Prisma SaaS Administrator's Guide

paloaltonetworks.com/documentation

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 8, 2019

Table of Contents

Get Started with Prisma SaaS

As you transition your sanctioned IT applications into the cloud, you increase the risk of compromising sensitive data and propagating malware. Prisma SaaS analyzes the data in your sanctioned software-as-a-service (SaaS) applications and performs policy-driven analysis so you can proactively detect issues and remediate them.

Prisma SaaS is a cloud-based service you can connect directly to your sanctioned SaaS applications using the API and provide data classification, sharing/permission visibility, and threat detection within the application. It provides complete insight into all user, folder, and file activity to help you determine if you are at risk for any data exposure or compliance-related policy violations.

Prisma SaaS

Prisma SaaS connects to your sanctioned SaaS application using the SaaS application's API. This API integration allows the service to discover and scan all assets retroactively when you first connect the SaaS application. Prisma SaaS scans and analyzes all your assets and applies policy to identify exposures, external collaborators, risky user behavior, and sensitive documents and identifies the potential risks associated with each asset. The service also performs deep content inspection and protects both your historical assets and new assets from malware, data exposure, and data exfiltration. As the service identifies incidents, you can assess them and define automated actions to eliminate or close the incident. After the initial scan of your historical assets, Prisma SaaS continuously monitors each SaaS application and applies policy against new or modified assets for ongoing incident assessment and protection.

To provide visibility into the security challenges with data classification and governance, security gaps owing to non-compliance, sharing/permission violations, and malware propagation within the sanctioned cloud applications on your network, Prisma SaaS focuses on the following key areas:

- **Content Security**— The content you store in each cloud application is an asset. Prisma SaaS provides visibility into your asset inventory to help you uncover accidental or malicious data exposure. Prisma SaaS discovers the assets residing in the cloud application, assesses the shared or exposed data within and outside your organization, and identifies the impact or risk to intellectual property and regulatory non-compliance. In addition to creating an incident and alerting the administrator, the service provides auto-remediation capabilities, including the option to quarantine, change sharing, or notify the owner.
- **User Activity Monitoring**—The service uses a combination of tools including machine language learning, predefined and user-defined data patterns, security configuration controls, and access to event logs auditing user access and activity on each cloud application. With these tools, it builds context on sensitive data within your environment, identifies thresholds for expected and unexpected behavior, and uses this intelligence to log a violation or alert you to risky user behavior and possible data leaks from accidental or malicious user activity.
- **Security Configuration Controls**—Prisma SaaS provides policies allowing you to manage and restrict privileged user activity, email forwarding, and retention rules, and protects you from misconfigurations such as lack of storage volume encryption, lack of enforcement for securing keys, credentials, and Multi-Factor Authentication. When any of these security issues occur, you can configure the service to generate an alert or log it as a policy violation.
- **Third-Party App Integrations**—Threats from third-party apps are serious because these apps have access to all or a large part of the data in the related cloud app. Protect your users and network from misconfigurations and known and unknown malware arising from these app integrations with a service that gives you the ability to approve, block, or restrict third-party app installation.

Prisma SaaS License Types

The following license types are available for Prisma SaaS:

- **Prisma SaaS All Apps License**—The All Apps license is a user-based license which grants one user the right to use Prisma SaaS to secure SaaS applications. A Prisma SaaS All Apps license is term-based at one or three years and has the capabilities to protect your sanctioned SaaS apps by:
- • Discovering cloud resources for over 20 SaaS apps.

  The service automatically scans your cloud apps using predefined data patterns, classifies all documents using machine learning, and checks hash on all Microsoft Office documents, PDF, and portable executable files against WildFire rules without requiring you to create any policies.
  - Monitoring for risky or suspicious user or admin behavior.

    You can review user activity logs enabling you to monitor and investigate the actions of your end users on the data and assets stored in your apps. You can track events, such as file and folder

downloads and uploads as well as failed login attempts, or you can learn how a user shared or collaborated on assets hosted in your SaaS applications.

- Providing advanced data classification.

  When you configure data classification labels for the files in your third-party apps you can control data sharing and prevent data exfiltration.
- Enforcing policy against security misconfigurations.

  Policy allows you to monitor and enforce responsible use of assets and protect them from malware, malware propagation and data leaks.
- Preventing malware propagation by scanning files using WildFire analysis.

  WildFire detects and protects against malicious portable executables, Microsoft Office Files, Adobe Portable Document Format (PDF) files, and known threats based on file hash (a unique fingerprint of a file as a result of running the file through a cryptographic hash function).
- Providing machine learning algorithms.

  Prisma SaaS uses supervised machine learning algorithms to sort sensitive documents into Financial, Legal and Healthcare categories for document classification to guard against exposures, data loss and data exfiltration.

  To improve detection rates for the sensitive data in your organization, you can define the machine learning data pattern match criteria to identify the sensitive information in your cloud apps and protect them from exposure.

- **Public Cloud Storage License**—This volume-based license helps you gain bucket and blob visibility and control for your AWS, Azure, and Google Cloud Storage and is term-based at one or three years. You can identify and remove public buckets and blobs from inadvertent exposure or use, prevent the propagation of malware and data exfiltration with advanced machine learning and DLP, and view an audit trail for stored buckets and blobs to detect anomalies.
- —Prisma SaaS licenses include a premium support entitlement.

Set Up Prisma SaaS on the Hub

Setting up Prisma SaaS on the Palo Alto Networks hub is simple. With your Palo Alto Networks Customer Support Portal (CSP) credentials, you can seamlessly switch between the Prisma SaaS app and other Palo Alto Networks apps on the hub, request support, and open a support case if needed.

Use the instructions below to set up the Prisma SaaS app on the hub. After the set up is complete, you can log in to Prisma SaaS, add your sanctioned SaaS applications, and configure policy to suit your needs for SaaS visibility and granular enforcement across all user, folder, and file activity within the managed SaaS applications.

The welcome email that you receive when you purchase Prisma SaaS includes an auth code. Unlike other apps, this auth code is automatically activated for you and Prisma SaaS is ready for set up. Please disregard the auth code in the email.

STEP 1 | Setup Prisma SaaS on the hub.

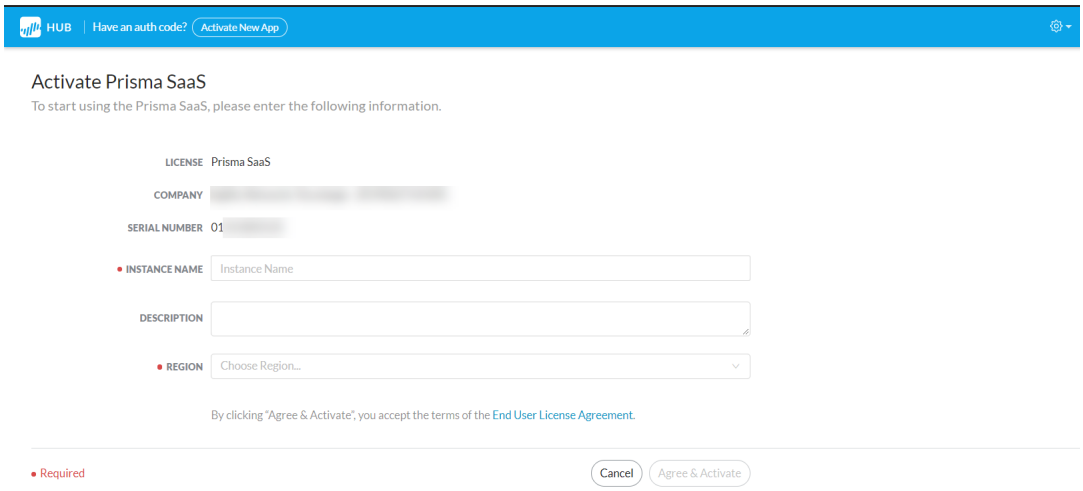
1. Log in to the hub.

   After the order fulfillment has completed, log in to the hub using your Palo Alto Networks Customer Support Portal (CSP) credentials.
2. Select the Prisma SaaS tile.

   If you don't see the tile, see Don't See the Prisma SaaS Tile on the Hub.

   The Prisma SaaS app is activated and ready for set up. Attempting to activate the auth code displays an error.

3. Enter an **Instance Name** to identify this app instance, and provide an optional **Description**.
4. Select the Prisma SaaS instance deployment **Region**.
5. Read the EULA and **Agree & Activate**.



STEP 2 | Access Prisma SaaS.

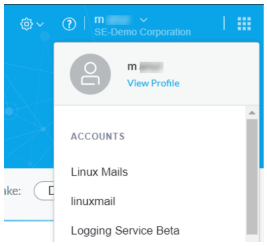
Your instance should be ready for you in approximately 30 minutes, and the Prisma SaaS support license is automatically activated for you.

Don't See the Prisma SaaS Tile on the Hub

If you do not see the Prisma SaaS tile when you log in to the hub using your Palo Alto Networks Customer Support Portal (CSP) credentials, check for the following:

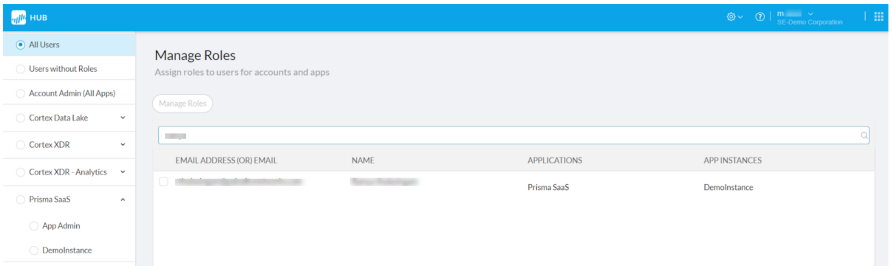
- Are you logged in to the correct account?

  Click on your name in the top right corner and verify the account name associated with your current login credentials. If not, select the correct account from the list.



- Do you have the permissions/role to set up the Prisma SaaS app?

  Only the Prisma SaaS administrator who was assigned during the order fulfillment process or the Account administrator has the correct permissions to set up Prisma SaaS app. Check that you have access to either Prisma SaaS or All Apps.



- Do you see the Prisma SaaS tile but it is on a different CSP account?

  Please call Palo Alto Networks Customer support to help you move the Prisma SaaS tile to the desired CSP account. You will need to be the account administrator to make the request.

Access Prisma SaaS

To start securing your sanctioned SaaS applications, begin by logging in to the Prisma SaaS service.

STEP 1 | Log in to Prisma SaaS.

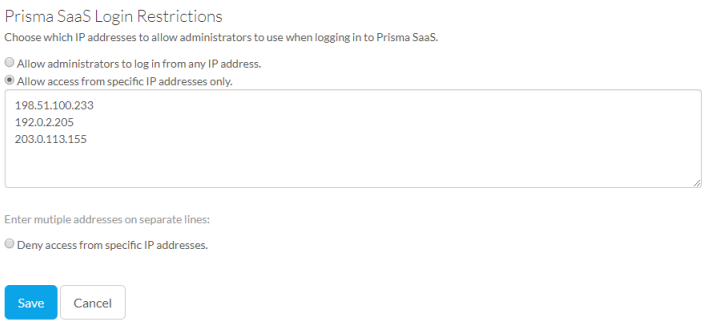
- If you have activated the Prisma SaaS app on the hub, sign in to the hub and select Prisma SaaS.
- If not, directly access the Prisma SaaS service. The URL format is https://<*your_company_name*>.aperture.paloaltonetworks.com.

STEP 2 | Restrict the IP addresses administrators can log in from.

For example, allow administrators to access Prisma SaaS only from corporate IP addresses or subnets.

You can add login restrictions using only IPv4 addresses; you can use dotted decimal (255.255.0.0) or CIDR notation (/16) to specify subnet masks.

1. Select **Settings** > **General Settings**.
2. Specify an IP address you will allow or deny Prisma SaaS administrative access from:
   - To restrict access to only one or a group of IP addresses, select **Allow access from specific IP addresses only** and add the IPv4 address(es), one address or subnet per line.



   - To block access only from one or a group of addresses, select **Deny access from specific IP addresses only** and add the addresses you want to block, one address or subnet per line.
3. **Save** your changes.

STEP 3 | Add Prisma SaaS Administrators.

Manage Prisma SaaS Administrators

To resolve incidents identified by Prisma SaaS, you must be able to understand the content and the context around each incident to determine if the incident poses a threat to sensitive data or intellectual property. Depending on the size of your organization, the number of SaaS applications you manage, and the total number of managed assets and users, you can create more than one administrative account with access to manage all cloud apps or an team administrator to manage a group of apps on Prisma SaaS.

For example, you can delegate risks found in financial documents to the team administrator of the Box folder for your finance department and delegate risks in your GitHub repository to the GitHub administrator in your engineering department without giving them access to every cloud app. If your administrator role has access to all SaaS applications, you can assign incidents to the appropriate administrator to resolve, either manually or by configuring automated remediation in the affected policy.

- Add Prisma SaaS Administrators
- Select an Authentication Method
- Reset Administrator Authentication
- Reset Administrator Password
- Unblock an Administrator
- View Administrator Activity Logs
- Create Prisma SaaS Teams (Beta)

Add Prisma SaaS Administrators

Initially, to create new administrator accounts on Prisma SaaS, log in as the administrator with the *Super Admin* role, which is the role assigned to the user specified in the order fulfillment email. With the Super Admin role, you can create additional administrator accounts, assign administrator roles, and create teams.

As an admin of a team, you can create other admin accounts with access to the SaaS applications assigned to your team but only a Super Admin role can create other Super Admin accounts. You do not need to create administrator accounts for end users who use the application to create or share content within each SaaS application.

With Prisma SaaS, if you add an administrator with an email that already exists in Customer Support Portal, their Prisma SaaS account will be linked to their CSP account. If you add an administrator with an email that does not exist in CSP, then an account will be created for them on Prisma SaaS, as well as an account in CSP tied to your organization.

STEP 1 | Select **Settings** > **Admin Accounts** and **Add Administrator**.

STEP 2 | Enter the **Name** and **Email** address of the new administrator.

STEP 3 | Choose an **Authentication Type**:

- Single Sign-On (SSO)—SAML SSO authentication enables you to grant admin access with seamless authentication using a single set of credentials. This option eliminates the need for application or service specific passwords. Configure SAML Single Sign-On (SSO) Authentication to activate this option. If you enable SSO, you do not have to create administrator accounts on the local database.
- Local Authentication— You can select Configure Google Multi-Factor Authentication (MFA) to grant admin access only after successfully presenting a pass code pair or QR barcode as evidence (additional factor) to authenticate to Prisma SaaS.

Local authentication is not supported for Prisma SaaS activated on the hub.

STEP 4 | Select the administrative **Role**:

You can select any of the following predefined roles, or you can Add a Custom Admin Role for enabling more granular access to the functional areas of Prisma SaaS. See Predefined Role Privileges for the list of functional areas configured for each predefined role.

- **Super Admin**—A read-write administrator account that allows full functionality within Prisma SaaS, including global account settings, creating administrator accounts, and assigning administrator roles.
- **Admin**—A read-write administrator account that allows full functionality within Prisma SaaS, including the ability to automatically or manually remediate risks and create additional administrator accounts.
- **Incident Management Admin**—An administrator account that allows granular access to investigate and remediate incidents only.
- **Limited Admin**—An administrator account that allows the administrator to assess incidents and remediate risks. This administrator cannot access Prisma SaaS settings or modify policy rules.
- **Read Only**—An administrator account that allows the administrator to view information collected by Prisma SaaS and generate reports but does not allow the administrator to make changes. For example, this administrator can access incidents, but cannot remediate risks.
- **Custom Role**—An administrator account with custom permissions to allow specific management tasks that meet your organizational needs.

STEP 5 | Select the **Team** to assign the administrator to.

If you have not created any custom teams, assign the administrator to the predefined **All Apps** team.

STEP 6 | Select the default **Language** for the new administrator.

STEP 7 | **Save** your changes.

To verify the role associated with administrator, search using the email address. You can also download a CSV file to view the complete list of all administrative users configured on Prisma SaaS.

Add a Custom Admin Role

If you want to define more granular access privileges than what the predefined roles provide, you can add custom admin roles. Custom roles allow you choose the privileges associated with the role so that you can to restrict access to specific pages or actions on Prisma SaaS. When you then assign the role to an administrator, they inherit the privileges associated with the role.

The easiest way to create a custom role is to clone a predefined role, such as the Limited Admin role, and modify it to enable the access privileges for the interface elements that you want to allow for the administrator.

STEP 1 | Select **Settings** > **Roles** and **Add a New Role**.

You can create up to 50 custom roles. If you'd like to clone a predefined role, pick a predefined role, and select **Actions** > **Clone**.

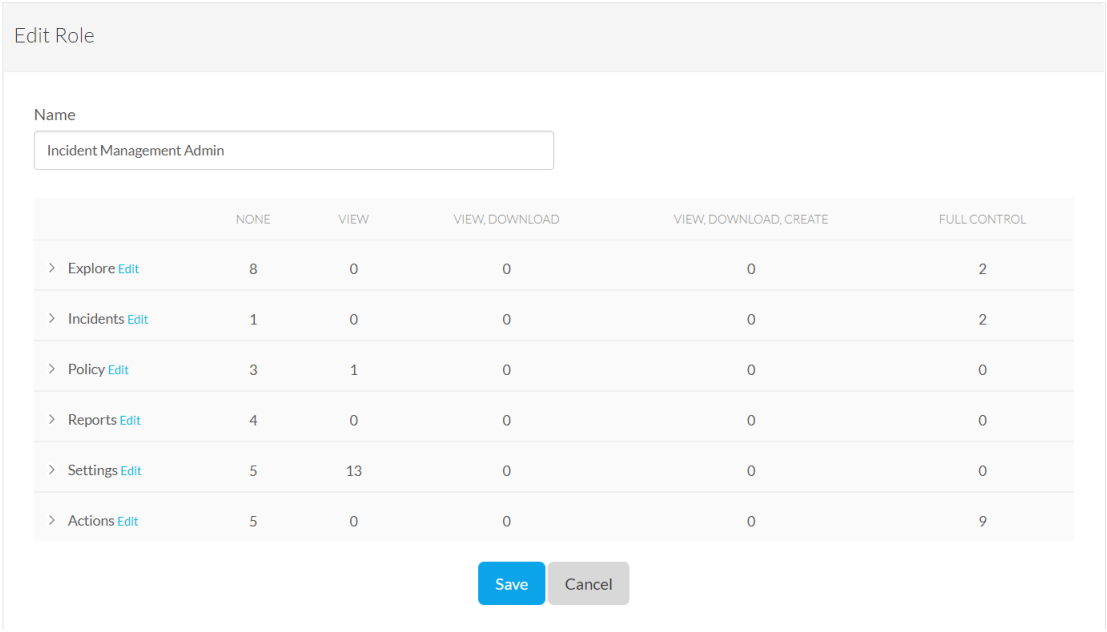
STEP 2 | Enter the **Name** for the new custom role.

STEP 3 | **Edit** the category—Explore, Incidents, Policy , Reports , Settings , Actions—for which you want to modify access privileges.

For each interface element within a category, you can pick from the following options where applicable:

- None—No access to the page.
- View— Can view data on the pages.
- View, Download—Can download snippets, CSV reports, and PDF reports, in addition to viewing data.
- View, Download, Create—Can create configuration elements such as policies, data patterns and signatures.
- Full Control—Can access and modify everything on the interface. Giving full control is equivalent to creating a Super Admin.

After you make a selection, minimize the category to view the total count for each option.



STEP 4 | **Save** your changes.

Predefined Role Privileges

The following table lists the access privileges that match each predefined role:

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
Explore					
Assets	Incident Management Admin	Read Only Limited Admin			Super Admin Admin

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
Asset Details		Read Only Limited Admin			Super Admin Admin Incident Management Admin
Snippets		Read Only Limited Admin			Super Admin Admin Incident Management Admin
People	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Domains	Incident Management Admin	Admin (Team) Read Only Limited Admin			Super Admin Admin (All Apps)
Activities	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Third-Party Apps	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Policy Violation	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Security Controls	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
SaaS Visibility	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Incidents					

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
Assets		Read Only Limited Admin			Super Admin Admin Incident Management Admin
Security Controls	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Quarantine		Read Only Limited Admin			Super Admin Admin Incident Management Admin
Policy					
Asset Rules		Read Only Limited Admin Incident Management Admin			Super Admin Admin
User Activity Rules	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Security Controls Rules	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Third-Party Apps Policy	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Reports					
SaaS Risk Assessment Report	Incident Management Admin	Read Only Limited Admin			Super Admin Admin

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
Remediation Activity Logs	Incident Management Admin	Read Only, Limited Admin			Super Admin Admin
GDPR Report	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Settings					
Cloud Apps & Scan Settings		Admin (Team) Read Only Limited Admin Incident Management Admin			Super Admin Admin (All Apps)
Data Patterns		Read Only Limited Admin Incident Management Admin			Super Admin Admin
Machine Learning Categories		Admin (Team) Read Only Limited Admin Incident Management Admin			Super Admin Admin (All Apps)
WildFire Analysis		Admin (Team) Read Only Limited Admin			Super Admin Admin (All Apps)

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
		Incident Management Admin			
Third-Party Classification	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
General Settings		Admin (Team) Read Only Limited Admin Incident Management Admin			Super Admin Admin (All Apps)
External Collaborators		Admin (Team) Read Only Limited Admin Incident Management Admin			Super Admin Admin (All Apps)
Authentication		Read Only Limited Admin Incident Management Admin Incident Management Admin			Super Admin Admin
Admin Accounts		Admin (Team) Read Only Limited Admin			Super Admin Admin (All Apps)

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
		Incident Management Admin			
Roles		Admin Read Only Limited Admin Incident Management Admin			Super Admin
Teams		Admin Read Only Limited Admin Incident Management Admin			Super Admin
Activity Logs	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
License Info		Read Only Limited Admin Incident Management Admin			Super Admin Admin
External Service	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Directory Service		Read Only Limited Admin Incident Management Admin			Super Admin Admin

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
SAML Proxy	Incident Management Admin	Read Only Limited Admin			Super Admin Admin
Email Templates		Read Only Limited Admin Incident Management Admin			Super Admin Admin
Remediation Email Digest		Read Only Limited Admin Incident Management Admin			Super Admin Admin
SaaS Visibility	Read Only Limited Admin	Incident Management Admin			Super Admin Admin
Actions					
Request Snippet	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Add Note	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Send Email	Read Only				Super Admin Admin Limited Admin Incident Management Admin

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
Quarantine Actions (Delete, Restore and Download)	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Quarantine a File	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Asset Change Sharing	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Apply Classification	Read Only Incident Management Admin				Super Admin Admin Limited Admin
Notify via Slack bot	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Edit Super Admin	Read Only Admin Limited Admin Incident Management Admin				Super Admin
Delete Super Admin	Read Only Admin				Super Admin

Prisma SaaS Service Interface Options	Privileges				
	None	View	View, Download	View, Download, Create	Full Control
	Limited Admin Incident Management Admin				
Reset Authentication for Super Admin	Read Only Admin Limited Admin Incident Management Admin				Super Admin
Dismiss Security Control	Read Only Incident Management Admin				Super Admin Admin Limited Admin
Assign Incident	Read Only				Super Admin Admin Limited Admin Incident Management Admin
Change Incident State	Read Only				Super Admin Admin Limited Admin Incident Management Admin

Select an Authentication Method

To strengthen your security posture, you can enforce multi-factor authentication (MFA) for Prisma SaaS and/or enable single-sign-on authentication (SSO) to verify admin users who access Prisma SaaS.

