default, third-party app governance users who are not explicitly granted revocation rights are unable to perform revoke operations.

5. After connection is achieved, it might take a while to pull and ingest all relevant application data depending on the size of your tenant. During this time, a message is displayed that the domain is being processed. After integration is completed, a success message appears, and the number of domains is updated. You then receive an email from Zscaler when the domain is ready for further review.

To learn more about SSPM Advanced, see What is Advanced Posture Management (government agencies, see What is Advanced Posture Management).

Google Marketplace

Google Marketplace integrations enables Zscaler to discover, allow, and block third-party SaaS applications authenticated via a corporate Google account in the ZIA Admin Portal after adding Google Workspace Marketplace as a tenant.

To learn more, see **About the 3rd-Party App Governance Report** (government agencies, see **About the 3rd-Party App Governance Report**).

Appendix A: API/OAuth Permissions for Google Applications

When creating custom connectors, provide the following application-specific API permissions to ensure that the Zscaler service has the access it needs.

Gmail

Google Permission	Associated Zscaler Actions
https://www.googleapis.com/auth/pubsub	Scanning
https://www.googleapis.com/auth/admin.directory.user	Scanning
https://www.googleapis.com/auth/admin.reports.audit.readonly	Scanning, Reporting
https://mail.google.com/	Scanning, Apply Label
https://www.googleapis.com/auth/admin.reports.usage.readonly	Scanning
https://www.googleapis.com/auth/admin.directory.user.security	Scanning
https://www.googleapis.com/auth/admin.directory.group.readonly	Scanning
https://www.googleapis.com/auth/admin.directory.orgunit.readonly	Scanning

Google Cloud Platform

Google Permission	Associated Zscaler Actions
iam.roles.get	Validation
iam.roles.list	Validation
storage.buckets.get	Onboarding, Scanning
storage.buckets.list	Onboarding, Scanning
storage.objects.get	Scanning
storage.objects.list	Scanning
resourcemanager.projects.get	Onboarding, Scanning
resourcemanager.projects.getIamPolicy	Onboarding, Scanning
resourcemanager.folders.get	Onboarding
resourcemanager.folders.getIamPolicy	Onboarding
resourcemanager.folders.list	Onboarding
resourcemanager.organizations.get	Validation
resourcemanager.organizations.getIamPolicy	Validation
storage.objects.getIamPolicy	Scanning
storage.buckets.getIamPolicy	Onboarding, Scanning
logging.logEntries.list	Scanning, Reporting
logging.privateLogEntries.list	Scanning, Reporting

Read Role + Web Hooks

Google Permission	Associated Zscaler Actions
iam.roles.get	Validation
iam.roles.list	Validation
storage.buckets.get	Onboarding, Scanning
storage.buckets.list	Onboarding, Scanning

Google Permission	Associated Zscaler Actions
storage.objects.get	Scanning
storage.objects.list	Scanning
resourcemanager.projects.get	Onboarding, Scanning
resourcemanager.projects.getIamPolicy	Onboarding, Scanning
resourcemanager.folders.get	Onboarding
resourcemanager.folders.getIamPolicy	Onboarding
resourcemanager.folders.list	Onboarding
resourcemanager.organizations.get	Validation
resourcemanager.organizations.getIamPolicy	Validation
storage.objects.getIamPolicy	Scanning
storage.buckets.getIamPolicy	Onboarding, Scanning
logging.logEntries.list	Scanning, Reporting
logging.privateLogEntries.list	Scanning, Reporting
pubsub.subscriptions.create	Scanning, Reporting
pubsub.subscriptions.delete	Scanning, Reporting
pubsub.subscriptions.get	Scanning, Reporting
pubsub.topics.attachSubscription	Scanning, Reporting
pubsub.topics.create	Scanning, Reporting
pubsub.topics.setIamPolicy	Scanning, Reporting
pubsub.topics.delete	Scanning, Reporting
pubsub.topics.getIamPolicy	Scanning, Reporting
pubsub.topics.get	Scanning, Reporting
pubsub.subscriptions.update	Scanning, Reporting