- Configure SAML Single Sign-On (SSO) Authentication on Prisma SaaS to improve user experience and reduce the administrative overhead of managing administrative accounts locally. By configuring Prisma SaaS as a SAML service provider, you can provide uninterrupted and secure access using a single set of login credentials.
- Configure Google Multi-Factor Authentication (MFA) when you Add Prisma SaaS Administrators to Prisma SaaS to ensure that attackers cannot steal login credentials (a single factor) and gain access to the sensitive information on the service.

Local authentication is not supported for Prisma SaaS activated on the hub. Learn how to enable MFA for your Palo Alto Networks CSP account.

Configure SAML Single Sign-On (SSO) Authentication

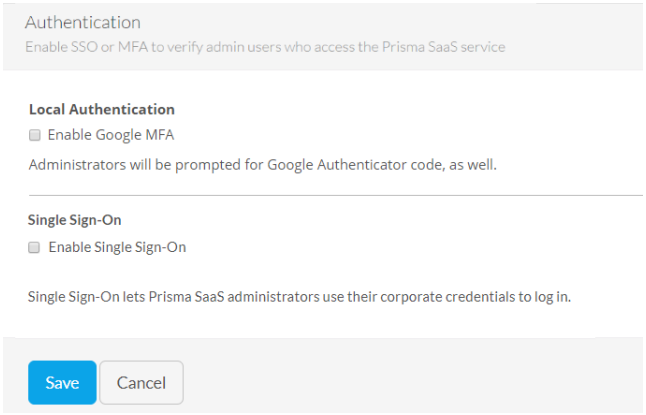
By default, Prisma SaaS uses local database authentication stored separately from your enterprise login account which requires you to create sign in accounts for each Prisma SaaS administrator. If your organization has standardized on SAML SSO authentication, you can eliminate duplicate accounts by configuring Prisma SaaS as a SAML service provider so administrators can use their enterprise credentials to access the service. You must be a Super Admin to set or change the authentication settings on Prisma SaaS.

For all Prisma SaaS instances provisioned after July 17, 2019, when you add an administrator through the Prisma SaaS UI, a Customer Support Portal account is automatically created and linked to the Prisma SaaS account.

STEP 1 | Enable SSO authentication on Prisma SaaS.

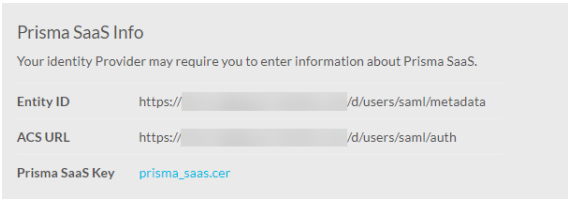
You must be a **Super Admin** to configure SSO authentication.

1. Select **Settings** > **Authentication**.
2. Select **Enable Single Sign-On** and **Save**.



3. Make a note of the Prisma SaaS **Entity ID** and **ACS URL** provided.

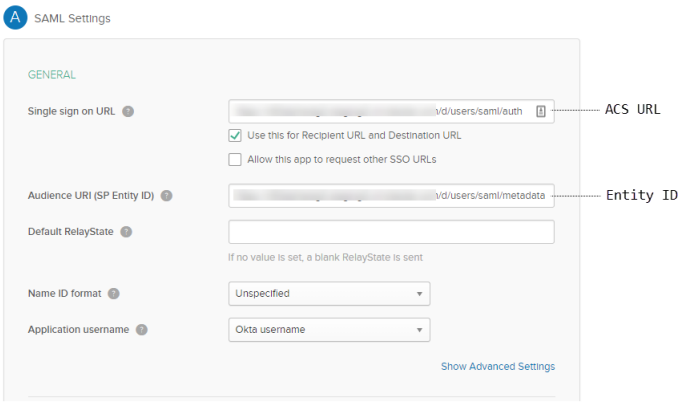
   The Identity Provider needs this information to communicate with Prisma SaaS.



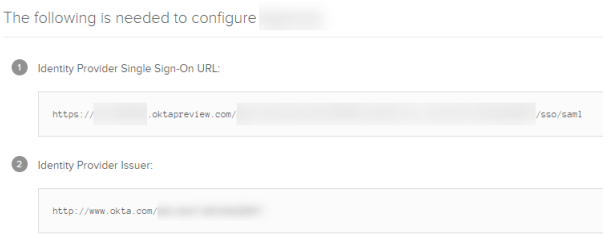
STEP 2 | Configure Prisma SaaS on your SAML Identity Provider.

This example uses Okta as your Identity Provider.

1. Add the Prisma SaaS **Entity ID**.
2. Add the Prisma SaaS **ACS URL**.
3. Obtain the IDP certificate from the Identity Provider and install the certificate on the IDP server. If you do not know where to obtain the certificate, contact your IDP administrator or vendor.

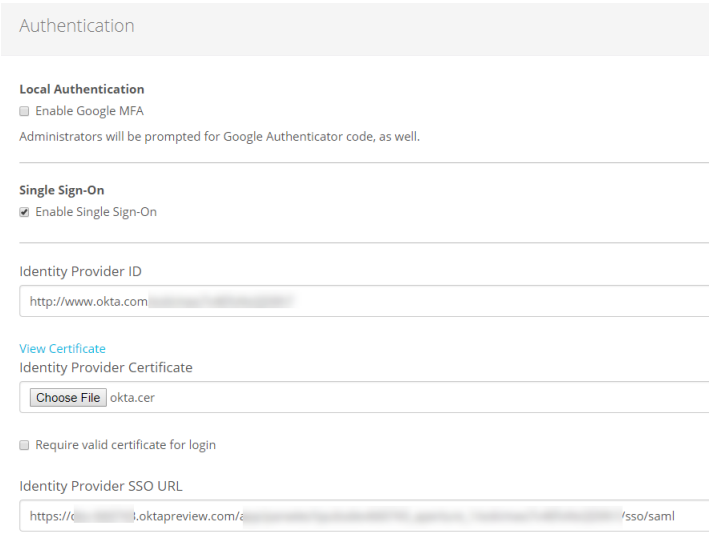


4. Save the Prisma SaaS configuration for your chosen Identity Provider and collect setup information provided.



STEP 3 | Configure SSO authentication on Prisma SaaS.

1. Enter the **Identity Provider SSO URL**.
2. Browse to add an **Identity Provider Certificate**. The identify provider uses this certificate to sign SAML messages. Alternatively, you can disable **Require valid certificate for login**.
3. Enter the SAML **Identity Provider ID**.



4. **Save** your changes.

STEP 4 | Select SSO as the authentication type for Prisma SaaS administrators.

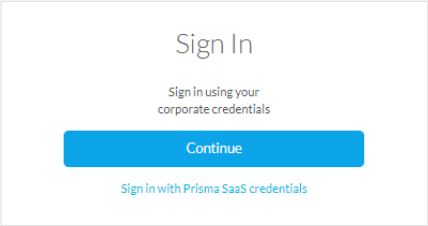
Configure the authentication type for each administrator after configuring the SSO on Prisma SaaS and identity provider.

As a Super Admin, you can change the Authentication Type for any account except your own. To change your Authentication Type, another Super Admin must configure your account.

1. Select **Settings** > **Admin Accounts**.
2. Create a new **Admin Account** or edit an existing one.
3. For the **Authentication Type**, select **Single Sign-On (SSO)**.

   After a Prisma SaaS administrator logs in successfully, the following message will display.

   When an Administrator has an account in the Prisma SaaS local database and a SSO log in, the following sign in screen displays.



Configure Google Multi-Factor Authentication (MFA)

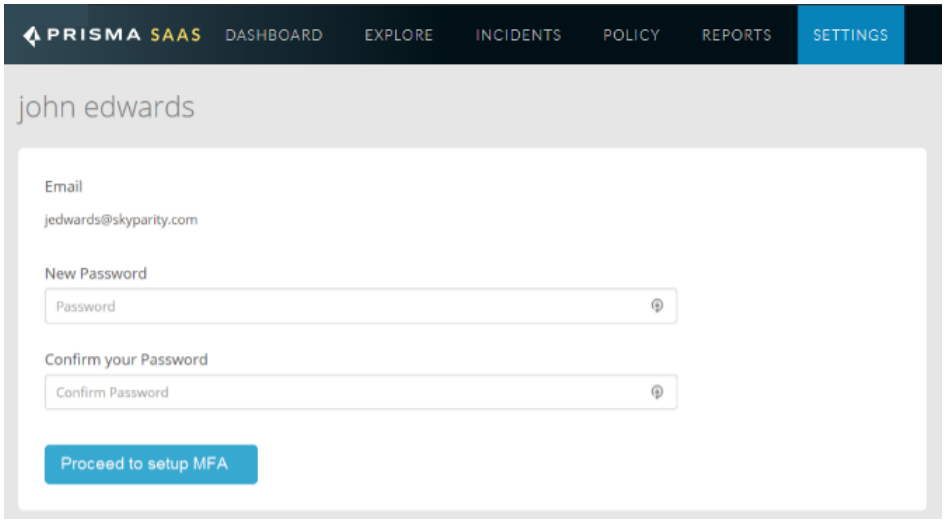
If your organization has not standardized a SAML SSO for Prisma SaaS administrator access, you can setup multi-factor authentication (MFA) to strengthen your security posture. You must be a Prisma SaaS Super Admin to set or change the authentication settings. When you enable MFA, you protect your account by logging in with your password and a unique verification code (sent to your phone via text, phone call, or the Google mobile app).

Google MFA Authentication is unavailable to Prisma SaaS instances set up after July 17, 2019.

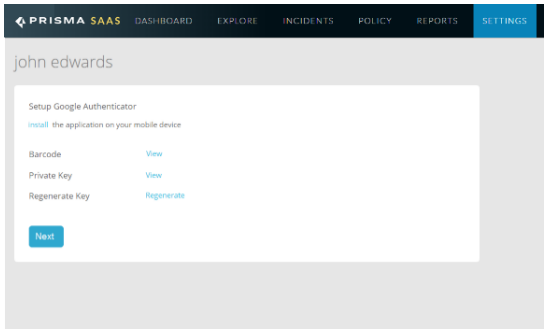
STEP 1 | Configure your device for MFA.

Your Android device must be running Android version 2.1 or later to use Google MFA. Your iPhone, iPod Touch, or iPad must have the latest operating system for your device, and your iPhone must be a 3G model or later in order to set up the app using a QR barcode.

1. Log in to Prisma SaaS using your current credentials. Click **Proceed to setup MFA**.

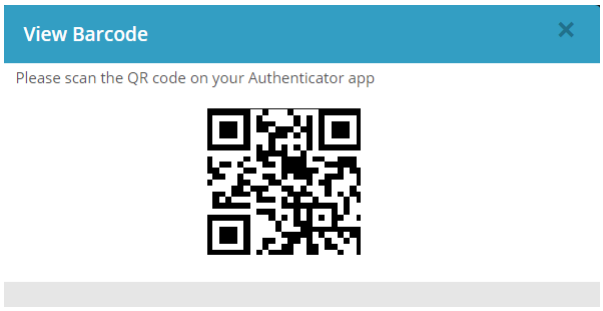


2. **Install** the Google Authenticator app to your mobile device.

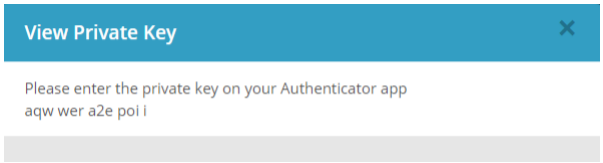


STEP 2 | Link your mobile device to your account on Prisma SaaS.

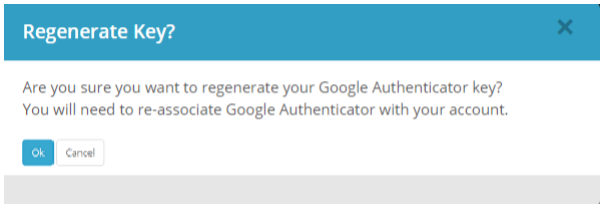
1. Using **QR Barcode**— Select Barcode **View**. If the authenticator app cannot locate a barcode scanner app on your mobile device, you can download and install one. If you want to install a barcode scanner app so you can complete the setup, select **Install**, and then go through the installation process. After installation, reopen Google Authenticator, and point your camera at the barcode on your computer screen.



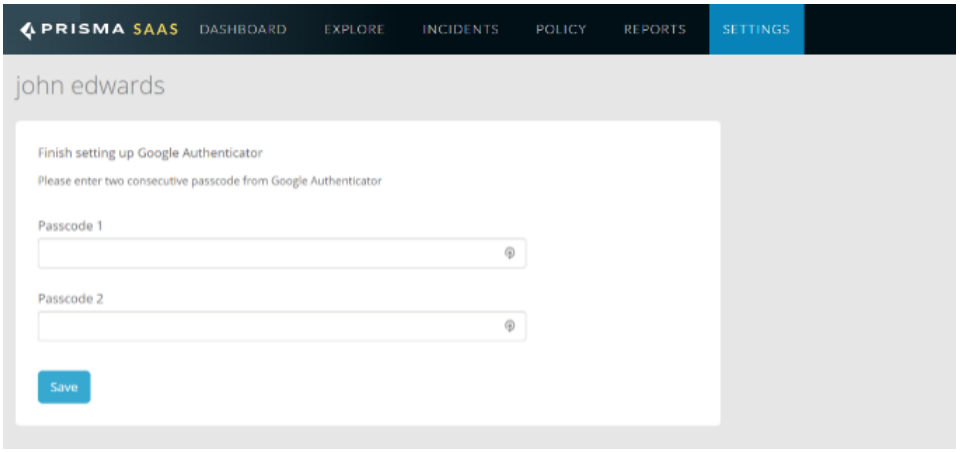
2. Using **Private Key**— Select Private Key **View** and then enter the **`private key`** on your authenticator app.



3. On the **Regenerate Key?** screen, click **OK** to receive two consecutive passcodes to sync to the authenticator app.



4. On Prisma SaaS, enter the two passcodes and **Save** the setup.



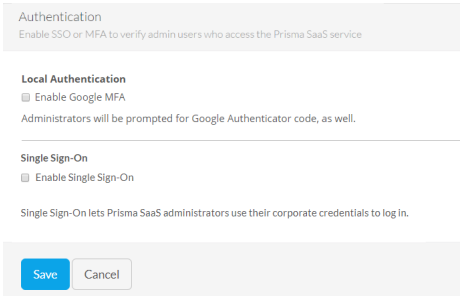
5. Read and **Accept** the End-User License Agreement (EULA).

   To test that the app is working, enter the verification **Code** from your mobile device and then **Verify**. A confirmation message will display if your code is correct. **Save** to exit the setup. If your code is incorrect, try generating a new verification code on your mobile device, and then entering it in your computer.

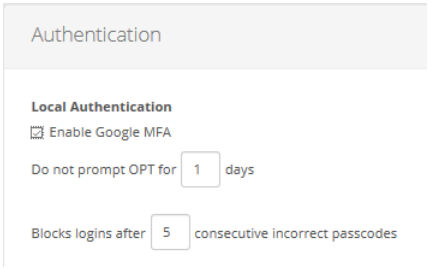
STEP 3 | Configure MFA on Prisma SaaS.

*As a Prisma SaaS **Super Admin**, you can change the Authentication settings for any account except your own. To change your Authentication settings, another Super Admin must configure your account.*

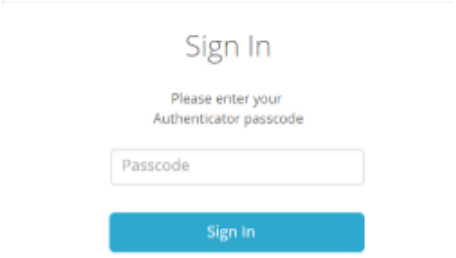
1. Select **Settings** > **Authentication**.
2. Select an **Authentication** method:
   - **Local Authentication**— Grants user access after successfully presenting a passcode pair or QR barcode evidence to the MFA mechanism.
   - **Single Sign-On**— A single sign-onlogin event provides automatic access to multiple authenticated services, and a single logout event automatically ends the session for multiple services.
   - **Save** your selection.



3. Define the settings for local authentication.
   - Enter the one-time password (OTP) prompt frequency in **Local Authentication** > **Do not prompt for OTP** to **0** for all log in attempts, or the number of days from **1** to **7**.
   - Enter the number of incorrect login attempts allowed in **Block logins after consecutive incorrect passcodes** between **1** and **30**. **Save** your settings.



Administrators will see this authentication message after entering their Prisma SaaS credentials.



Reset Administrator Authentication

As a Prisma SaaS **Super Admin**, you can reset the Authentication settings for any account except your own. To change your Authentication settings, another Super Admin must reset your account. If you are the only Super Admin and require a reset, please contact customer support to open a case. After a reset, authentication must be set up again.

The ability to reset administrator authentication option on Prisma SaaS is only available for instances set up before July 17, 2019.

STEP 1 | Select **Settings** > **Admin Accounts**.

STEP 2 | Click the Name of the administrator and select **Reset MFA**.

If you do not see the Reset MFA link, you do not have the privilege necessary to modify the settings. When you successfully reset authentication, the administrator receives an email that includes a link to pair their device and setup their authentication.

Reset Administrator Password

Administrators with a Super Admin role can reset the password for any administrator account but an administrator with the Admin role can only reset the password for other Admin role administrators, or administrators with a Limited Admin or Read Only role.

The ability to reset an administrator password on Prisma SaaS is available on instances set up before July 17, 2019. For instances set up after July 17, 2019, reset your password through the Customer Support Portal*.*

STEP 1 | Select **Settings** > **Admin Accounts**.

STEP 2 | Click the **Name** of the administrator and **Force Change Password**.

If you do not see the Force Change Password link, you do not have the privilege necessary to modify the settings. When you successfully reset a password, the administrator receives an email that includes a link to change their password.

Unblock an Administrator

As a **Super Admin**, you can unblock any account except your own. To unblock your account, another Super Admin must unblock you. If you are the only Super Admin, contact customer support to open a case.

The ability to unblock an administrator is unavailable on Prisma SaaS instances set up after July 17, 2019.

STEP 1 | Select **Settings** > **Admin Accounts**

STEP 2 | Click the **Name** of the administrator and select **Unblock User**.

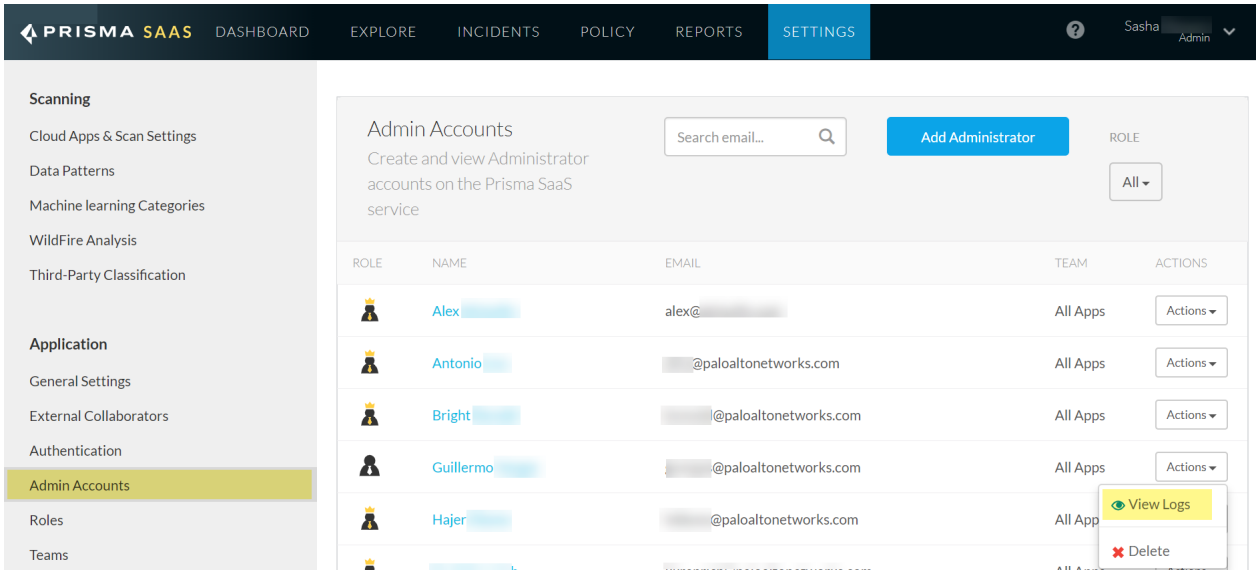
If the Unblock User link is not visible, you do not have the permissions necessary to unblock the account. When you successfully unblock a user, the administrator receives an email alerting them their account is unblocked.

View Administrator Activity Logs

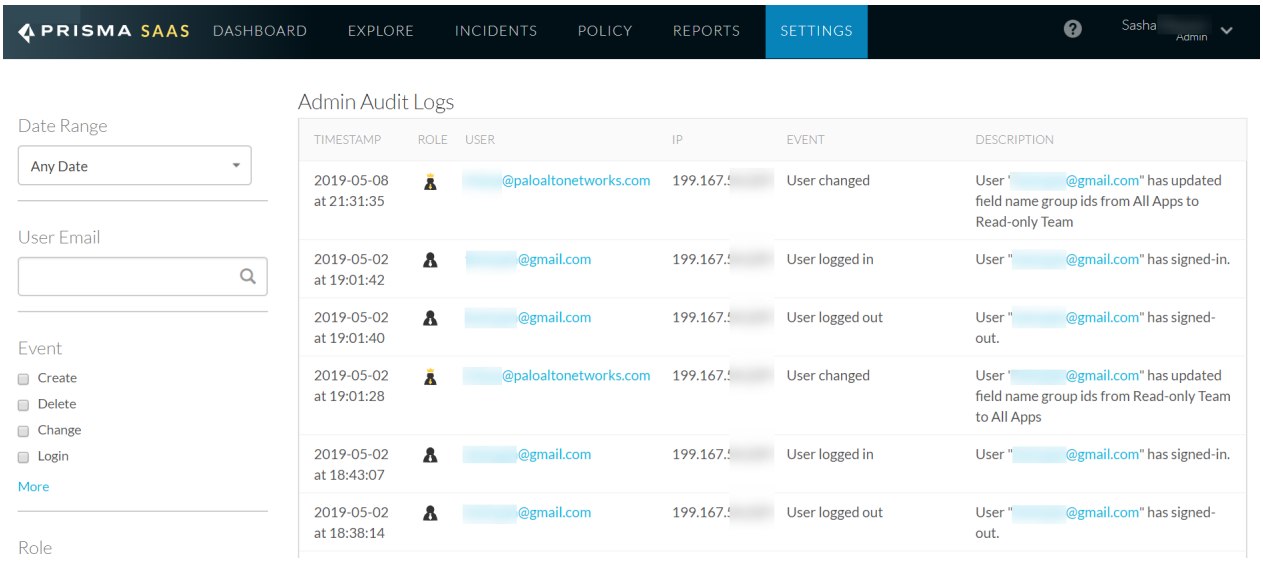
Prisma SaaS captures actions performed by each administrator in a log so you can audit activity and track changes. If an administrator has privileges to access all apps, they can audit activity and track changes for all administrators, but a team administrator only has access to the admin activity logs for the cloud apps they monitor.

You can view the activity logs for a specific administrator or use faceted search to narrow the list of all activity logs by searching for a date range or type of event. This enables you to search for a specific type of incident or investigate incidents within a certain time frame instead of navigating through pages of unrelated events. After collecting a list of specific events for reporting purposes, you can download the results of your search by clicking **CSV**.

- View the administrative activity logs for a specific admin.
  1. Select **Settings** > **Admin Accounts**.
  2. Select **View Logs**.

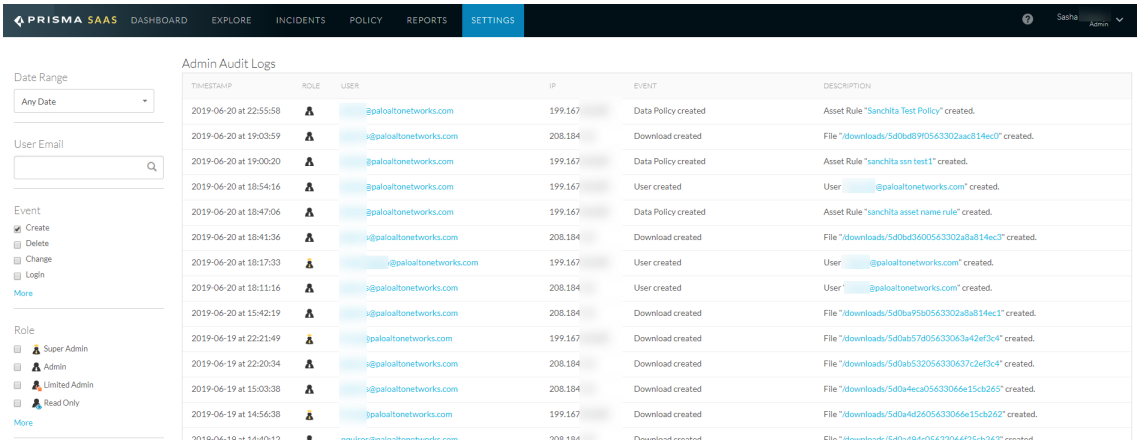


3. **Admin Audit Logs** display the timestamp of related events, admin role, email address, IP address, event type, and event description. Use faceted search to specify a date range or event to narrow the results even further.



- Select **Settings** > **Activity Logs** to audit the activity for all administrators configured on Prisma SaaS.

  Use faceted search to narrow the results by specifying a date range, user email, event type, or role.



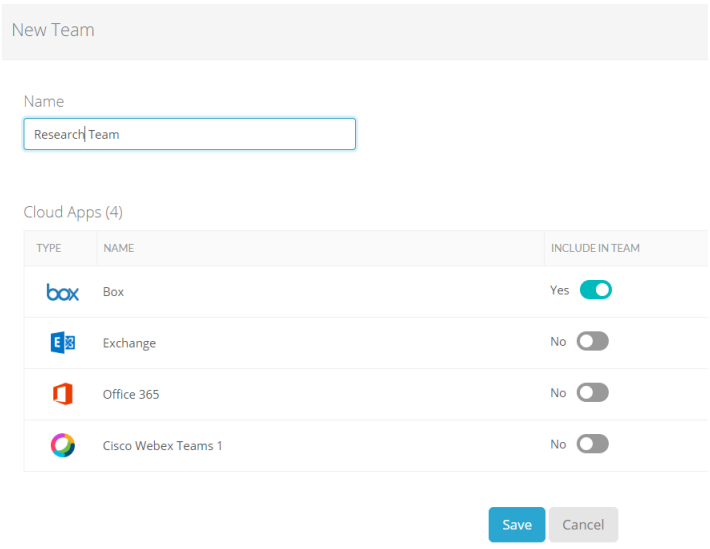
Create Prisma SaaS Teams (Beta)

As a Super Admin, you can create a team to group cloud apps and restrict admin access to cloud app, incidents, and assets on Prisma SaaS. Instead of granting access to all apps, you can assign an admin to a team and grant access to just a few apps. With the Super Admin role, you can create teams or edit administrator accounts, and assign administrators to teams.

A team administrator has access to Policies and Rules that can affect all apps. See Predefined Role Privileges *for more information on permissions for a team administrator.*

STEP 1 | Create a custom team.

1. Select **Settings** > **Teams** and **Add New Team**.
2. Enter the **Name** and select the applications the team will have access to.
3. **Save** to create your new team.

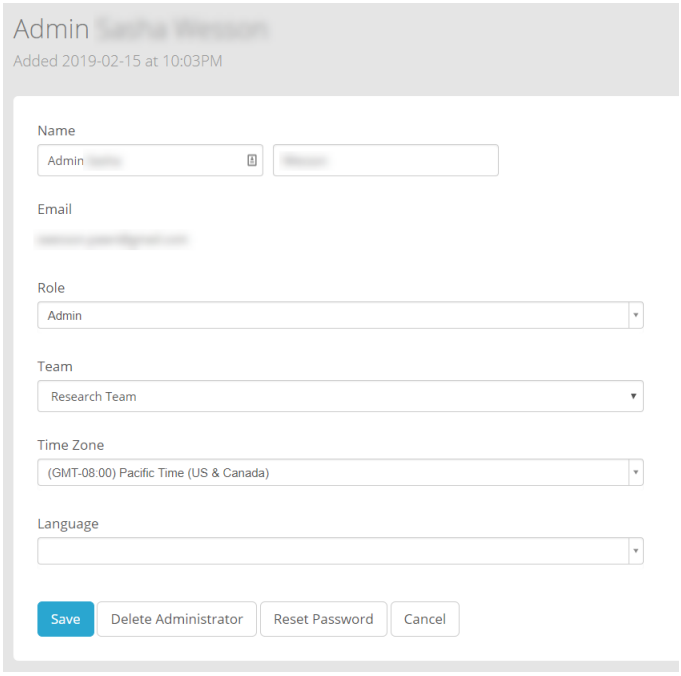


STEP 2 | Add an administrator to a team.

Only an administrator with a Super Admin role can move other administrators to a team.

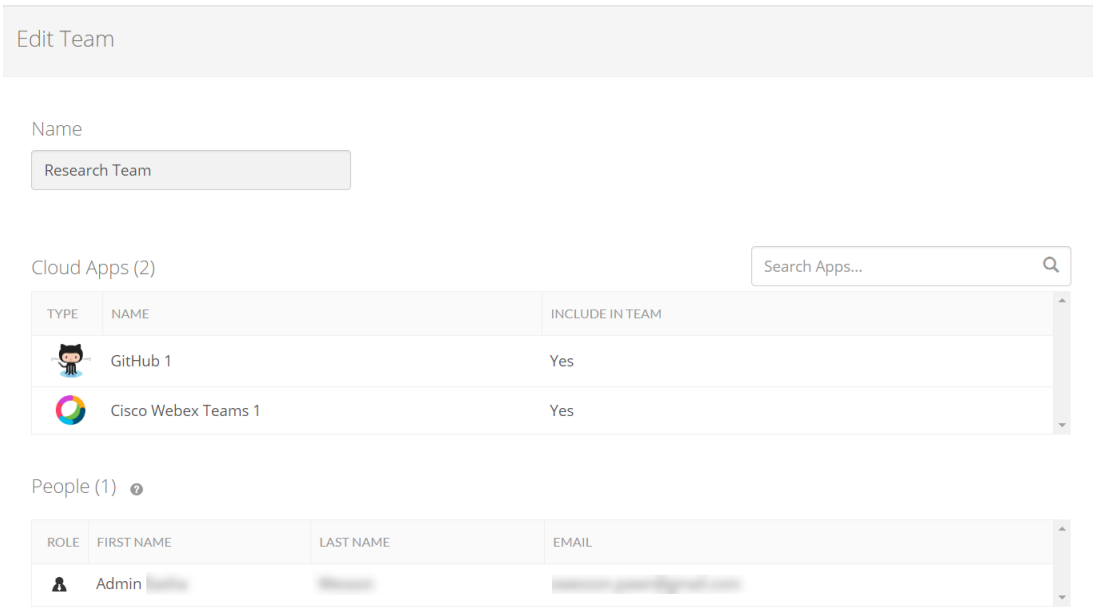
1. Select **Settings** > **Admin Accounts** and select an administrator.
2. Select the team you want to assign the administrator to.

3. **Save** your changes.



STEP 3 | Review the administrators and cloud apps assigned to the team.

1. Go to **Settings** > **Teams** and select the Team.



Configure Prisma SaaS Global Scan Settings

Before you start scanning, define any collaborators and the asset exposure level to trigger incident reports, and configure global settings for Prisma SaaS to use when scanning your sanctioned SaaS applications.

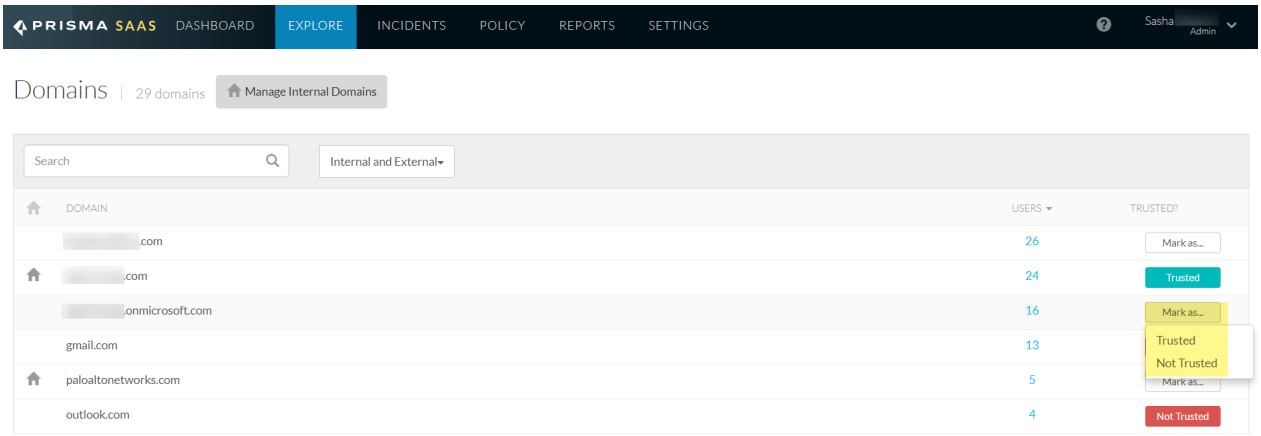
Collaborators

Although different SaaS applications have different terminology for sharing and collaboration, within Prisma SaaS, a collaborator is any person who can access, view, preview, download, comment, or edit a managed asset. To provide granular control over what types of sharing pose a risk within your organization, Prisma SaaS classifies Collaborators differently:

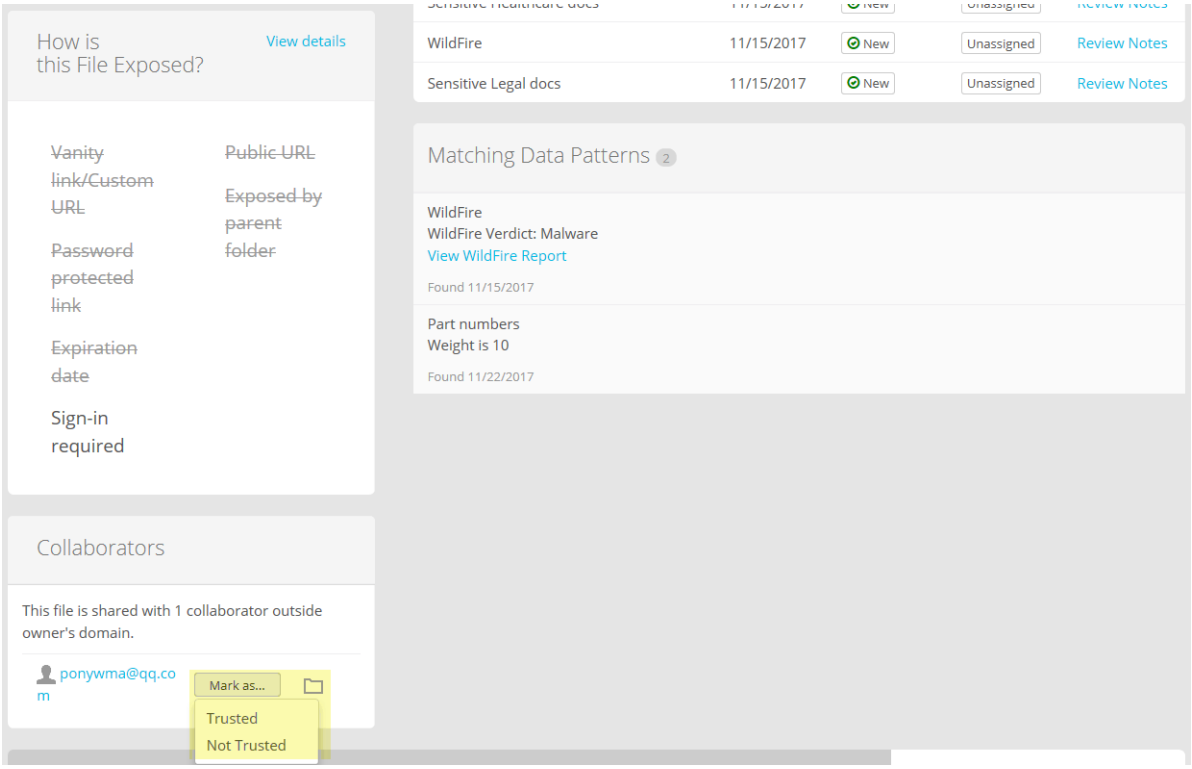
Because Collaborators apply to all cloud apps on Prisma SaaS, you must be an administrator with a Super Admin role or an Admin with access to all apps to modify this setting.

- **Internal vs. External Users**—Prisma SaaS uses the domain name in the email address associated with the user's cloud app account to determine whether the user is internal to your organization or not. You must Define Your Internal Domains before you begin scanning your application data so Prisma SaaS can properly identify assets shared with users who are external to your organization.
- **Trusted vs. Untrusted Users**—Using Prisma SaaS, you can configure a policy rule to create an incident if an external user has access to an asset. In some cases, sharing with external users—even though they are not part of your organization—does not pose a threat. For example, they may be partners or other trusted third-parties who you can mark as **Trusted**. Or, if you have entire domains that belong to trusted partners or user groups, you can mark those domains as **Trusted** so those users with email addresses from that domain are trusted users.

  When you Assess Incidents, you can update the domain trust settings in **Explore** > **Domains** and mark the domain as either trusted or untrusted.



Alternatively, you can explicitly designate an external collaborator as **Trusted** to exclude from incident discovery or **Untrusted** to ensure both new and modified assets shared create incidents. Changing trust settings for a user or a domain changes the underlying global policy Prisma SaaS uses when scanning assets. Trust settings enable more granular policy control while still allowing you to distinguish between internal and external sharing.



Exposure Level

Prisma SaaS uses an exposure level status to describe how your shared assets appear in an application. Although every SaaS application has its own settings for controlling how and with whom users may share assets, Prisma SaaS provides a mechanism for setting and enforcing acceptable exposure levels consistently across all your managed applications. On Prisma SaaS, each policy rule—both the default rules as well as any custom rules you define—enable you to set a level of exposure identifying an asset as being at risk (except for Sensitive Documents rules, which match documents with predefined characteristics).

The exposure level is just one match criteria available in a policy rule and, therefore, determining the minimum level of exposure posing a threat depends on the other match criteria, and what threat the policy rule protects against. For example, the WildFire policy rule scans all your assets for files containing malware. In this case, a file containing malware poses a threat no matter the exposure level. However, if you add a Sensitive Credential policy rule to protect an engineering GitHub repository used for sharing code throughout the company, any external sharing poses a risk, so you should configure the rule to match on Public and External exposures.

Prisma SaaS scans assets for the following exposure levels:

Exposure Level	Description
Public	An asset is Public if it contains either of the following:

Exposure Level	Description
	• **Public share settings**—Assets found on a public repository or publicly indexed on Google. • **Shared links**—The owner created a public link, vanity URL, or password-protected link for direct access to the asset.
External	The owner invited one or more users outside of your organization to collaborate on the asset.
Company	The owner created a company-wide URL giving anyone in the company direct access to the asset.
Internal	Includes assets the owner has not shared. Also includes assets the owner has shared, but only with users within the company. These users have an email address in the enterprise domain name.
Shared via Custom URL	The owner created a custom link, vanity URL, or password-protected link for direct access to the asset and then shared this asset (directly or indirectly) using the link.  *This option is for Box assets only and hidden if you are not using Prisma SaaS to secure Box applications.*

Define Your Internal Domains

One of the first things you need to do is to define your internal domains. Prisma SaaS uses the list of internal domains you define to determine if the Collaborators on an asset are internal to your company, or if the asset shared with external users. Prisma SaaS determines this by matching the domain name in a collaborator's email address against the list of internal domains defined. Depending on your policy rules, Prisma SaaS may identify an asset as an incident if shared with external users.

Because Prisma SaaS uses the internal domains list to determine the Exposure Level of an asset during the scan process, you must define your internal domains list before you begin scanning your cloud apps.

 *The Internal Domains list applies to all cloud apps on Prisma SaaS so you must be an administrator with a Super User role or an Admin with access to all apps to modify this setting.*

STEP 1 | Select **Settings** > **Cloud Apps & Scan Settings**.

STEP 2 | Enter a comma-separated list of your **Internal Domains**.

STEP 3 | **Save** your changes.

Define Trusted and Untrusted Users and Domains

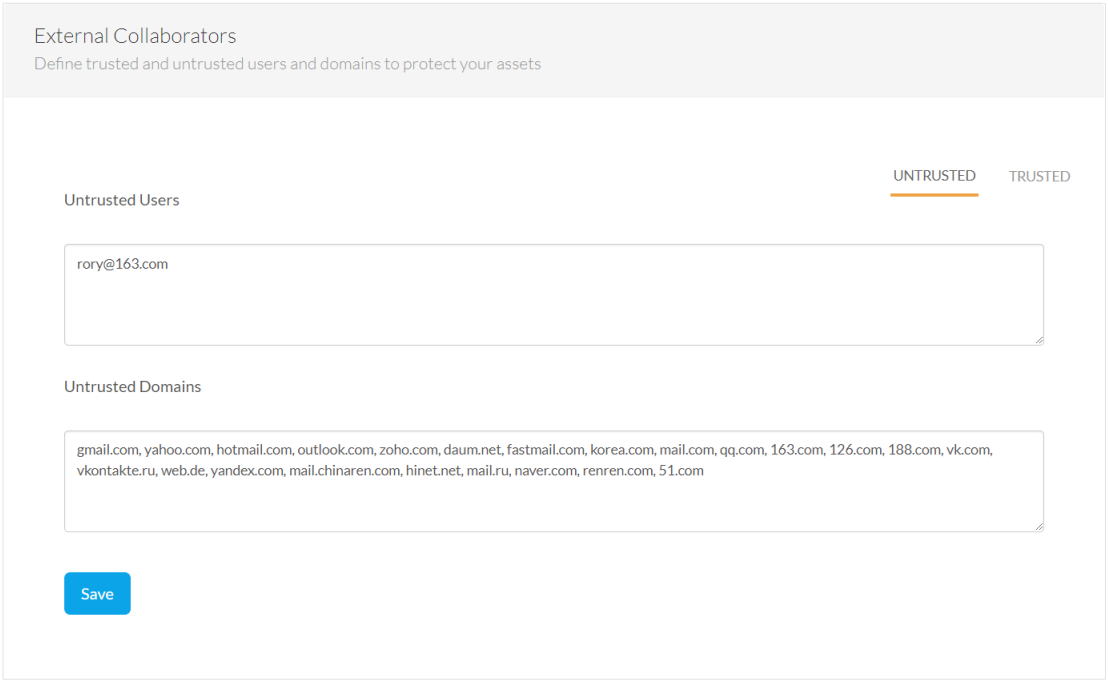
One of the first things you did when setting up Prisma SaaS was Define Your Internal Domains to determine if the user is internal to your organization. If an external user has an email address that does not belong to an internal domain, you can use Prisma SaaS to define users and domains as trusted or untrusted to protect

your assets and have better granular control over who has access. Once you define external users and domains, Prisma SaaS reports any assets shared inadvertently or maliciously.

Because the Trusted and Untrusted Users and Domains list applies to all cloud apps on Prisma SaaS, you must be an administrator with a Super Admin role or Admin with access to all apps to modify this setting.

STEP 1 | Select **Settings** > **External Collaborators**.

STEP 2 | Select **Untrusted** and enter the email address in **untrusted users** and the domains in **untrusted domains**.



STEP 3 | **Save** your setting.

Enable Data Masking

Data masking allows you to control the exposure of sensitive data, such as credit card numbers or Social Security numbers, displaying required information in clear text to the administrator and other non-privileged users who can view the snippet of content matched as an incident. For example, with complete data masking enabled, Prisma SaaS will display a credit card number as XXXX-XXXX-XXXX-XXXX.

Because the Data Masking setting applies to all cloud apps on Prisma SaaS, you must be an administrator with a Super Admin role or Admin role with access to all apps to modify this setting.

STEP 1 | Specify the storage and reporting of sensitive data by Prisma SaaS.

For financial and PII policy rules, Prisma SaaS displays a snippet of 100 bytes of content before and after the violation.

Select **Settings** > **Cloud Apps & Scan Settings**.

- **Do not mask**—Displays all the values in clear text.

- **Partial Mask** —Displays only the last four digits in clear text.
- **Full mask**—Does not display any values.

STEP 2 | Save the changes.

Save your changes.

Set the Time Zone on Prisma SaaS

Change the time zone from UTC/GMT to your local time zone on Prisma SaaS to display your local date and timestamp.

By default, Prisma SaaS displays all dates and timestamps—activity log timestamps, incident dates and times, and file access logs—in Coordinated Universal Time (UTC/GMT). You can change the time zone settings so Prisma SaaS displays date and time information in your local time zone, but the changes to the time zone you can make depend on your administrative role:

- **Super Admin Role**—Administrators with a Super Admin role can change the default time zone globally. All administrators who log in will see data in the time zone set by the Super Admin.
- **Admin Role**—Administrators with an Admin role and has access to all apps, can change the time zone for their own sessions. For example, if a Super Admin set the time zone to Pacific Time but you are in New York, you could set the time zone for your own account to Eastern Time so you can view the data in the context of your local time zone.