Read/Write Role

Google Permission	Associated Zscaler Actions
iam.roles.list	Validation
logging.sinks.get	Reporting
storage.buckets.get	Onboarding, Scanning
storage.buckets.list	Onboarding, Scanning
storage.objects.get	Scanning
storage.objects.list	Scanning
resourcemanager.projects.get	Onboarding, Scanning
resourcemanager.projects.getIamPolicy	Onboarding, Scanning
resourcemanager.folders.get	Onboarding
resourcemanager.folders.getIamPolicy	Onboarding
resourcemanager.folders.list	Onboarding
resourcemanager.organizations.get	Validation
resourcemanager.organizations.getIamPolicy	Validation
storage.objects.getIamPolicy	Scanning
storage.buckets.getIamPolicy	Onboarding, Scanning
logging.logEntries.list	Scanning, Reporting

Google Permission	Associated Zscaler Actions
logging.privateLogEntries.list	Scanning, Reporting
storage.objects.setIamPolicy	Policy action
storage.objects.update	Policy action
storage.objects.create	Policy action
storage.objects.delete	Policy action
storage.buckets.update	Policy action
storage.buckets.setIamPolicy	Policy action
pubsub.subscriptions.create	Scanning, Reporting
pubsub.subscriptions.delete	Scanning, Reporting
pubsub.subscriptions.get	Scanning, Reporting
pubsub.topics.attachSubscription	Scanning, Reporting
pubsub.topics.create	Scanning, Reporting
pubsub.topics.setIamPolicy	Scanning, Reporting
pubsub.topics.delete	Scanning, Reporting
pubsub.topics.getIamPolicy	Scanning, Reporting
pubsub.topics.get	Scanning, Reporting
pubsub.subscriptions.update	Scanning, Reporting

Google Drive

Google Permission	Associated Zscaler Actions
https://www.googleapis.com/auth/admin.directory.user	Scanning
https://www.googleapis.com/auth/drive	Scanning, Policy Actions
https://www.googleapis.com/auth/admin.reports.audit.readonly	Scanning
https://www.googleapis.com/auth/admin.reports.usage.readonly	Scanning, Reporting
https://www.googleapis.com/auth/admin.directory.user.security	Scanning
https://www.googleapis.com/auth/admin.directory.group.readonly	Scanning
https://www.googleapis.com/auth/admin.directory.orgunit.readonly	Scanning
https://www.googleapis.com/auth/drive.admin.labels	Apply Label

Google Workspace

Google Permission	Associated Zscaler Actions
https://www.googleapis.com/auth/admin.directory.user	Scanning
https://www.googleapis.com/auth/drive	Scanning
https://www.googleapis.com/auth/admin.reports.audit.readonly	Scanning
https://www.googleapis.com/auth/admin.reports.usage.readonly	Scanning
https://mail.google.com/	Scanning
https://www.googleapis.com/auth/admin.directory.user.security	Scanning
https://www.googleapis.com/auth/admin.directory.group.readonly	Scanning
https://www.googleapis.com/auth/admin.directory.orgunit.readonly	Scanning
https://www.googleapis.com/auth/gmail.settings.sharing	Remediation
https://www.googleapis.com/auth/gmail.settings.basic	Remediation