STEP 1 | Select **Settings** > **Admin Accounts**.

STEP 2 | Select your **Name** in the list of Admin Accounts.

STEP 3 | Select the **Time Zone** you want Prisma SaaS to use when displaying dates and timestamps.

STEP 4 | **Save** your changes.

Configure the Email Alias and Logo for Sending Notifications

Prisma SaaS is configured with an SMTP service enabling you to send email notifications when a policy violation occurs. When you email a user, the default display name is Prisma SaaS and the sender email address is **`no_reply@paloaltonetworks.com`**. Although asset owners can reply to this default sender email address, **`no_reply`** discourages them. Best practice is to change this default and others to personalize your communications. Use the logo feature to legitimize the email sender so asset owners do not mistake your email as spam.

Because General Settings applies to all the cloud apps on Prisma SaaS, you must be an administrator with a Super Admin role or an Admin role with access to all apps to modify this setting.

STEP 1 | Select **Settings** > **General Settings** > **Workflow Settings**, specify your settings, then **Save**:

- **Sender Name**—Name of the sender of the email message. Best practice is to use a name with imperative, such as Security Administrator or Compliance Auditor.
- **Reply-to-Email**—Address to use for communications. Best practice is to use a distribution list or an alias with a group of administrators or compliance auditors. Optionally, you can choose an alias that automatically triggers a helpdesk ticket upon reply.
- **Default Time Zone**—Local time zone to display in communications.
- **Default Language**—Supported language of choice for communications.

STEP 2 | Upload an **Email Logo**. Browse to select the image, then **Save**.

Configure the Default Language

As part of the Prisma SaaS internationalization project to expand globally and improve user experience, you can customize the default local language. By enabling the default local language, you can improve team collaboration, ease of access, and productivity on the assets in your cloud apps using a shared local language.

Because Default Language applies to all cloud apps on Prisma SaaS, you must be an administrator with a Super Admin role or an Admin with access to all apps to modify the language setting.

STEP 1 | Select **Settings** > **General Settings**.

STEP 2 | Select the **Default Language**.

STEP 3 | **Save** your changes.

Secure Cloud Apps

Palo Alto Networks Prisma SaaS allows you to consistently define and enforce policy for securing data across all your sanctioned software as a service (SaaS) applications. Although each application has its own settings to secure how users can store and share data, the settings and levels of enforcement vary by application. By adding your applications to Prisma SaaS, you have visibility into and control over how your users are accessing and sharing data across your sanctioned applications.

When Prisma SaaS first connects to an application, it scans all the assets in the application and matches against the policy rules to retroactively uncover incidents and then displays all active incidents on the Dashboard. To maximize the results from this initial discovery process, configure the global scan settings for policy, examine your corporate acceptable use policy for SaaS applications, and review the default policy rules in Prisma SaaS before you start the scan.

Configure Prisma SaaS to control unmanaged device access to your sanctioned applications by redirecting traffic through your next generation firewall. Utilizing your existing corporate Identity Provider, add Prisma SaaS and SaaS application integration to authenticate requests and grant access to users using Prisma SaaS as SAML proxy.

Additionally, you can use Prisma SaaS to connect to your Cortex Data Lake to access your next-generation firewall or GlobalProtect Cloud Service logs to present a holistic view of sanctioned and unsanctioned SaaS application usage. This visibility on Prisma SaaS allows you granular control over access, unsanctioned application usage, and external exposure of data.

While Prisma SaaS performs deep content inspection, it does not store any data from your monitored applications. It stores only metadata about your assets, which is data about your data.

- Supported SaaS Applications
- Add Cloud Apps to Prisma SaaS
- Add Unsanctioned Device Access Control to Prisma SaaS
- Monitor Scan Results on the Dashboard (Basic DLP)
- SaaS Application Visibility on Prisma SaaS
- Use Faceted Search to Filter Assets
- Use Advanced Search and Use Advanced Search Expressions
- Reauthenticate to a Cloud App
- Stop Scanning a Managed Cloud App
- Rescan a Managed Cloud App

Supported SaaS Applications

SaaS applications are cloud apps owned and managed by an application service provider, but you retain full control of the data, including who can create, access, share, and transfer information stored in the hosted application. Although most SaaS applications allow you to configure rules about sharing and exposing data, rules vary from application to application, which makes it challenging to ensure consistent security policy across all applications, assets, and users.

Prisma SaaS provides centralized policy and enforcement for your applications so you can protect your corporate data at all times. The service scans content to detect data exfiltration and malware propagation, monitors user activity, and provides activity-based alerting to notify you of malicious or risky behavior. This visibility allows you to assess incidents, quarantine users and data, and remediate any violations to protect against threats caused by malware, inadvertent sharing, excessive permissions, and data exposure.

The following table lists the applications that Prisma SaaS supports, the versions supported, and briefly describes what type of content is scanned for each application.

SaaS Application	Versions Supported	Description
Amazon S3		On the Simple Storage Service(S3), Prisma SaaS scans files in S3 buckets. Begin Scanning an Amazon S3 App.
Amazon Web Services		On the Amazon Web Services (AWS) console, you can check for security group settings that allow external access to your AWS resources and for services that can exit from your AWS VPC. It also checks for password complexity and enables you to identify users who can log in to the AWS account without multi-factor authentication (MFA). Begin Scanning an Amazon Web Services App.
Box	Business Business Plus Enterprise	On Box, the cloud-based file-sharing and collaboration application, you can scan data in files and folders. Begin Scanning a Box App.
Cisco Webex Teams	Starter Plus Business Enterprise	On Webex Teams, the cloud-based teamwork application that supports file sharing and secure messaging, you can scan data in files and messages. *If you are using the Standard service plan for Cisco Webex Teams, consider upgrading to the Pro Pack service plan before you add the app to Prisma SaaS. The Pro Pack plan provides visibility into events such as messages and files posted on the app, and users added to spaces, occurring more than 90 days ago.*

SaaS Application	Versions Supported	Description
		Begin Scanning a Cisco Webex Teams App (Beta).
Citrix Sharefile	Team Business Virtual Data Room	On Citrix ShareFile, a file synchronization and storage service, you can scan files and folders. Begin Scanning a Citrix ShareFile App (Beta) .
Confluence	Confluence Cloud	On Confluence, the centralized platform for knowledge sharing, document management, project planning, you can scan pages and attachments. Begin Scanning a Confluence App (Beta).
Dropbox	Business Standard Advanced Enterprise	On Dropbox, a personal cloud storage service used for file sharing and collaboration, you can scan files and folders. Begin Scanning Dropbox
GitHub		You can scan all files (source code and intellectual property) stored on this collaborative web-based service. Begin Scanning GitHub
Gmail	Business Enterprise	On the Gmail application, you can scan email content and attachments and identify if users have configured email forwarding rules in their Inbox. Begin Scanning a Gmail App
Google Cloud Platform	Business Enterprise	On Google Cloud Platform, you can scan projects, buckets, and files. Begin Scanning a Google Cloud Storage App.
Google Drive	Business Enterprise	On Google Drive, the cloud storage and file backup application, you can scan files and folders. Begin Scanning a Google Drive App
G Suite Marketplace	Business Enterprise	On the Business and Enterprise versions of G-Suite Marketplace you can scan 3rd party apps. Begin Scanning Third-Party Apps on the G Suite Marketplace
Jive	Cloud version	On Jive, the commercial collaboration and knowledge management tool, you can scan questions, discussions, documents, blogs, files, and comments. Add a Jive App.
Microsoft Azure Storage	Business Enterprise	On Microsoft Azure Storage, you can scan storage accounts, containers, and files. Prisma SaaS provides activity monitoring, activity-based alerting, remediation.

SaaS Application	Versions Supported	Description
		Begin Scanning a Microsoft Azure Storage App
Microsoft Exchange	Home and Firstline Workforce are not supported	On Microsoft Exchange you can scan email content and attachments. Prisma SaaS also allows you to identify users who have configured email retention policies other than those policies configured by the corporate administrator, and if users have configured email forwarding rules in their Inbox. Begin Scanning a Microsoft Exchange App.
Office 365	Home and Firstline Workforce are not supported	You can scan files and folders on all versions of OneDrive. Begin Scanning Microsoft Office 365 Apps.
Salesforce	Standard Premier Sandbox	On the Salesforce customer relationship management (CRM) service, Prisma SaaS scans both structured and unstructured content. While Prisma SaaS stores the metadata for all unstructured files, it stores structured file data selectively. For example, a Salesforce Chatter message has structured data and is stored only when the content in the message matches a defined data pattern but an attachment on Salesforce Chatter has unstructured data, so Prisma SaaS scans the attachment and stores the metadata. Begin Scanning a Salesforce App.
Slack for Enterprise	Enterprise	On the cloud-based team collaboration tool, Slack, you can scan messages and attachments. Begin Scanning a Slack for Enterprise App.
ServiceNow		Prisma SaaS enables you to scan tables and attachments on ServiceNow. Begin Scanning a ServiceNow App.
Workplace by Facebook		On Workplace, the collaborative enterprise platform run by Facebook, you can scan posts, comments, and files. Begin Scanning a Workplace by Facebook App (Beta).
Yammer		Prisma SaaS can scan messages and attachments on this collaboration tool included with Office 365. Begin Scanning Yammer.

Add Cloud Apps to Prisma SaaS

To begin securing the Supported SaaS Applications, you must connect them to Prisma SaaS by authenticating to the application using an administrator account (the specific privilege requirements vary from application to application). After you successfully authenticate, Prisma SaaS receives a token from the cloud app for establishing and maintaining a secure connection. Prisma SaaS then connects directly to the application programming interface (API) for that app, which enables the scanning of all historical data that resides within the app, as well as continually monitoring modified or new data, and identifying policy violations and incidents.

To perform data discovery, Prisma SaaS gets metadata for all your files and folders on the application. Metadata includes file properties and attributes, and application-level metadata such as file owner, email recipients, and collaborators. For certain apps with structured data such as Salesforce, and messaging apps such as Slack, Facebook Workplace, and email apps, Prisma SaaS scans both structured and unstructured data. All files such as attachments that are unstructured, the files are scanned and the metadata is always stored. Even though Prisma SaaS scans structured data, it does not store metadata for every field and message unless the field or message has some content that matches a data pattern defined on Prisma SaaS. This is done to minimize the privacy risk by storing all of your metadata.

- Begin Scanning an Amazon S3 App
- Begin Scanning an Amazon Web Services App
- Begin Scanning a Box App
- Begin Scanning a Cisco Webex Teams App (Beta)
- Begin Scanning a Citrix ShareFile App (Beta)
- Begin Scanning a Confluence App (Beta)
- Begin Scanning Dropbox or Yammer
- Begin Scanning GitHub
- Begin Scanning a Gmail App
- Begin Scanning a Google Cloud Storage App
- Begin Scanning a Google Drive App
- Begin Scanning Third-Party Apps on the G Suite Marketplace
- Add a Jive App
- Begin Scanning a Microsoft Azure Storage App
- Begin Scanning a Microsoft Exchange App
- Begin Scanning Microsoft Office 365 Apps
- Begin Scanning a Salesforce App
- Begin Scanning a ServiceNow App
- Begin Scanning a Slack for Enterprise App
- Begin Scanning a Workplace by Facebook App (Beta)

Begin Scanning an Amazon S3 App

As you prepare to scan your Amazon S3 account, take note of the following values, as they are required to complete the setup of the Amazon S3 app on Prisma SaaS:

Item	Description
AWS account ID	Required to enable the Amazon S3 Bucket created in CloudTrail.

Item	Description
Access key ID	Grants Prisma SaaS permission to access Amazon S3.
Secret access key	The administrator root access key used to configure IAM services.
CloudTrail bucket name (or full path if the CloudTrail feature is already enabled)	Enables the Amazon S3 app to log management and data events to a CloudTrail bucket of your choice.
Region	A configured area in CloudTrail that is scanned.
Role	When scanning multiple AWS S3 accounts, each IAM role defines a set of permissions that grant access to actions and resources in AWS.

- Complete the setup steps to Scan a Single Amazon S3 Account
- Complete the setup steps to Cross Account Scan Multiple Amazon S3 Accounts
- Add the Amazon S3 App to Prisma SaaS when your scan setup is complete.

Scan a Single Amazon S3 Account

Before you can scan an Amazon S3 app, you must configure AWS IAM policy, user, role, and (optional) an S3 bucket in which CloudTrail will log events that occur in your Amazon S3 buckets.

To configure the Amazon S3 app to scan a single AWS account:

STEP 1 | Log in to your AWS Console aws.amazon.com.

STEP 2 | Select **Services** > **Security, Identity & Compliance** > **IAM**.

STEP 3 | Configure the Prisma SaaS policy used to connect to the Amazon S3 app.

1. Select **Policies** > **Create policy** and then select **Create Your Own Policy**.
2. Enter the **Policy Name** as **`prisma-saas-s3-policy`** and provide an optional description of the policy.
3. Copy and paste the following configuration into the **Policy Document** section:

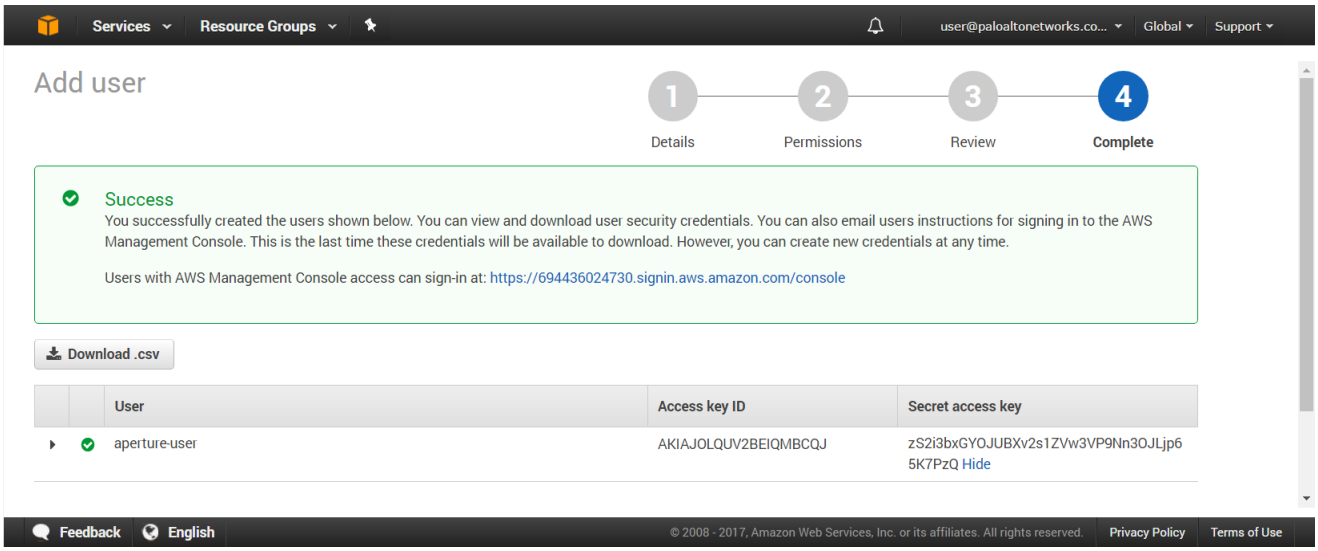
```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "s3:Get*",
               "s3:List*",
               "s3:Put*",
               "s3:Delete*",
               "s3:CreateBucket",
```

```
                "iam:GetUser",
                "iam:GetRole",
                "iam:GetUserPolicy",
                "iam:ListUsers",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:DescribeTrails",
                "cloudtrail:LookupEvents",
                "cloudtrail:ListTags",
                "cloudtrail:ListPublicKeys",
                "cloudtrail:GetEventSelectors",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcs",
                "config:Get*",
                "config:Describe*",
                "config:Deliver*",
                "config:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Click **Create Policy**.

STEP 4 | Configure the account Prisma SaaS will use to access the Amazon S3 logs:

1. Select **Users** > **Add user**.
2. Enter the user name as **`prisma-saas-s3-user`**.
3. To generate an access key ID and secret access key for Prisma SaaS to use to access the Amazon S3 service, enable Programmatic access.
4. Select **Next: Permissions**.
5. Select Attach existing policies directly.
6. Search for and select the check box next to the prisma-saas-s3-policy you created in the previous step.
7. Click **Next: Review** > **Create User**.



Note your Access key ID and Secret access key.

8. Click **Close**.

STEP 5 | If you have not already done so, configure CloudTrail logging. This enables the Amazon S3 app to log management and data events to the CloudTrail buckets of your choice.

1. To copy your AWS account ID into memory, click your username at the top right and copy the Account number. You will need your account number later in this procedure.
2. Select **Services** > **Management Tools** > **CloudTrail** > **Trails** > **Add new trail**.
3. Enter the Trail name **`prisma-saas-s3-trail`**.
4. Set **Apply trail to all Regions** to **Yes**.
5. In the **Data events** area, enter the name of each bucket that you want Prisma SaaS to scan. You can also choose **Select all S3 buckets in your account** to enable Prisma SaaS to scan all of your S3 buckets. The interface offers auto-completion as you type. Repeat the process to select additional buckets.
6. To create a bucket in which CloudTrail will store management and data event logs, enter the **S3 bucket** name as **`prisma-saas-s3-<AWS account ID>`** in the **Storage location** area.

   Take note of the S3 bucket (CloudTrail bucket name) and region.
7. Click **Create**.

STEP 6 | You can now Add the Amazon S3 App to Prisma SaaS.

Cross Account Scan Multiple Amazon S3 Accounts

To enable scanning of S3 buckets across multiple AWS accounts, you must Begin Scanning an Amazon S3 App AWS IAM policy, user, and role on the primary account, and then configure users, roles, policies and CloudTrail trails for both the primary and secondary accounts. The account in which all CloudTrail is stored is referenced as the primary account. All other accounts are referenced as secondary accounts.

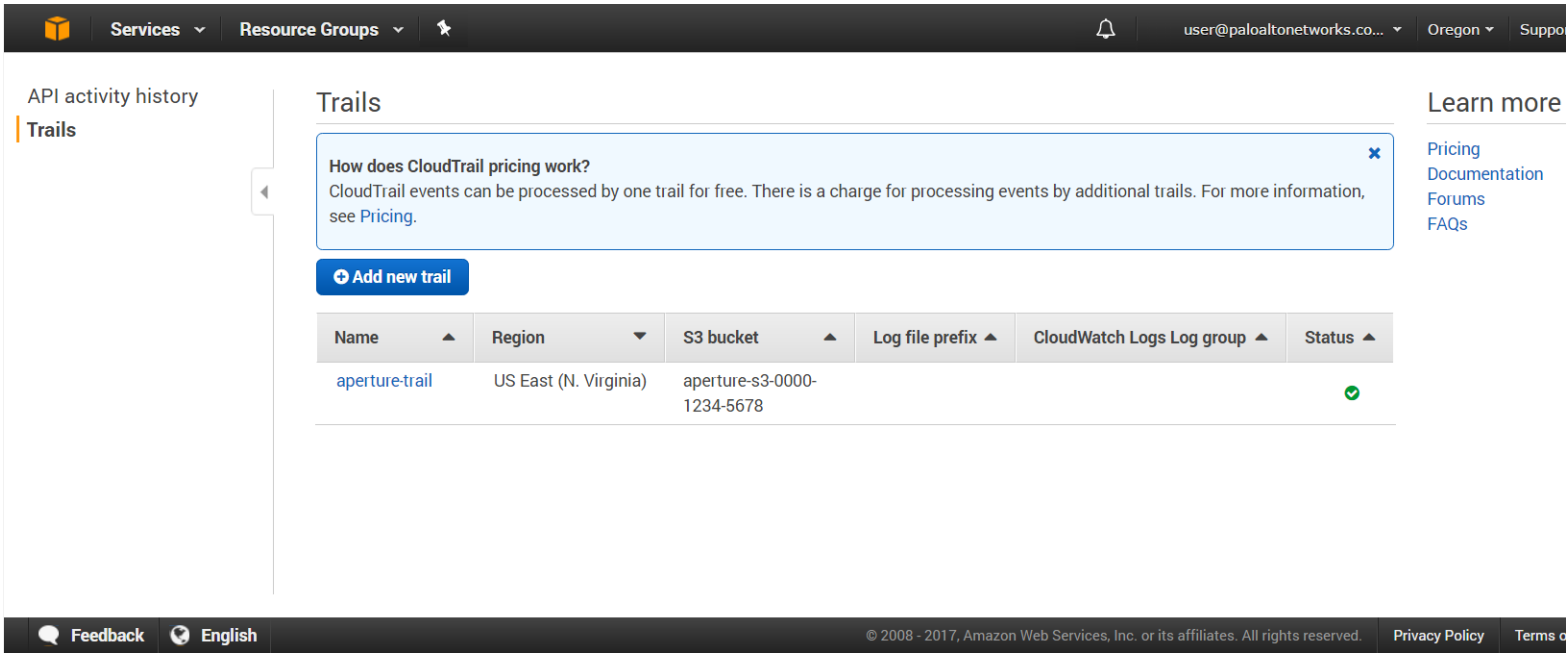
To configure AWS S3 scanning across multiple accounts:

STEP 1 | Configure CloudTrail on the primary account.

1. Log in to your AWS Console aws.amazon.com.
2. Select **Services** > **CloudTrail** > **Trails** > **Create Trail**.
3. Enter the Trail name **`prisma-saas-s3-primary-trail`**.
4. Set **Apply trail to all Regions** to **Yes**.
5. In the **Data Events** area, enter the name of each S3 bucket that want to enable scanning on your primary account. You can also choose **Select all S3 buckets in your account** to enable Prisma SaaS to scan all of your S3 buckets in your primary account.
6. In the **Storage location** area, create a bucket in which CloudTrail will store management and data event logs, enter the **S3 bucket** name as **`prisma-saas-s3-<AWS account ID>`**.

   You can also use an existing bucket for the log storage location, if one exists.



STEP 2 | Configure a role and an associated policy on each secondary account.

1. Log in to your AWS Console aws.amazon.com.
2. Configure an IAM role by selecting **IAM** > **Roles** > **Create Role**.
3. Select **Another AWS Account Type** as type of trusted entity.
4. Enter the AWS account number of your primary account in **Specify accounts that can use this role**. Leave the other **Options** unchecked and select **Next: Permissions**.
5. Click **Create Policy** and a new window will open.
6. Click the **JSON** tab and copy and paste the following configuration into the **Policy Document** section:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "s3:Get*",
               "s3:List*",
               "s3:Put*",
               "s3:Delete*",
               "s3:CreateBucket",
               "iam:GetUser",
               "iam:GetRole",
               "iam:GetUserPolicy",
               "iam:ListUsers",
               "cloudtrail:GetTrailStatus",
               "cloudtrail:DescribeTrails",
               "cloudtrail:LookupEvents",
               "cloudtrail:ListTags",
               "cloudtrail:ListPublicKeys",
               "cloudtrail:GetEventSelectors",
               "ec2:DescribeVpcEndpoints",
               "ec2:DescribeVpcs",
               "config:Get*",
```

```
                "config:Describe*",
                "config:Deliver*",
                "config:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

7. Click **Review Policy** and enter the **Policy Name** as **`prisma-saas-s3-secondary-policy`** and provide an optional description of the policy.
8. Click **Create Policy**.
9. **Refresh** the policy window and select **prisma-saas-S3-secondary-policy**.
10. Select **Next: Review** and enter the role name **`prisma-saas-s3-secondary-role`**.
11. Create the role by entering in **Role name**. Before creating the role, verify the following:
    1. **Trusted entities** contain the primary account number.
    2. **prisma-saas-s3-secondary policy** displays in **Policies**.
    3. When verification is complete, click **Create Role**.
12. Select the role just created and copy the role ARN into memory (for example **`arn:aws:iam::222222222:role/prisma-saas-s3-secondary-role`**). You will need the role ARN later in this procedure.

STEP 3 | Configure the CloudTrail bucket in the primary account to give CloudTrail service access to each secondary account prefix.

1. Log in to your AWS Console aws.amazon.com.
2. Select **Services** > **S3**.
3. Select the CloudTrail S3 bucket you just created, for example **prisma-saas-s3-[aws account id].**
4. Select **Permissions** > **Bucket Policy**.
5. Verify that the bucket policy has a **Statement to Allow Action S3:PutObject** for the primary account prefix, for example, **`“Resource”: “arn:aws:s3:::prisma-saas-s3-[aws account id]/AWSLogs/[aws account id]/*”,`**
6. Modify this resource entry to add the account prefix for each secondary account, similar to the following:

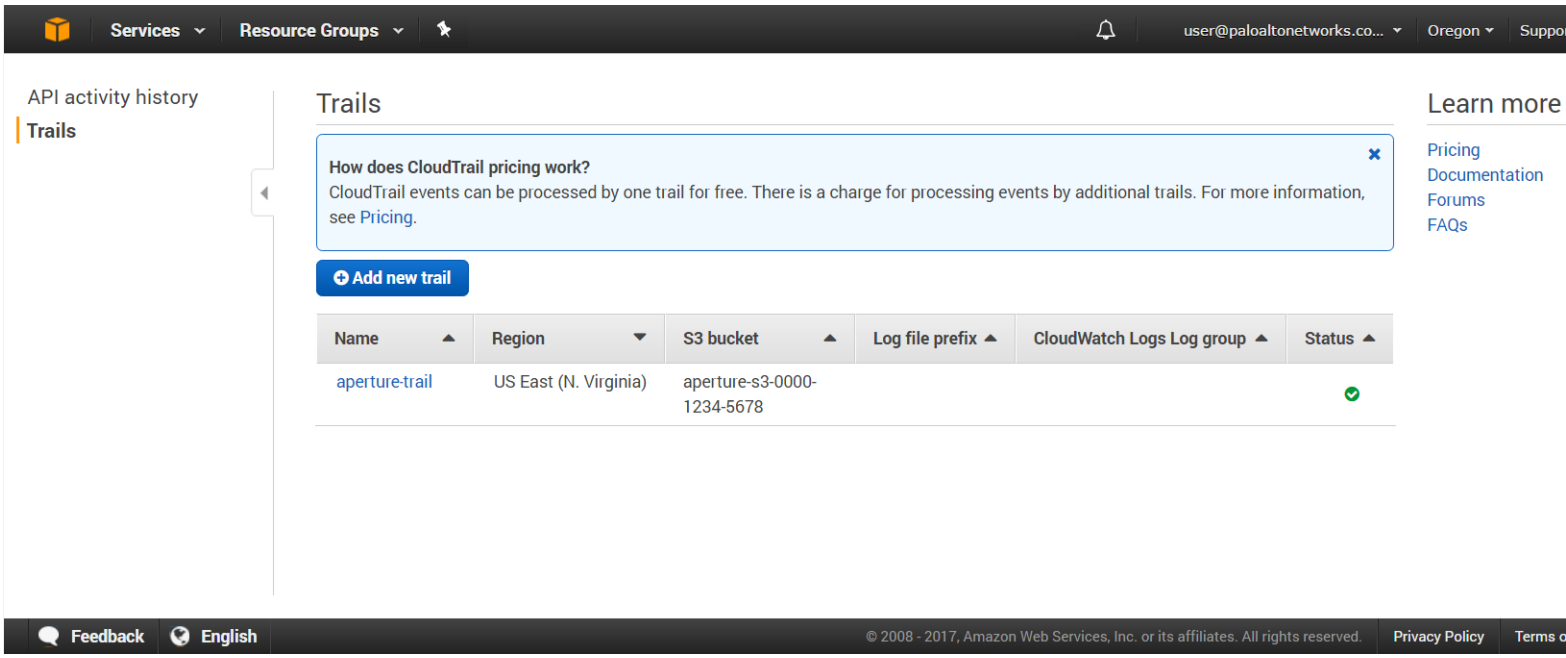
```
 "Resource":
 [
 "arn:aws:s3:::prisma-saas-s3-[aws account id]/AWSLogs/[aws account id]/
*",
 "arn:aws:s3:::prisma-saas-s3-[aws account id]/AWSLogs/111111111/*",