Appendix B: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

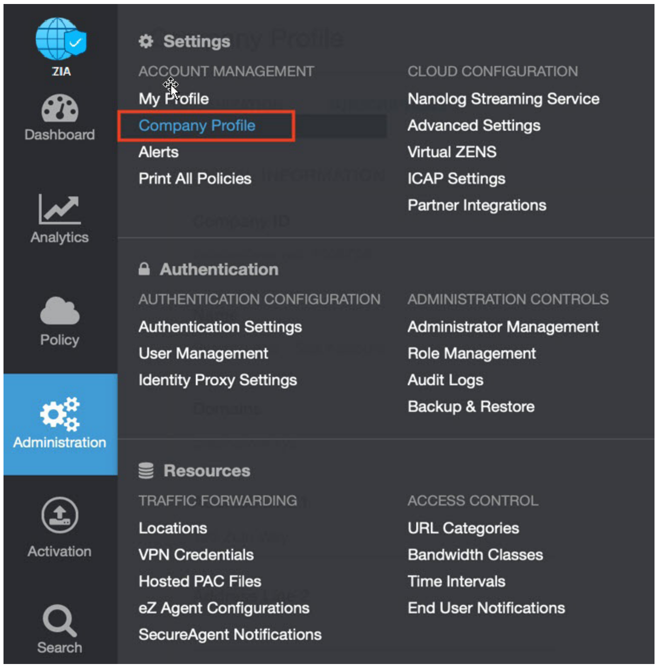
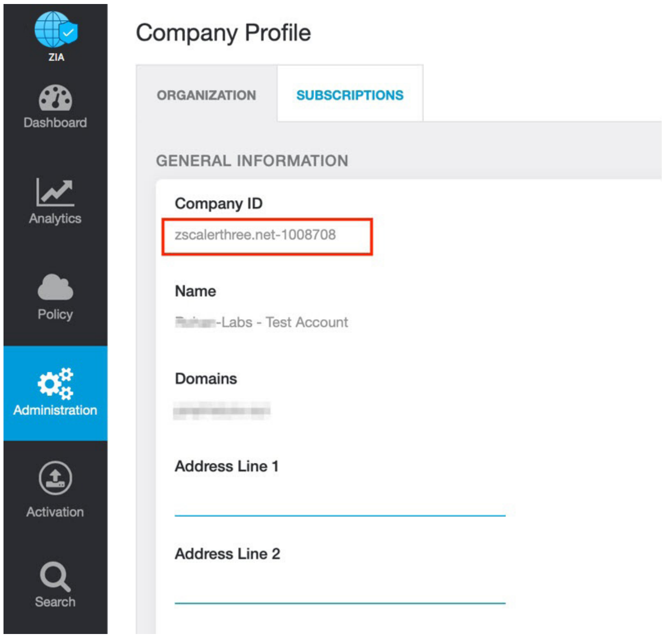


Figure 17. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.



Company Profile

GENERAL INFORMATION

Company ID
zscalerthree.net-1008708

Name
[redacted]-Labs - Test Account

Domains
[redacted]

Address Line 1

Address Line 2

Figure 18. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

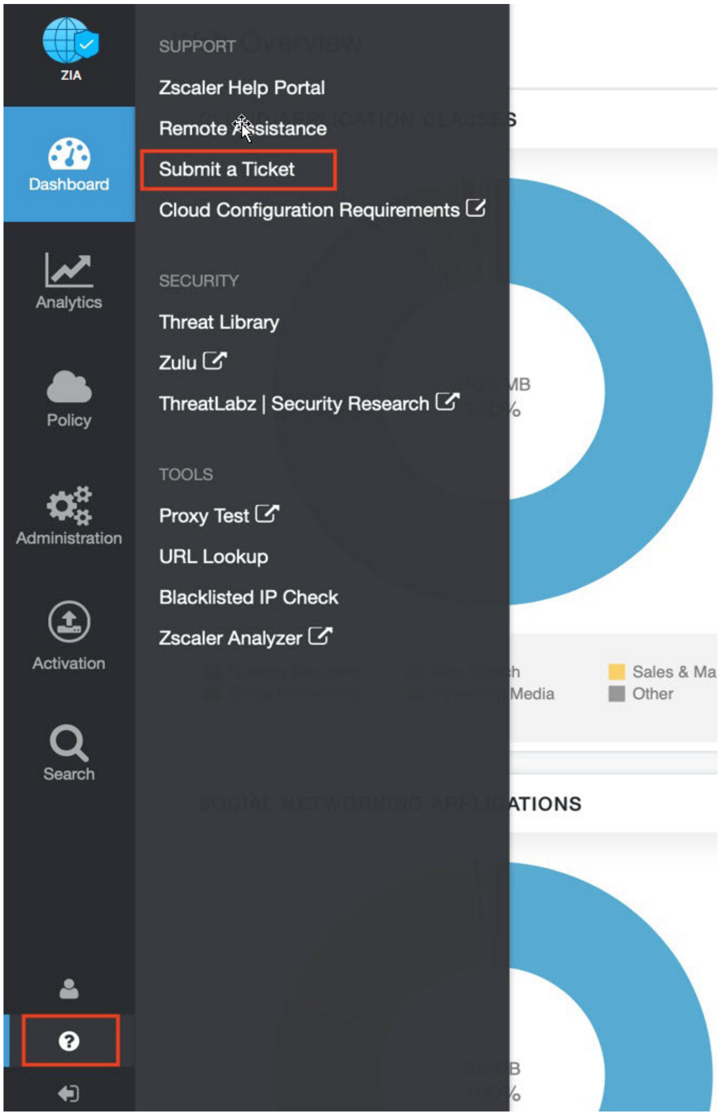


Figure 19. Submit a ticket