 "arn:aws:s3:::prisma-saas-s3-[aws account id]/AWSLogs/222222222/*",

 "arn:aws:s3:::prisma-saas-s3-[aws account id]/AWSLogs/333333333/*"

 ],
```

7. **Save** the resource modification.

STEP 4 | Configure CloudTrail on each secondary account to associate with the primary account.

1. Select **Services** > **CloudTrail** > **Trails** > **Create trail**.
2. Enter the Trail name **`prisma-saas-s3-secondary-trail`**.
3. Set **Apply trail to all Regions** to **Yes**.

4. In the **Data events** area, enter the name of each bucket in your secondary account for which you want to enable scanning. You can also choose **Select all S3 buckets in your account** to enable Prisma SaaS to scan all of your secondary S3 buckets. The interface offers auto-completion as you type. Repeat the process to select additional buckets.
5. To configure a bucket in which CloudTrail will store management and data event logs for this account, enter the bucket name of the CloudTrail bucket in the primary account, for example **`prisma-saas-s3-<AWS account ID>`** in the **Storage location** area and click **Create**.



STEP 5 | Configure a user in the primary account that will access each of the secondary accounts.

1. Select **Services** > **IAM**.
2. Select **Users** > **Add user**.
3. Enter the user name as **`prisma-saas-s3-user`**.
4. Select **Programmatic access** to generate an access key ID and secret access key for Prisma SaaS to use to access the Amazon S3 service.
5. Select **Next: Permissions**.
6. Create a user policy.
    1. Select **Attach existing policies directly** > **Create Policy**. A new window will open. You will attach this policy to the user account that authorizes Prisma SaaS to scan the Amazon S3 accounts.
    2. Click the **JSON** tab and copy and paste the following configuration into the **Policy Document** section:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3:Get*",
    "s3:List*",
    "s3:Put*",
    "s3:Delete*",
    "s3:CreateBucket",
```

```
    "iam:GetUser",
    "iam:GetRole",
    "iam:GetUserPolicy",
    "iam:ListUsers",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudtrail:ListTags",
    "cloudtrail:ListPublicKeys",
    "cloudtrail:GetEventSelectors",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcs",
    "config:Get*",
    "config:Describe*",
    "config:Deliver*",
    "config:List*"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::111111111:role/prisma-saas-s3-cross-account-
access-role"
  },
  {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::222222222:role/prisma-saas-s3-cross-account-
access-role"
  },
  {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::333333333:role/prisma-saas-s3-cross-account-
access-role"
  }
 ]
}
```

This policy document has three pseudo secondary accounts 222222222,111111111,333333333 referenced in it. You will need to edit the policy to reflect the account numbers of each of your secondary accounts.

7. Click **Review Policy** and enter the **Policy Name** as **`prisma-saas-s3-primary-policy`** and provide an optional description of the policy.
8. Click **Create Policy**.
9. **Refresh** the first window and select **prisma-saas-s3-primary policy**, and click **Next** > **Review** and then **Create User**.

Note the Access key ID and Secret access key for the user. You will need these numbers later in this setup.

10. Click **Close**.

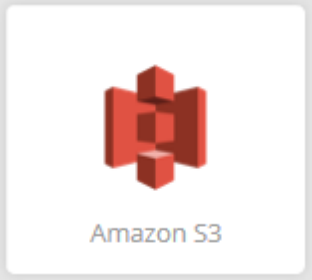
STEP 6 | You can now Add the Amazon S3 App to Prisma SaaS.

Add the Amazon S3 App to Prisma SaaS

When scan setup is complete, you can add the Amazon S3 app to Prisma SaaS and begin scanning your new Amazon S3 app for policy violations.

STEP 1 | Add the Amazon S3 app to Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Amazon S3**.



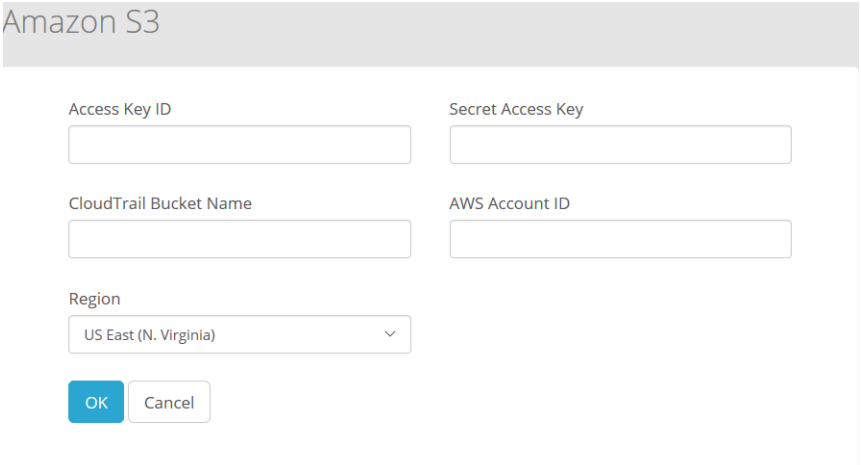
STEP 2 | Configure your Amazon S3 settings. There are two methods to set up the Amazon S3 app on Prisma SaaS based on whether you are configuring a account or accounts.

STEP 3 | Connect a single AWS account.

1. Connect a single AWS account by clicking **Connect to Account**.
2. Enter the **Access Key ID** and **Secret Access Key** that you noted earlier when you completed the Begin Scanning an Amazon S3 App for your app scan.
3. Enter the **CloudTrail Bucket Name** (S3 bucket name).

   Because S3 allows your bucket to be used as a URL that can be accessed publicly, the bucket name that you choose must be globally unique. If some other account has already created a bucket with the name that you chose, you must use another name.
4. Enter the **AWS Account ID**.

   To find your AWS account ID number on the AWS Management Console, select Support on the navigation bar on the upper-right, and then select Support Center. Your signed-in account ID displays in the upper-right corner below the Support menu.
5. Select the **Region**.
6. Click **OK**. Prisma SaaS adds the Amazon S3 app to the list of Cloud Apps.



STEP 4 | Connect multiple AWS accounts.

AWS allows you to combine CloudTrail log files from multiple AWS regions and separate accounts into a single S3 bucket. Aggregating your log files in a single bucket simplifies storage and management of your Trails.

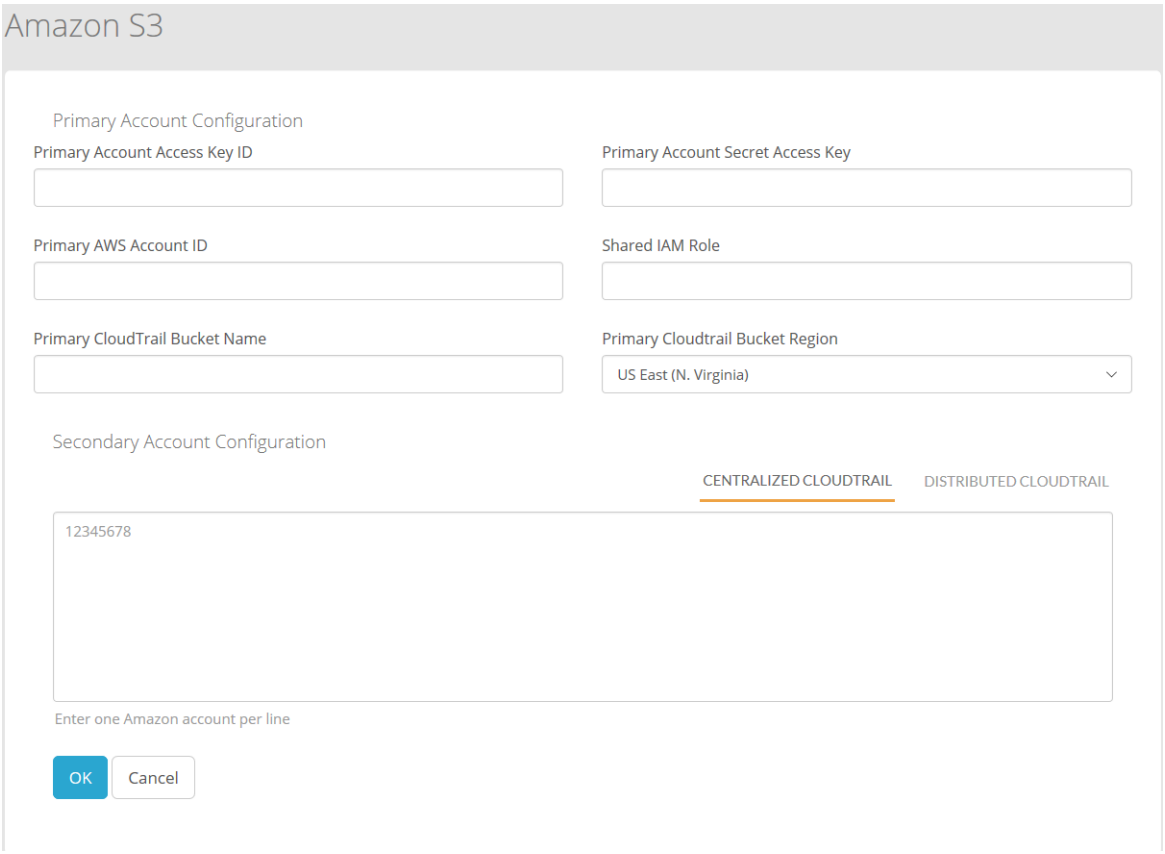
1. Enter the **Primary Account Access Key ID** and **Primary Account Secret Access Key** that you noted earlier when you completed the Begin Scanning an Amazon S3 App for your app scan.
2. Enter the **Primary AWS Account ID**.

   To find your AWS account ID number on the AWS Management Console, select Support on the navigation bar on the upper-right, and then select Support Center. Your signed-in account ID displays in the upper-right corner below the Support menu.
3. Enter the **Shared IAM Role**.

   The shared IAM role delegates access to resources in different AWS accounts that you own (Production and Development). By configuring cross-account access with a role, you don't need to create individual IAM users in each account. In addition, users don't have to sign out of one account and sign into another in order to access resources that are in different AWS accounts.
4. Enter the **Primary CloudTrail Bucket Name** (S3 bucket name).

   Because S3 allows your bucket to be used as a URL that can be accessed publicly, the bucket name that you choose must be globally unique. If some other account has already created a bucket with the name that you chose, you must use another name.
5. Select the **Primary CloudTrail Bucket Region**.
6. In **Secondary Account Configuration** select a CloudTrail configuration:
   - **Centralized CloudTrail**— logging for all AWS accounts goes to a single CloudTrail bucket in the primary account. Enter one Amazon account per line with no delimiters.
   - **Distributed CloudTrail**— logging for each AWS account goes to a separate CloudTrail bucket in the account's location. Enter one **`Amazon Account: Bucket Name: Region`** per line with a colon (:) as a delimiter.

   If you are configuring both centralized and distributed CloudTrails, use Distributed CloudTrail.
7. Click **OK** to add the Amazon S3 app to the list of Cloud Apps on Prisma SaaS.



STEP 5 | (Optional) Give a descriptive name to this app instance and specify an incident reviewer.

1. Select the Amazon S3 link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Amazon S3 from other instances you are managing.

STEP 6 | Define global scan settings.

- Define Your Internal Domains
- Define Trusted and Untrusted Users and Domains
- Enable Data Masking

STEP 7 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for incidents unique to the assets in the new app.

STEP 8 | (Optional) Configure or edit a data pattern.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 9 | Start scanning the new Amazon S3 app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.

2. In the Cloud Apps row that corresponds to the new Amazon S3 app, select **Actions** > **Start Scanning**.

   The status changes to Scanning. Prisma SaaS starts scanning all assets in the associated Amazon S3 app and begins identifying incidents. Depending on the number of Amazon S3 assets, it may take some time for the service to complete the process of discovering all assets and users. However, as soon as you begin to see this information populating on the Prisma SaaS **Dashboard**, you can begin to Assess Incidents.

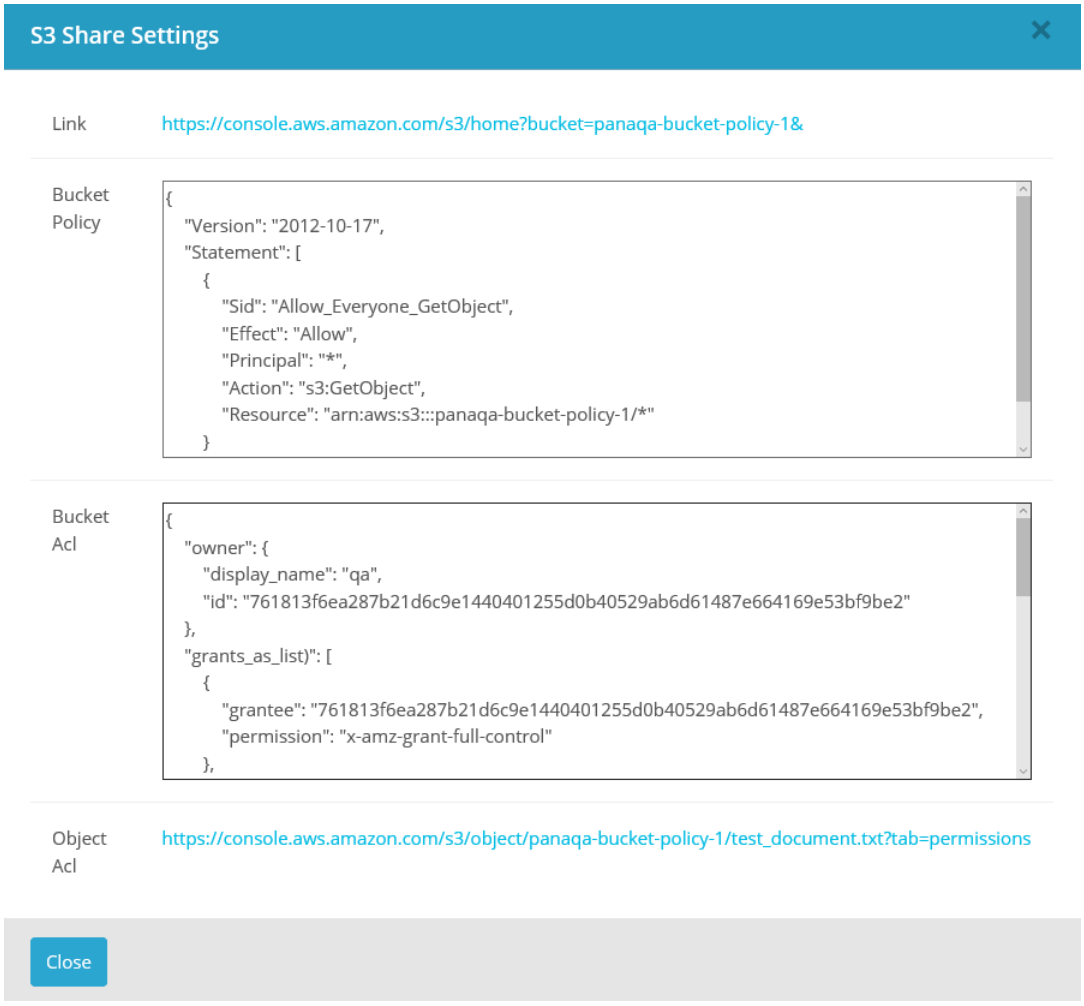
STEP 10 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective.

Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

STEP 11 | Review exposure details.

1. To get more details on the exposure, select a **Bucket** to view the **S3 Share Settings**. This view displays the bucket policy and access control lists (ACL) with a link to the asset in the associated bucket so that you can get more context into the exposure.



Begin Scanning an Amazon Web Services App

Prisma SaaS has deprecated support for the Amazon Web Services app. To continue monitoring your resources deployed on AWS, try Prisma Cloud.

Before you can begin monitoring an Amazon Web Services app, you must configure Prisma SaaS policy, user, and (optional) an Amazon bucket for CloudTrail to log events in. As you configure your Amazon Web Services account, note the following values required to complete the setup of the Amazon Web Services app on Prisma SaaS:

Item	Description
AWS account ID	Required to enable the Amazon Web Services Bucket created in CloudTrail.
Access key ID	Grants Prisma SaaS permission to access Amazon Web Services.
Secret access key	The administrator root access key used to configure IAM services.
CloudTrail bucket name (or full path if the CloudTrail feature is already enabled)	Enables the Amazon Web Services app to log management and data events to a CloudTrail bucket of your choice.
Region	The monitored CloudTrail region.

To begin monitoring an Amazon Web Services app:

STEP 1 | Prepare your Amazon Web Services account to work with Prisma SaaS.

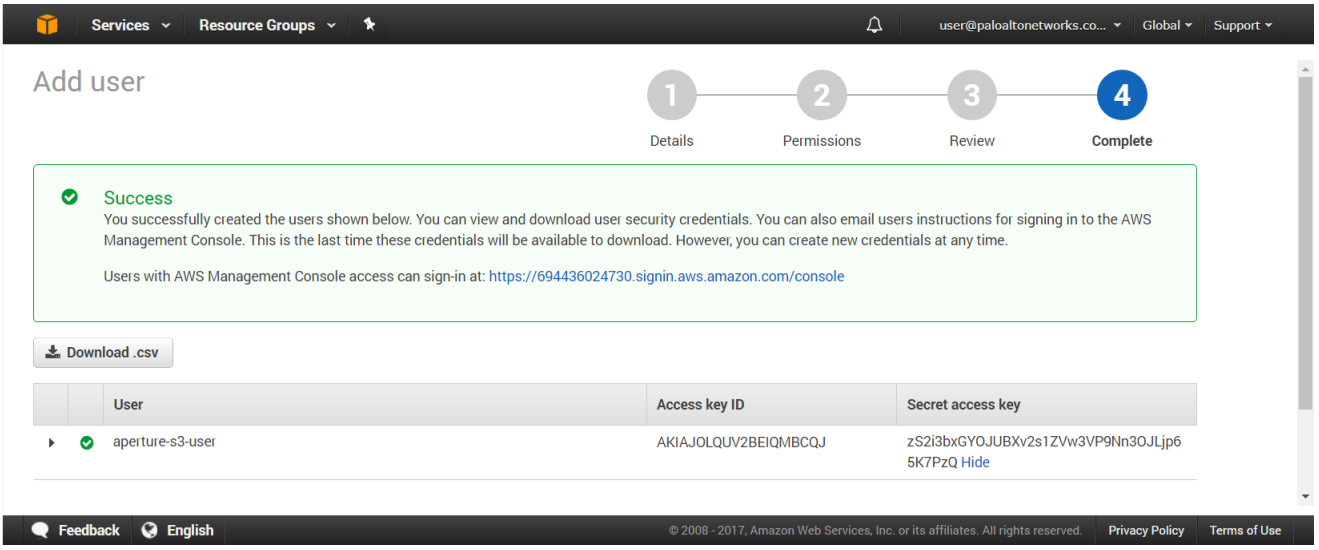
1. Log in to the AWS Console (aws.amazon.com).
2. Select **Services** > **Security, Identity & Compliance** > **IAM**.
3. Configure the Prisma SaaS policy to connect to the Amazon Web Services app.
    1. Select **Policies** > **Create policy** and then select **Create Your Own Policy**.
    2. Enter the **Policy Name** as **`prisma-saas-aws-policy`** and provide an optional description of the policy.
    3. Copy and paste the following configuration into the **Policy Document** section:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
```

```
"ec2:DescribeInstances",
"ec2:DescribeSecurityGroups",
"ec2:DescribeImages",
"ec2:DescribeVolumes",
"iam:List*",
"iam:Get*",
"kms:ListKeys",
"kms:DescribeKey",
"kms:GetKeyRotationStatus",
"cloudtrail:GetTrailStatus",
"cloudtrail:DescribeTrails",
"cloudtrail:LookupEvents",
"cloudtrail:ListTags",
"cloudtrail:ListPublicKeys",
"cloudtrail:GetEventSelectors"
],
"Resource": "*"
}
]
}
```

4. Click **Create Policy**.

4. Configure the account Prisma SaaS will use to access the Amazon Web Services logs:
    1. Select **Users** > **Add user**.
    2. Enter the username as **`prisma-saas-aws_ec2_and_iam-user`**.
    3. To generate an access key ID and secret access key for Prisma SaaS to use to access the Amazon Web Services service, enable **Programmatic access**.
    4. Select **Next: Permissions**.
    5. Select **Attach existing policies directly** and select the policy **`prisma-saas-aws_ec2_and_iam-policy`**.
    6. Search for and select the check box next to the policy you created in the previous step.
    7. Click **Next: Review** > **Create User**.

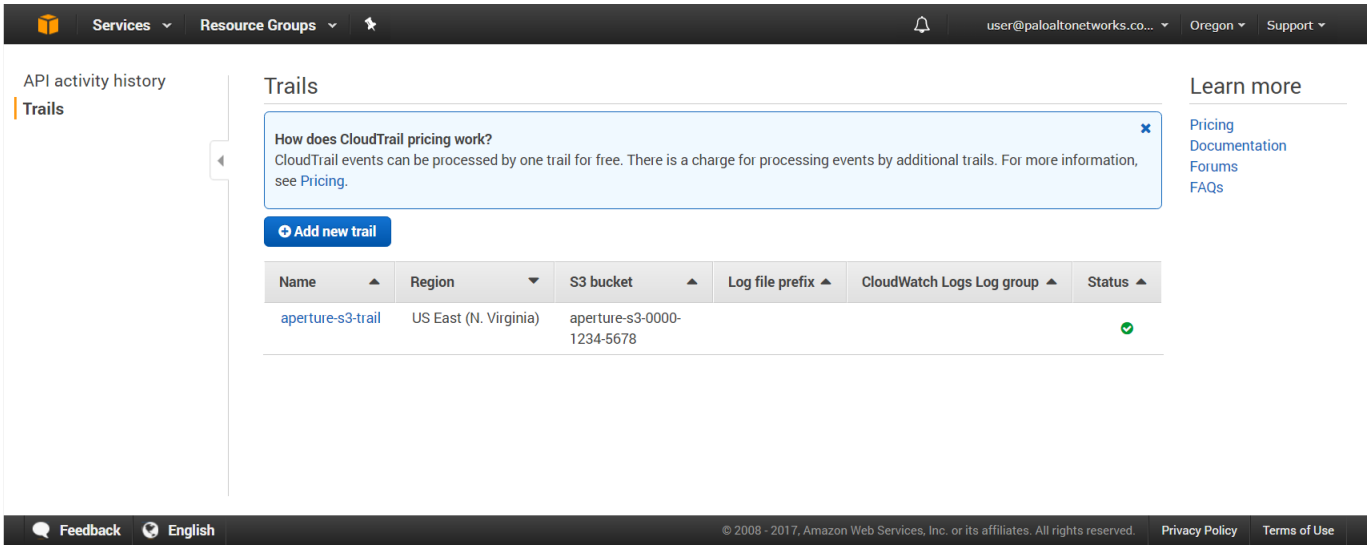


Note your Access key ID and Secret access key.

8. Click **Close**.

5. (Optional) If you have CloudTrail logging enabled for all regions, skip this step, if not, configure CloudTrail logging. This feature enables the Amazon Web Services app to log management and data events to a CloudTrail bucket of your choice.

   1. To copy your AWS account ID into memory, click on your username at the top right, select the Account number, and press **Ctrl-C**. You will need the number later in this procedure.
   2. Select **Services** > **Management Tools** > **CloudTrail** > **Trails** > **Add new trail**.
   3. Enter the Trail name **`prisma-saas-aws_ec2_and_iam-trail`**.
   4. Set **Apply trail to all Regions** to **Yes**.
   5. To create a bucket in which CloudTrail will store management and data event logs, enter the **S3 bucket** name as **`prisma-saas-aws_EC2<AWS account ID>`** in the **Storage location** area.



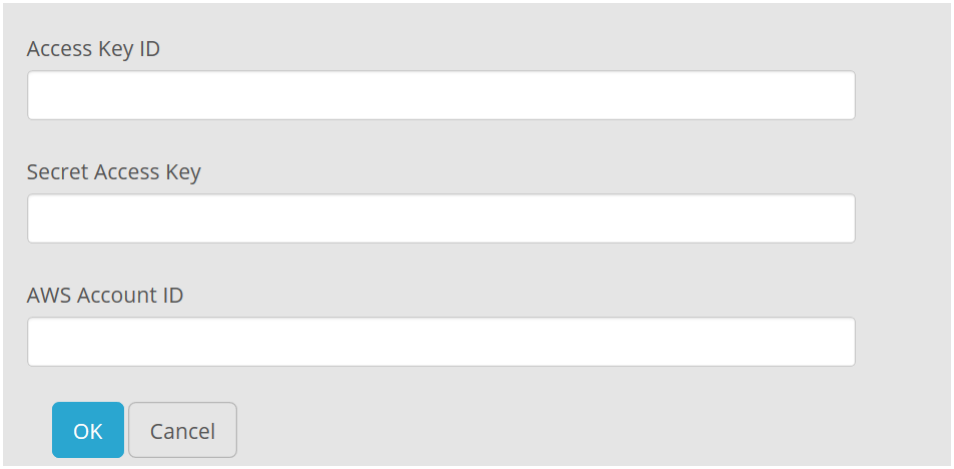
Take note of the AWS bucket (CloudTrail bucket name).

6. Click **Create**.

STEP 2 | Add the Amazon Web Services app to Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Amazon Web Services**.

3. Configure your Amazon Web Services settings. There are two methods to set up the Amazon Web Services app on Prisma SaaS based on whether you already had CloudTrail logging set up in your AWS account or if you set it up per the instructions in this procedure.
   - **New CloudTrail configuration**
     1. Click **Connect to Account**.



     2. Enter the **Access Key ID**, **Secret Access Key**, and the **AWS Account ID**, you noted in the previous steps.
4. Click **OK**.

   Prisma SaaS adds the Amazon Web Services app to the list of Cloud Apps.

STEP 3 | (Optional) Give a descriptive name to this app instance and specify an incident reviewer.

1. Select the Amazon Web Services link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Amazon Web Services from other instances you are managing.

STEP 4 | Define global settings.

- Define Your Internal Domains
- Define Trusted and Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically monitors the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for incidents unique to the new app.

STEP 6 | (Optional) Configure or edit a data pattern.

When you add a new cloud app, Prisma SaaS automatically monitors the app against the default data patterns and displays the match occurrences. You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start monitoring the new Amazon Web Services app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Amazon Web Services app, select **Actions** > **Start Scanning**.

   Prisma SaaS starts monitoring all assets in the associated Amazon Web Services app and begins identifying incidents. Depending on the number of Amazon Web Services assets, it may take some time for the service to complete the process of discovering all assets and users. However, as soon as you begin to see this information populating on the Prisma SaaS **Dashboard**, you can begin to Assess Incidents.

STEP 8 | Monitor the results.

As Prisma SaaS starts monitoring files and matching them against enabled policy rules, Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective. Monitoring the progress during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Box App

If you plan to use Selective Scanning using Azure Active Directory, you must connect Azure Active Directory before adding your Box application so Prisma SaaS can discover and scan assets belonging to the user groups you want to monitor. To begin scanning a Box instance:

STEP 1 | Ensure that the Box account you plan to use with Prisma SaaS has sufficient privileges.

Enabling the Edit settings for your company option suppresses email notifications. If you do not enable this setting, every collaborator on an asset receives an email notification each time Prisma SaaS accesses an asset. When you suppress email notification, actions will still appear in the user's update feeds and in the audit logs.

To connect Prisma SaaS, log in to a Box account with Administrator privileges. Make sure the following settings are enabled:

1. From within Box, select **Admin Console** > **Users and Groups** and select the Administrator account you want to use.
2. **Allow this user to see all managed users**.

STEP 2 | Add the Box application to Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, select **Add a Cloud App**.
2. Select **Box**.

3. Click **Connect to Box Account**.
4. Enter the email address and password for the Administrator account you want Prisma SaaS to use when connecting to Box and then click **Authorize**.

   Prisma SaaS validates the administrator account and if the account has the right authentication permissions to access all the Box assets. If the account does not have adequate permissions, an on-screen status displays an error alerting you to fix the issue.
5. After authentication succeeds, select **Grant access to Box**.

   The new Box instance is added to the list of Cloud Apps as Box *n*, where *n* is the number of Box instances you have connected to Prisma SaaS. For example, if this is the second Box instance connected, the name displays as Box 2.

STEP 3 | (Optional) Give a descriptive name to this instance and specify an incident reviewer.

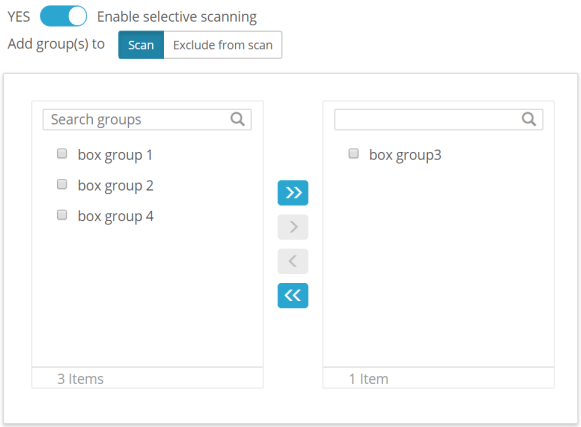
1. Select the Box *n* link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Box from other instances you are managing.
3. Specify an **Incident Reviewer Account**. Use this setting with caution because the account you provide becomes a collaborator on all risks — even private files.
4. Click **Done** to save your changes.

STEP 4 | (Optional) Choose the user groups whose assets and accounts you want to monitor.

Begin Selective Scanning Using Azure Active Directory Groups for users who belong to specific groups on if you want Prisma SaaS to scan content. By default, selective scanning is not enabled. If you want to enable selective scanning later, you must delete the Box instance and add it back so Prisma SaaS can discover all assets and events for all users. All assets and events previously stored will be deleted and incidents reported for users no longer included in the selected groups are automatically closed.

1. Select **Enable selective scanning** and choose the groups you want to include or exclude from scanning from the list of groups using >> to add all groups or > to add selected groups.

   If a group is edited or removed from selective scanning, it can take up to 7 days to remove assets or activities, and close any related incidents. Adding a group back to selective scanning will record new user activities but not old, previously removed user activities.



2. Select **Save** to continue.

STEP 5 | Define global scan settings.

- Define Your Internal Domains
- Define Trusted and Untrusted Users and Domains
- Enable Data Masking

STEP 6 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for incidents unique to Box.

STEP 7 | (Optional) Configure or edit a data pattern.

When you Prisma SaaS scans the Box assets, sometimes the data patterns do not meet your business needs or return enough incidents. You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 8 | Start scanning assets on the Box instance.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Box app, select **Actions** > **Start Scanning**.

   Prisma SaaS starts scanning all assets in the associated Box instance and begins to identify incidents. Depending on the number of Box users and assets, it may take some time for the service to complete the process. However, as soon as you begin to see this information populating on the Prisma SaaS **Dashboard**, you can begin to Assess Incidents.

STEP 9 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, you can Monitor Scan Results on the Dashboard (Basic DLP) to verify that the policy rules are effective. Monitoring the progress of the scan during the discovery phase enables you toFine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Cisco Webex Teams App (Beta)

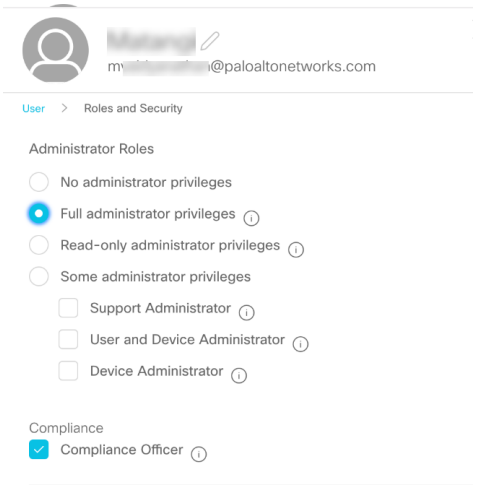
Prisma SaaS scans messages and files shared on spaces within the Cisco Webex Teams application. To begin scanning a Cisco Webex Teams application:

STEP 1 | Ensure that the Webex Teams account you plan to use with Prisma SaaS has sufficient privileges.

To connect a Webex Teams instance to Prisma SaaS, you must use a Webex Teams account with Administrator privileges. Make sure the following settings are enabled:

1. Log in to https://admin.webex.com, select **Users** > **admin_account_username** > **Roles and Security**.
2. Enable **Full administrator** and **Compliance Officer** privileges.

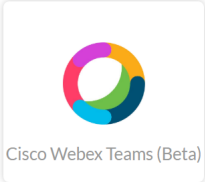
   Make sure to request another administrator to assign the Compliance Officer role to you, so your account has the correct privileges required to search for sensitive information in the Cisco Webex Teams app.



The Webex Teams standard service plan supports data generated during the last 90 days. To enable longer-term visibility, consider upgrading to Cisco Webex Teams Pro Pack service plan before connecting to Prisma SaaS.

STEP 2 | Add the Webex Teams app.

1. From the Prisma SaaS **Dashboard**, select **Add a Cloud App**.
2. Select the **Cisco Webex Teams** app.



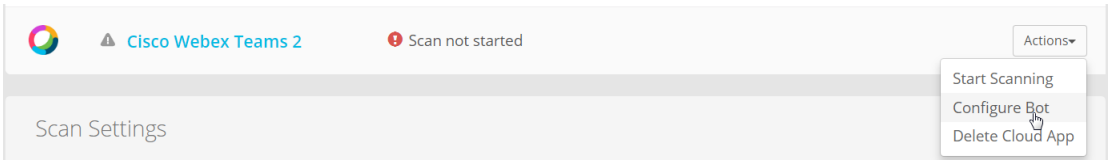
3. **Connect to Webex Teams Account**.
4. Prisma SaaS redirects you to Cisco identity broker to authorize access so that you can enter the email address and password for the Administrator account you want to use when connecting to the Webex Teams application.
5. Review and **Accept** the permissions to onboard the account to Prisma SaaS.

   The new Webex Teams instance is added to the list of Cloud Apps as Webex Teams *n,* where *n* is the number of Webex Teams instances you have connected to Prisma SaaS. For example, if this is the second Webex Teams instance you connected to Prisma SaaS, the name displays as Webex Teams 2.

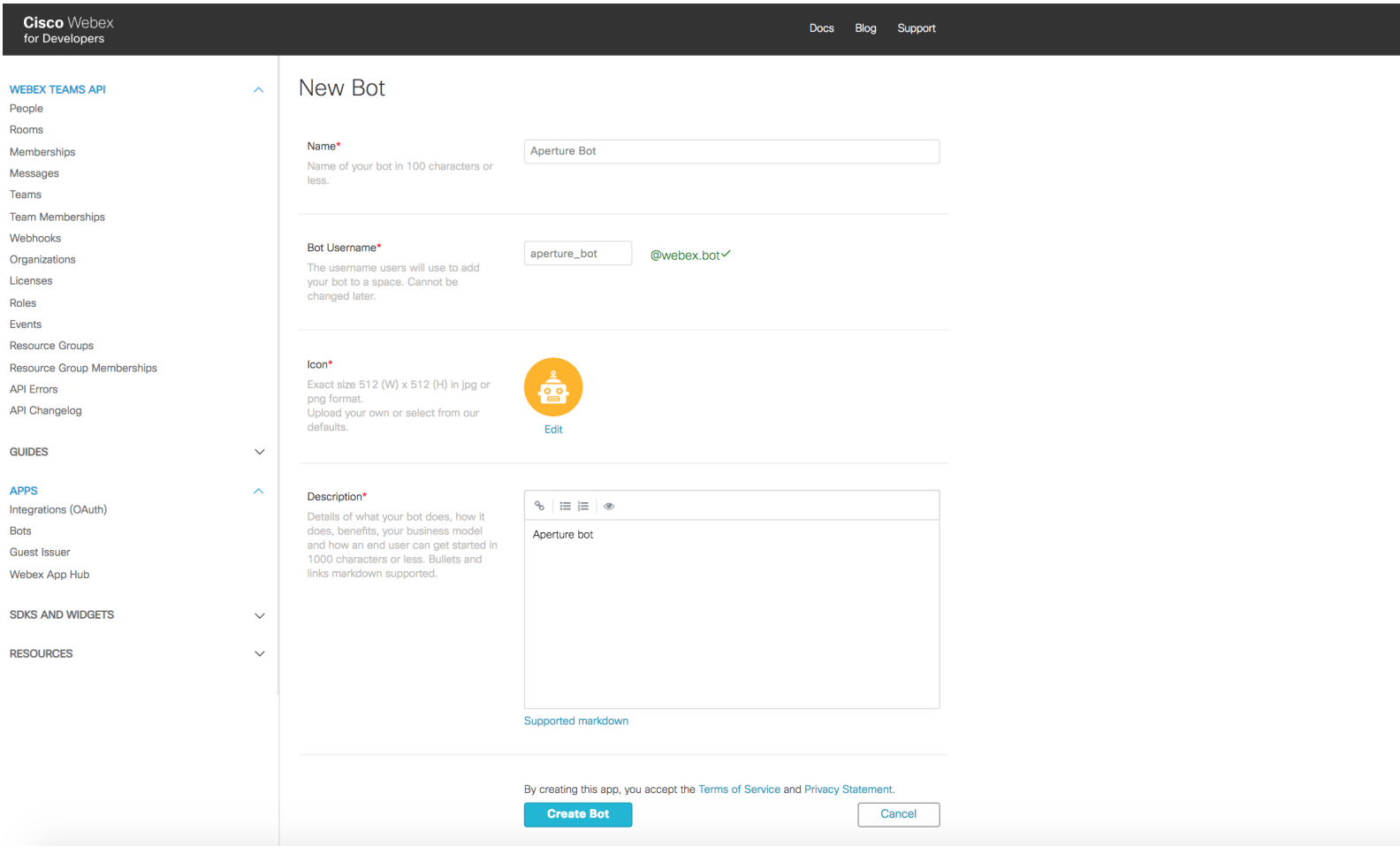
   If you want to give a descriptive name for the instance, select the link on **Settings** > **Cloud Apps & Scan Settings**, and enter a new name.

STEP 3 | Configure a bot.

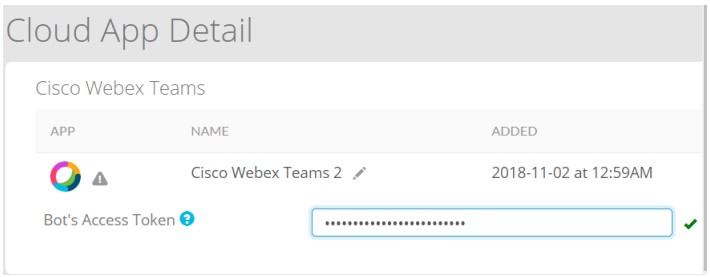
A bot is a machine account that automates the process of sending messages to users on your behalf. To use a bot, you must create an access token to enable the bot to send these messages. When you Add a New Asset Rule, select the **Notify via bot** auto-remediation action, and Prisma SaaS will send a direct message on Webex Teams to the user whose messages or files triggered the incident. If you do not create a bot, Prisma SaaS sends a message using the administrator's name to the space where the user originally shared the file or message.



1. Create a bot on the Webex developer portal using your administrator credentials, and copy the access token.



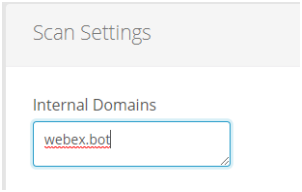
2. Select **Actions** > **Configure Bot** on **Settings** > **Cloud Apps & Scan Settings**
3. Paste the access token on the app, and save your changes.



STEP 4 | Define global scan settings.

- Define Your Internal Domains

When you add the Webex bot, Prisma SaaS automatically adds **webex.bot** to the list of internal domains to ensure that the bot activity is restricted to the internal domain. Do not delete this entry from the list.



- Define Trusted and Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules or edit existing policy rules.

When you add a new cloud application, Prisma SaaS automatically scans assets against the default data patterns and displays the match occurrences. If you want to generate incidents and identify potential issues that are unique to the new instance, as a best practice consider the business use of your app to determine whether you want to Add a New Asset Rule.

STEP 6 | (Optional) Configure or edit a data pattern.

If you find the existing data patterns do not identify the incidents you want to prevent from occurring, you can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the Cisco Webex Teams instance for issues.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Webex Teams instance, select **Actions** > **Start Scanning**.

   Prisma SaaS starts scanning all assets—files, messages—and spaces in the associated Webex Teams application and identifies incidents. Depending on the number of Webex Teams users and assets, it may take some time for the service to complete the process. However, as soon as you begin to see this information populating on the Prisma SaaS **Dashboard**, you can begin to Assess Incidents.

   On a Webex Teams account, Prisma SaaS monitors the following activities:

   - *Adding or removing a user from a space.*
   - *Adding a moderator to a space.*
   - *Deleting a message — the deletion of a message is logged if the message had a file attached to it, or if the message had a policy violation and created an incident.*

   All activities that occurred before you added the Cisco Webex Teams application to Prisma SaaS are not displayed on Explore > Activities.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, you can Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Citrix ShareFile App (Beta)

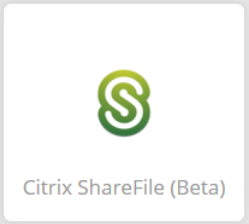
To begin scanning Citrix ShareFile application:

STEP 1 | Add your Citrix ShareFile domain(s) as an internal domain on Prisma SaaS.

The domain name can have multiple formats, such as **`YourSubdomain.citrixsharefile.com.`** See Define Your Internal Domains.

STEP 2 | Add the ShareFile app.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Citrix ShareFile**.



3. Enter the login credentials for an account with administrative privileges on the Citrix ShareFile page to which you are redirected to enable communication between Prisma SaaS and the ShareFile apps.
4. Review and **Accept** the changes so that Prisma SaaS can perform scans on your assets in ShareFile.

   Upon successful authentication, the new ShareFile app is added to the list of Cloud Apps as Citrix ShareFile *n,* where *n* is the number of ShareFile app instances that you have connected to Prisma SaaS, for example ShareFile1.

STEP 3 | (Optional) Give a descriptive name to this app instance.

1. Select the ShareFile instance on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of ShareFile from other instances you are managing.
3. Click **Done** to save your changes.

STEP 4 | Define global scan settings.

- Define Trusted and Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add Citrix ShareFile, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for incidents unique to the ShareFile.

STEP 6 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the new ShareFile app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new ShareFile app, select **Actions** > **Start Scanning**.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, you can Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Confluence App (Beta)

Before you can begin scanning a Confluence app, you must configure the application links required for authentication and communication between Prisma SaaS and your Confluence account. As you prepare the Confluence account, take note of the following values, as they are required to complete the setup of the Confluence app on Prisma SaaS:

Item	Description
Application URL	The Confluence URL entered in **Prisma SaaS** > **Confluence Custom Configuration**.
Consumer Key	Any descriptive name you assign in Confluence for the server's consumer key.
Public Key	The application's public key. This field is mandatory and its contents must match the public key supplied by Prisma SaaS.

STEP 1 | Prepare your Confluence account to connect to Prisma SaaS.

1. From the Prisma SaaS Dashboard, **Add a Cloud App**.
2. Select **Confluence**.

3. **Click here to prepare your Confluence Account**.
4. Log in to your Atlassian console with Administrator privileges (for example, **`https://acmecorp.atlassian.net/`**).
5. Configure the Application links.
    1. Click **Configure Application** > **Application Links**.
    2. Enter **`https://aperture.paloaltonetworks.com`**, and then **Create New Link**.
    3. Click **Continue** on any error messages.

    Note the Application URL located at the top of the window. You will need this URL later in this procedure.

    4. Enter **`Prisma SaaS`** in **Application Name** and **Confluence** in **Application Type**.
    5. Select **Create Incoming Link** to link Confluence to the Application URL.
    6. Click **Continue** to save your changes.
    7. Enter any value for **Consumer Key** and **Consumer Name**.

Take note of the Consumer Key.

6. Copy the **`Public Key`** from **Prepare Your Confluence Account** on Prisma SaaS and paste it into Confluence, **Link Applications**, and then **Continue**.
7. **Edit** the **Application Link** in **Connections** to set the **Incoming** option to **Oauth** and **Save** your setting.
8. Close the setup window on Prisma SaaS.

STEP 2 | Add the Confluence app.

1. Log in to your Atlassian console with Administrator privileges (for example, **`https://acmecorp.atlassian.net/`**).
2. From the Prisma SaaS Dashboard, select **Add a Cloud App**.
3. Select **Confluence**.
4. **Connect to Confluence Account**.
5. In **Confluence Custom Configuration** enter the **`Application URL`** and **`Consumer Key`** that you recorded earlier in this procedure.
6. Click **OK**.
7. **Allow** Prisma SaaS access to your Confluence account.

   Upon successful authentication using an account with the appropriate privileges, the new Confluence app is added to the list of Cloud Apps as Confluence *n,* where *n* is the number of Confluence app instances you have connected to Prisma SaaS. For example, if this is the second Confluence app you have added, the name displays as Confluence 2.

STEP 3 | Give a descriptive name to this app instance.

1. Select the Confluence instance on the Cloud Apps list.
2. (Optional) Enter a descriptive **Name** to differentiate this instance of Confluence from other instances you are securing.
3. Click **Done** to save your changes.

STEP 4 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for risks unique to the new app.

STEP 6 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the new app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Confluence app you just added, select **Actions** > **Start Scanning**.

   Prisma SaaS starts scanning assets in the associated Confluence app and begins identifying incidents. Depending on the number of Confluence users and assets, it may take some time for service to

complete the process of discovering all assets and users. However, as soon as you begin to see this information populating on the Prisma SaaS Dashboard, you can begin to Assess Incidents.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

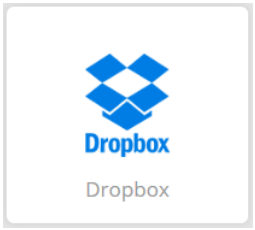
Begin Scanning Dropbox or Yammer

Use the following procedure to add Dropbox or Yammer as a monitored cloud application on Prisma SaaS.

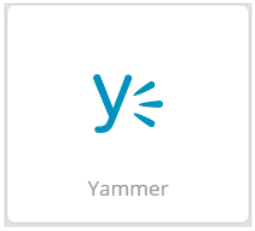
The Yammer application is not supported in the APAC region.

STEP 1 | Add the SaaS application.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select the application and enter the email address and password for the account.
   - For Dropbox, the account must have administrative user privileges.



   - For Yammer, the account must have network administrator privileges.



3. **Connect to the <application name > account**.

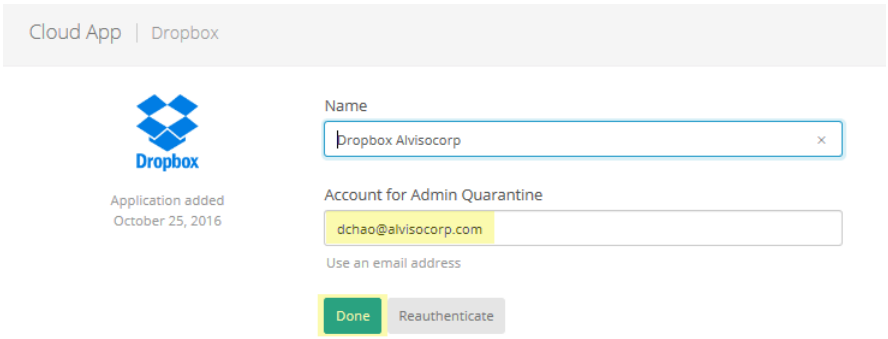
   The application is added to the list of **Cloud Apps** on Prisma SaaS.

STEP 2 | (Optional) Enter a descriptive name for the app instance.

In the list of **Cloud Apps**, click application name and add a descriptive name so that you can identify this instance from any other instances of the same application.

STEP 3 | Enable Admin quarantine for Dropbox.

Enter the Admin account email in **Settings** > **Cloud Apps & Scan Settings** > **Dropbox** > **Account for Admin Quarantine**. Click **Done** to save your setting.



STEP 4 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add a cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays any match occurrences. As a best practice, consider the business use of your applications to determine if you need to Add a New Asset Rule to look for incidents unique to Dropbox or Yammer.

STEP 6 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning Dropbox or Yammer for incidents.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new app you just added, select **Actions** > **Start Scanning**.

   Prisma SaaS scans assets in the associated app and identifies possible incidents. Depending on the number of users and assets, it may take some time to complete the process. However, as soon as you begin to see this information populating the Prisma SaaS dashboard, you can begin to Assess Incidents.

STEP 8 | Monitor the results of the scan.

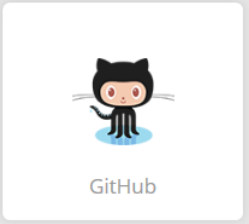
As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning GitHub

You can connect a GitHub to Prisma SaaS to scan for public exposure of repository folders or source code files to ensure your company's proprietary information is secure. With GitHub, you can control if Prisma SaaS scans a collection of owner accounts connected to an organization or a single owner account.

STEP 1 | Add GitHub to Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, select **Add a Cloud App**, and click the **GitHub** icon.

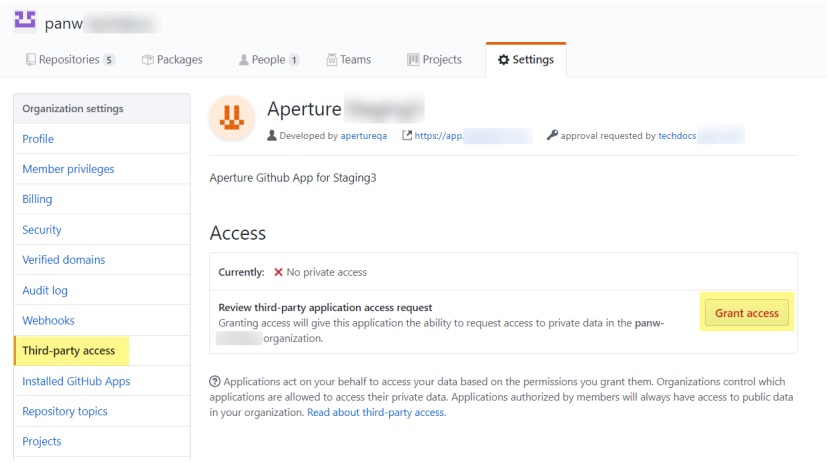


2. Click **Connect to GitHub Account**, enter your username or email address, and your password.

   You must sign in with an account that has owner privileges.
3. Authorize Prisma SaaS access to your GitHub account.

STEP 2 | (Optional) If your GitHub account is part of an organization, you must grant Prisma SaaS access to begin scanning of organization repositories.

1. Log in to GitHub, click your profile icon, and select **Settings**.
2. Select the organization name, click **Third-party access**, and **Grant Access** to Aperture (now known as Prisma SaaS).



STEP 3 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of GitHub to determine if you need to Add a New Asset Rule to look for incidents unique to GitHub.

STEP 4 | Start scanning GitHub for incidents.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the application instance you just added, select **Actions** > **Start Scanning**.

   Prisma SaaS scans all assets in the associated app and begins to identify incidents. Depending on the number of users and assets, it may take some time to complete the process. However, as soon as you begin to see this information populating on the Prisma SaaS dashboard, you can begin to Assess Incidents.

STEP 5 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard to verify your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the policy rules to ensure better results.

Begin Scanning a Gmail App

To begin scanning a Gmail app:

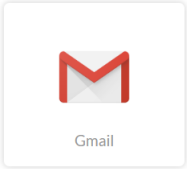
STEP 1 | Enable the privileges required for communication between Prisma SaaS and the Gmail app.

To establish communication between the two services, confirm the following:

- The Google administrator account has administrative privileges to read, write, and relocate assets in the app.
- The app is enabled for API access. API access provides visibility into the assets in Gmail and grants access to Prisma SaaS to monitor any sharing of assets.
- Ensure that the Google administrator email domain matches the existing domain on Prisma SaaS. For domain exceptions, contact customer support.

STEP 2 | Add the Gmail app.

1. From the Prisma SaaS **Dashboard**, select **Add a Cloud App**.
2. Select **Gmail** and enter the email address for the Google account with administrative privileges.



3. Click **Connect to Gmail Account**.
4. Enter the Google account password.

   Upon successful authentication, the new Gmail app is added to the list of Cloud Apps as Gmail *n*, where *n* is the number of Gmail app instances that you have connected to Prisma SaaS, for example Gmail 1.

STEP 3 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 4 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for risks unique to Gmail.

STEP 5 | Define security control scan settings.

STEP 6 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the Gmail app for policy violations and data exposure.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the Gmail app, select **Actions** > **Start Scanning**.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard to verify your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Google Cloud Storage App

Before you begin scanning a Google Cloud Storage app, you must create a service account and enable Administrator and client API access. As you prepare the Google Cloud Storage account, take note of the following values that you need to setup the app on Prisma SaaS:

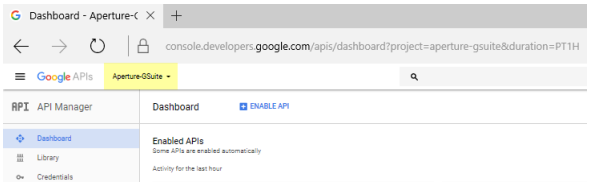
Item	Description
New Private Key	A P12 format private key certificate issued from your Google service account. This required certificate is uploaded on Prisma SaaS when adding the Google Cloud Storage app.
Private Key Password	The default password for the new private key.
Client ID	The client ID is entered when enabling Google Cloud Storage domain-wide delegation, and on Prisma SaaS when adding the Google Cloud Storage app.
Google Administrator email	The email entered to create a service account in Google Cloud Storage, and on Prisma SaaS when adding the Google Cloud Storage app.

STEP 1 | Create a service account in Google for Google Cloud Storage.

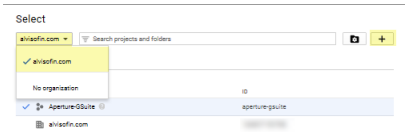
1. Log in to Google Developer Console as the Google Cloud Storage administrator.

   If you have not used the Developer Console before, Agree to the Google Cloud Platform Terms of Service.

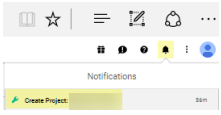
2. At the top of the screen next to your most recent project name, open your projects list, and then **Create a new project**.



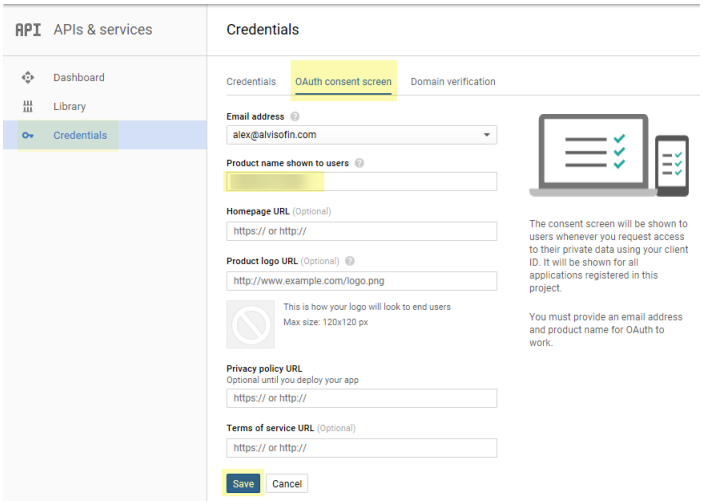
3. Select your organization (domain) and add your new project.



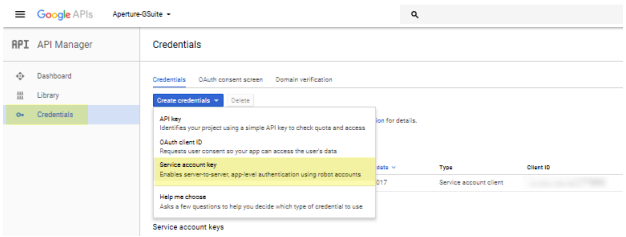
4. Name your project and **Create**.
5. Click Notifications and **Create Project: <project name>**.



6. Search for **Credentials**.
7. Select **OAuth Consent screen** and enter **`Prisma SaaS Google Cloud Storage`** in **Product Name Shown to Users** and **Save** the project.

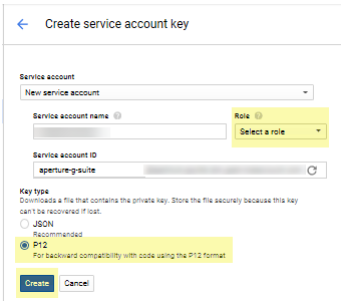


8. Select **Credentials** > **Create Credentials** > **Service Account Key**.



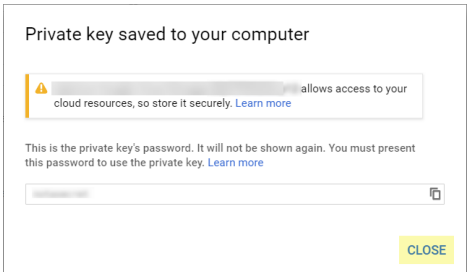
9. Select **New Service Account** and enter a service account name. Select **P12** for **Key Type** and **Create** the service account key.

Select Create Without Role if a warning message displays.

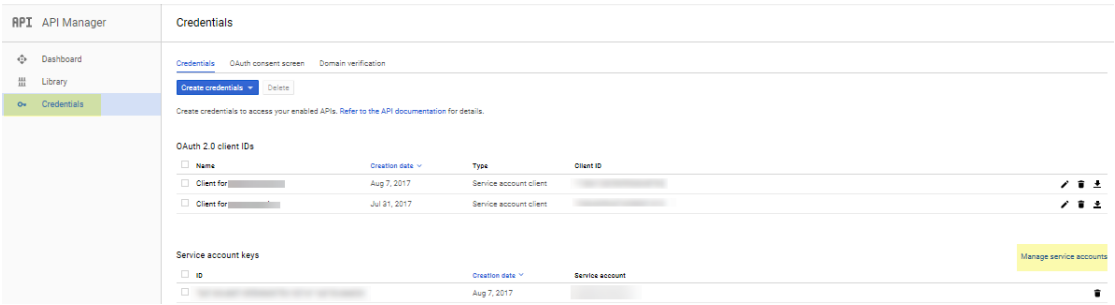


10. When the default password and new private key are issued, **Save** to your computer.

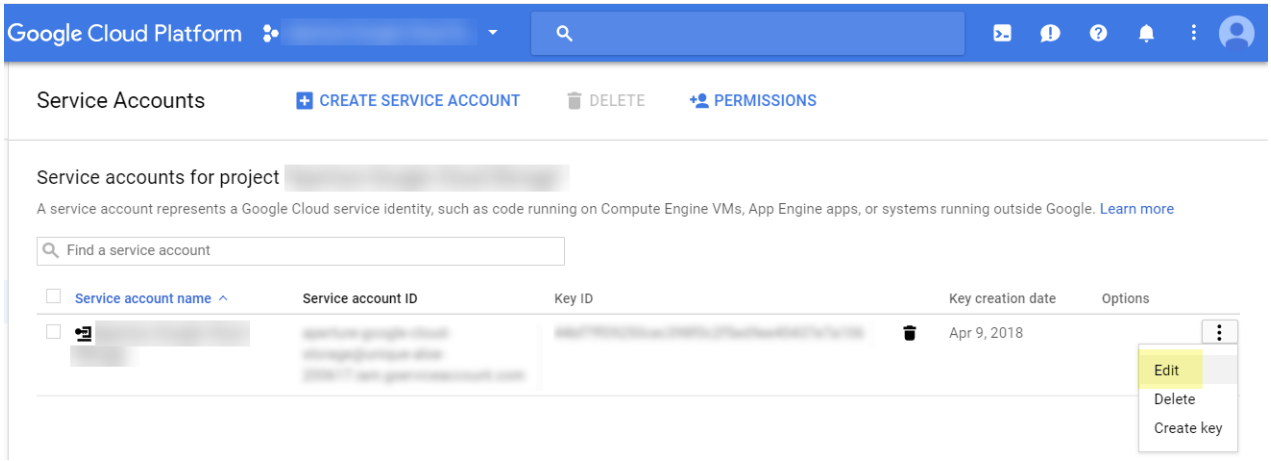
Store the private key securely because the key cannot be recovered if lost, and is required for adding the Google Cloud Storage app on Prisma SaaS.



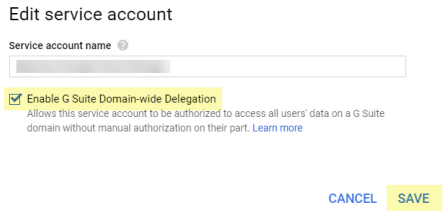
11. Select **Credentials** > **Manage Service Accounts**.



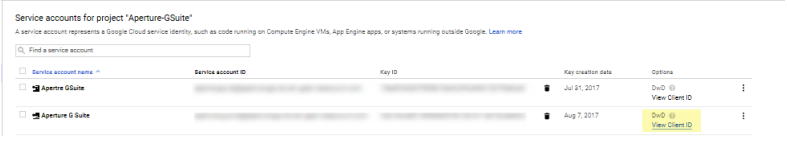
12. Click the three dots to the right of the service account you created and select **Edit**.



13. **Enable G Suite Storage Domain-wide Delegation** and **Save** the setting.



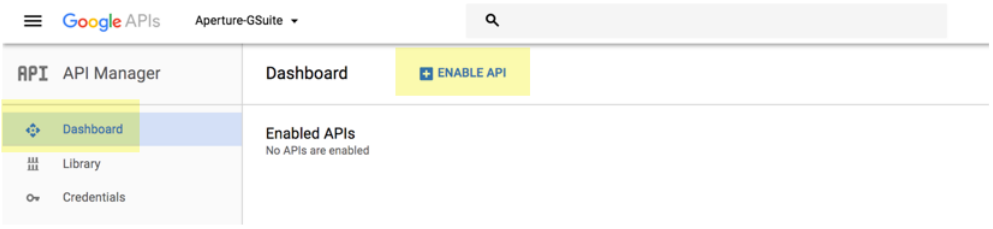
14. Click **View Client ID** for **<project name>**.



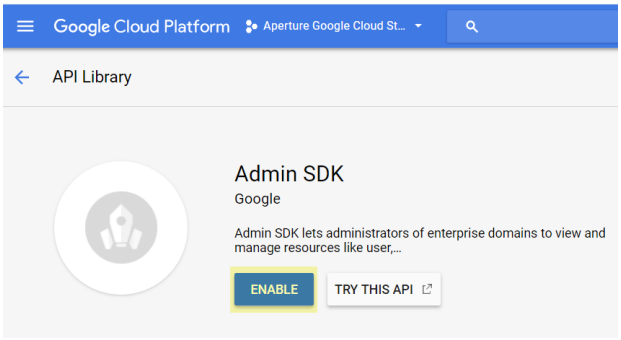
Note the value of the Client ID, and Save the ID.

STEP 2 | Enable API Access in Google Cloud Storage.

1. In your account, select **APIs & Services** > **Dashboard** > **Enable APIs and Services**.



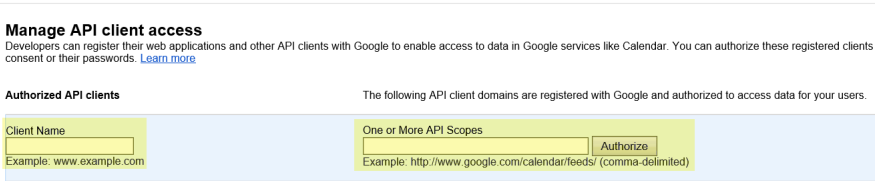
2. Select Google Cloud Storage **Admin SDK API**, and then **Enable** the API.



3. Go back to **Dashboard** > **APIs & Services** > **Library** and **Enable** the following APIs:
    1. **Google Cloud Resource Manager API**.
    2. **Google Cloud Storage**.
    3. **Google Cloud Pub/Sub API**.

STEP 3 | Enable API Client access to Google Cloud Storage.

1. In a new browser window, log in to Google Admin Account as the Google Cloud Storage Administrator.
2. Select **Security** > **Show more**.
3. Select **Advanced Settings** > **Manage API Client Access**.
4. Enter the **`Client ID`** previously noted in **Client Name**.



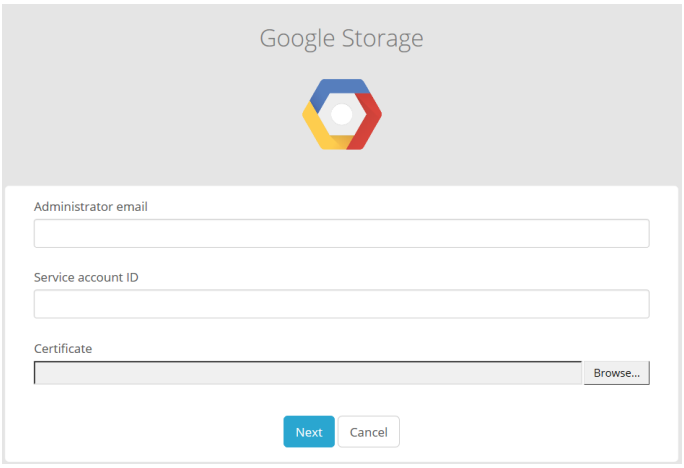
Copy and paste the following scope in **One or More API Scopes**, and then **Authorize** access to data in Google services.

```
https://www.googleapis.com/auth/admin.directory.user.security,https://
www.googleapis.com/auth/cloud-platform,https://www.googleapis.com/
auth/devstorage.read_write,https://www.googleapis.com/auth/
admin.directory.group
```

STEP 4 | Add the Google Cloud Storage app.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.

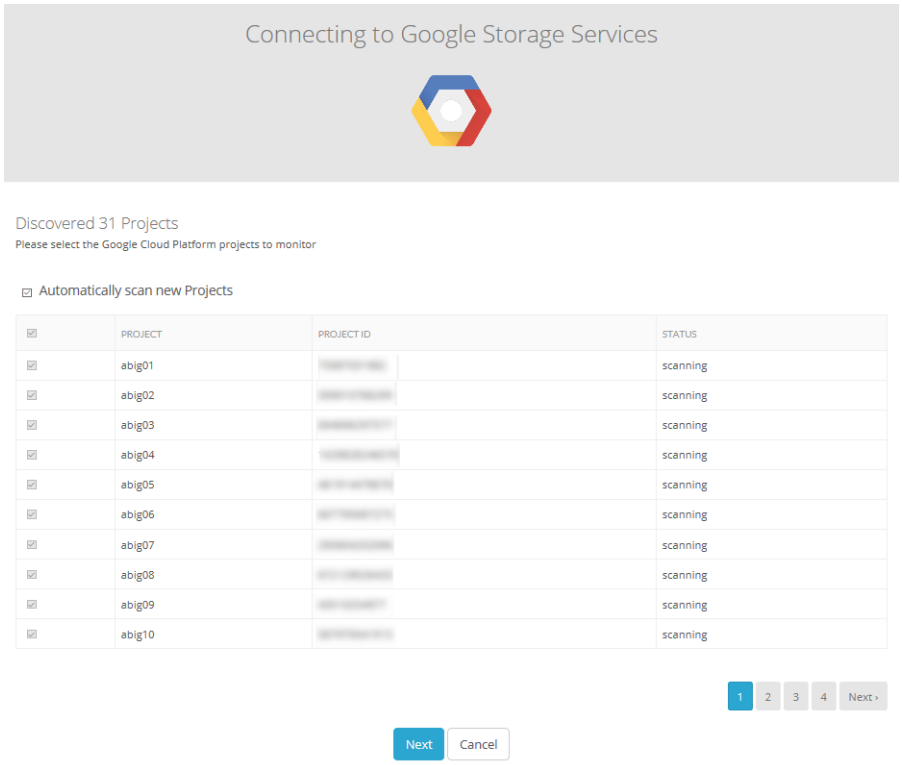
2. Select **Google Cloud Storage** and then **Click here to prepare your Google Cloud Storage Account**.
3. Enter the Google **Administrator Email**, the **Service account ID** previously noted, and click **Certificate** to browse and upload the P12 format private key certificate issued from your Google service account. Click **Next**.



STEP 5 | Review the initial project scan discoveries and select the projects to monitor.

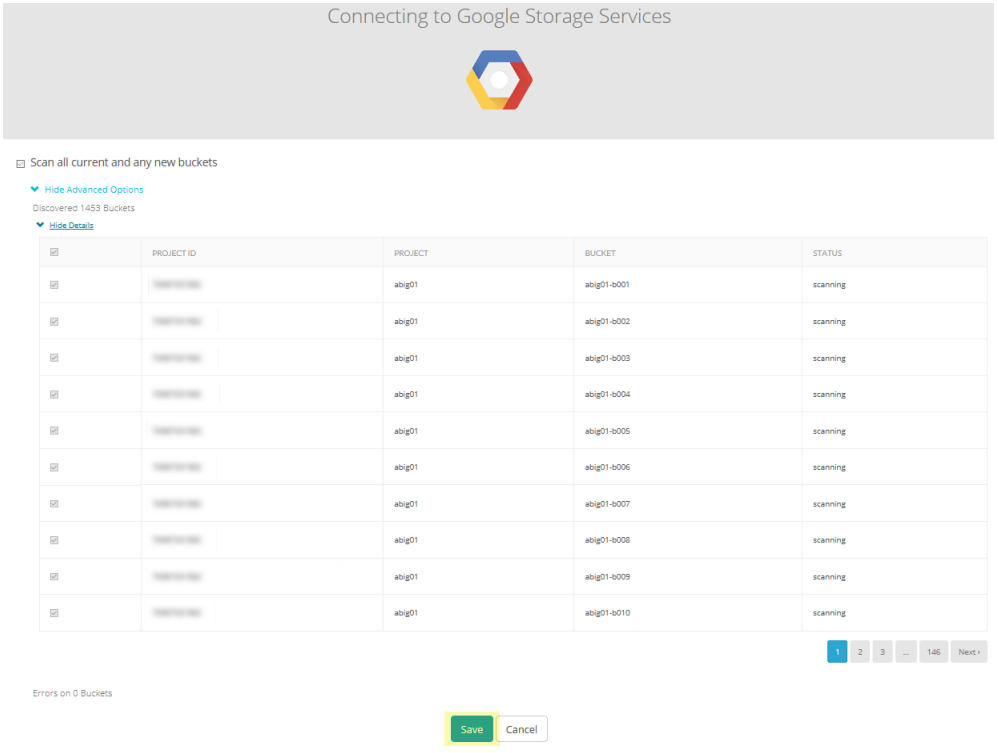
If you Cancel the setup at any time, you must start over again.

1. Enable **Automatically scan new projects** to scan all new projects.
2. To select individual projects, select the **Project** to scan from the list.
3. **Save** your scan setting to proceed scanning all discovered projects.
4. **Cancel** if you do not want to proceed with scanning the discovered projects.



STEP 6 | Review the initial bucket scan discoveries and select the buckets to monitor.

1. Enable **Scan all current and any new buckets** to scan all new buckets.
2. To select individual buckets, select the **Bucket** to scan from the list.
3. **Save** your scan setting to proceed scanning all discovered buckets.
4. **Cancel** if you do not want to proceed with scanning the discovered buckets.



STEP 7 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 8 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of Google Storage to determine whether you need to add new asset rules, security control rules, or user activity rules to look for risks unique to the new app.

STEP 9 | (Optional) Configure or edit a data pattern.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 10 | Start scanning the new Google Cloud Storage app for risks.

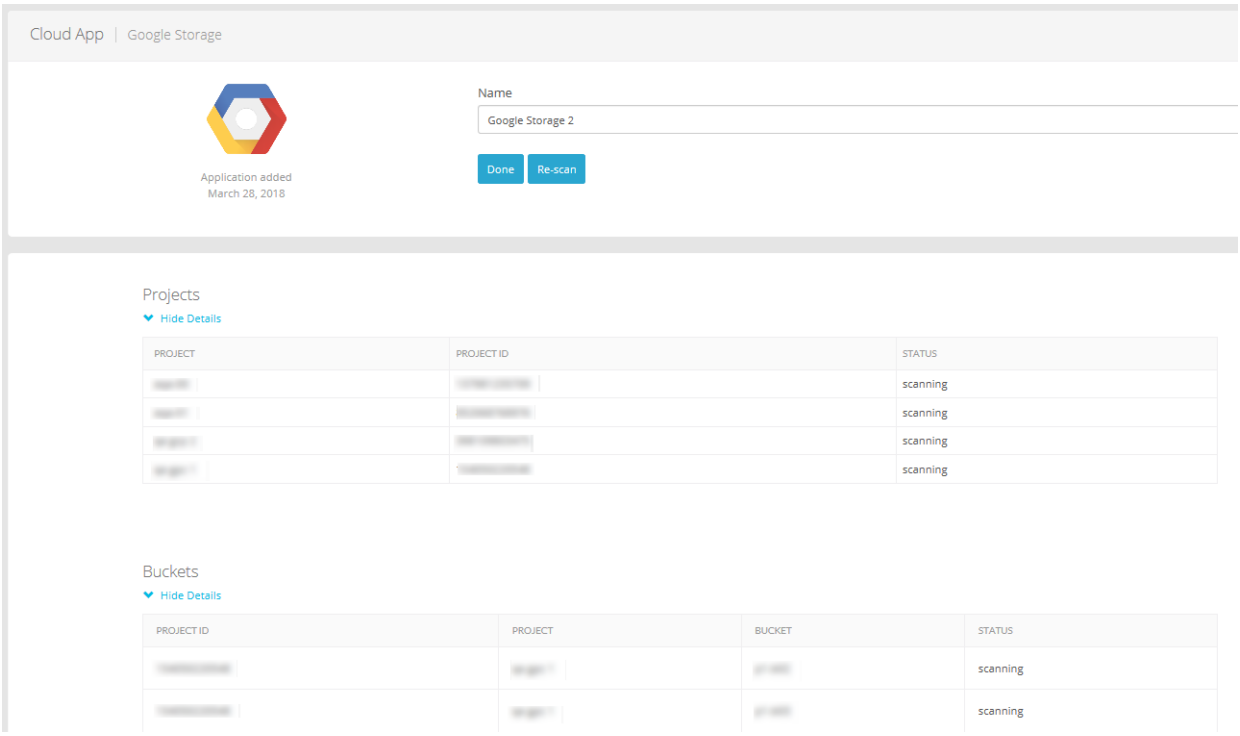
1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Google Cloud Storage app, select **Actions** > **Start Scanning**.

STEP 11 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, Monitor Scan Results on the Dashboard to verify that your policy rules are effective.

Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

STEP 12 | (Optional) To view the status of the **Projects** and **Buckets** that are currently being scanned, select **Settings** > **Cloud App and Scan Settings**. Select a Google Cloud Storage App from the list of **Cloud Apps** and expand the **Projects Buckets** to view the scan details.



Begin Scanning a Google Drive App

To begin scanning a Google Drive app:

STEP 1 | Enable the privileges required for communication between Prisma SaaS and the Google Drive app.

To establish communication between the two services, confirm the following:

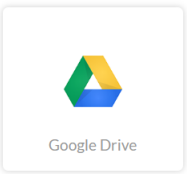
- The Google Drive administrator account has administrative privileges to read, write, and relocate assets in the app.
- The app is enabled for API access. API access provides visibility into the assets in Google Drive and allows Prisma SaaS to monitor the sharing of assets.
- Ensure that the Google administrator email domain matches the existing domain on Prisma SaaS. For domain exceptions, contact customer support.

STEP 2 | Add the email address of the Google Drive administrator to Prisma SaaS.

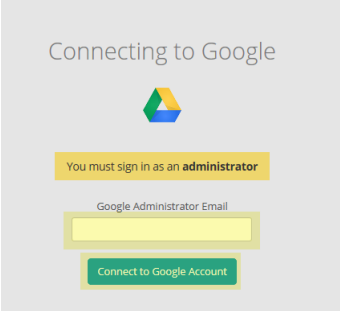
You must add the email address as an administrator and assign a super admin role, before you can connect the Google Drive app to Prisma SaaS, see how to Add Prisma SaaS Administrators.

STEP 3 | Add the Google Drive app.

1. From the Prisma SaaS **Dashboard**, select **Add a Cloud App**.
2. Select **Google**.

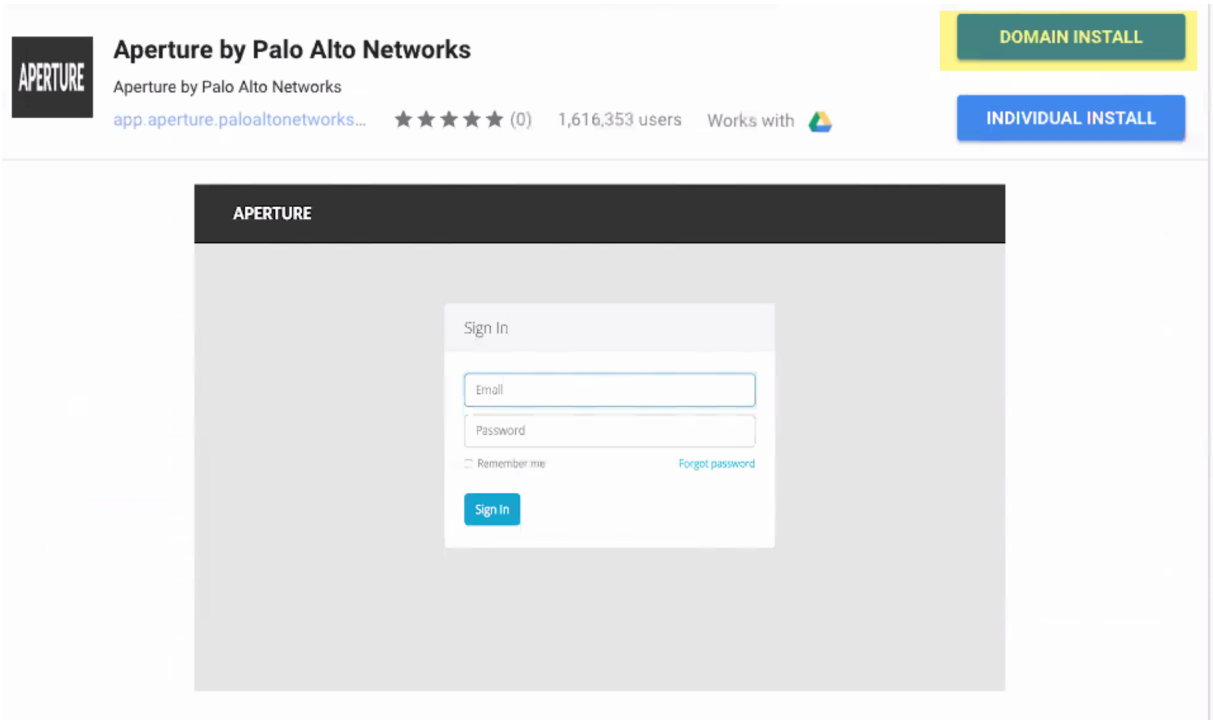


3. Enter the email address for the Google account with administrative privileges and **Connect to Google Account**.



If you missed adding the email address of this administrator account to Prisma SaaS, you will encounter an email address invalid error message. See Step 2 to add the email address.

4. Select **Install app** on the Google apps marketplace page.

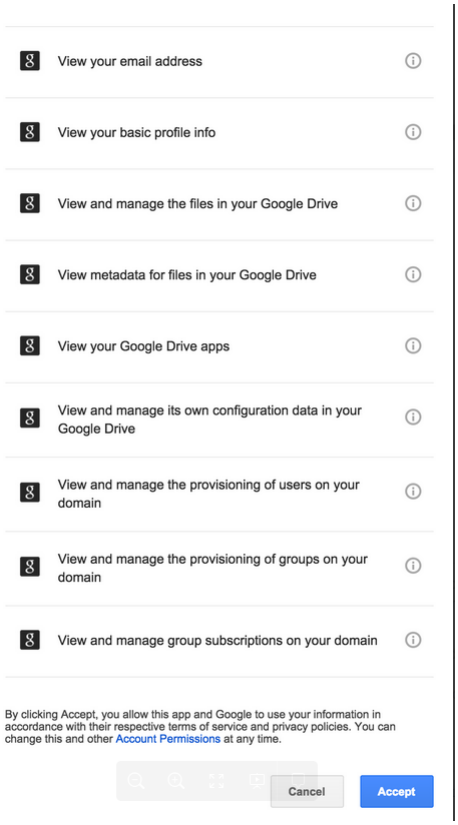


5. Authenticate your account by entering the account password on the Google login page.

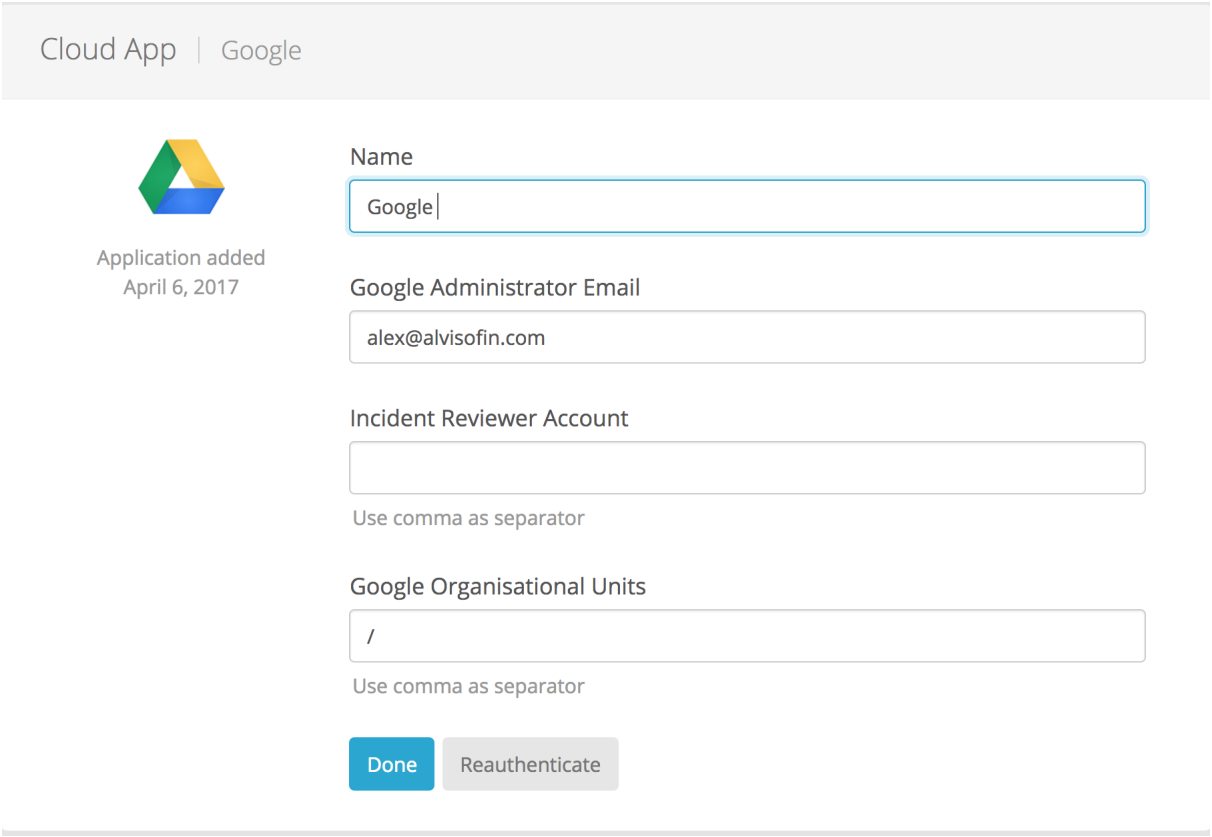
   After authentication, Cloud Apps lists your Google Drive app as Google *n*, for example Google 1. The *n* is the number of Google Drive app instances that you have connected to Prisma SaaS.

Prisma SaaS validates that you have provided an administrator account and that the account has the right permissions to authenticate and access all the assets within Google Drive. If the account does not have adequate permissions, the on screen status displays an error.

6. (Optional) Review and accept the changes to enable Prisma SaaS access to your assets in Google Drive.

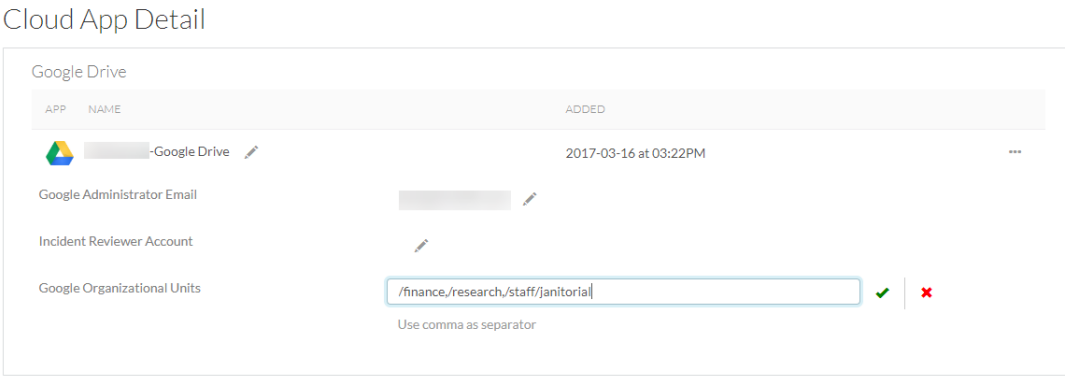


STEP 4 | (Optional) Give a descriptive name to this app instance and specify an incident reviewer.



1. Select the Google *n* link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Google Drive from other instances you are managing.
3. Specify an **Incident Reviewer Account**. Use this setting with caution. The account you provide becomes a collaborator on all risks — even private files.
4. (Optional) Enter the **Organizational Units** to scan.

   You can enter multiple OUs including the OU name and sub-OU. For example, your domain is companydomain.com and you want to selectively three OUs— the finance, research, staff/janitorial OUs, enter the OUs as a comma-separated list—**`/finance,/research,/staff/janitorial`**. If you leave this field blank, all units are scanned.

5. Click **Done** to save your changes.

STEP 5 | Set up a Google Remediation account.

1. Select **Settings**, and select the corresponding Google Drive app.
2. Enter an email address for the **Google Remediation Account**. This account grants access to all assets (files and folders) in the corresponding Google Drive account.
3. Click **Done** to save your changes.

STEP 6 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 7 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for risks unique to Google Drive.

STEP 8 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 9 | Start scanning the new Google Drive app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Google Drive app, select **Actions** > **Start Scanning**.

STEP 10 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning Third-Party Apps on the G Suite Marketplace

Before you begin scanning third-party apps, you must create a service account and enable Administrator and client API access in G Suite. As you prepare the G Suite account, take note of the following values, as they are required to complete the setup of the G Suite Marketplace app on Prisma SaaS:

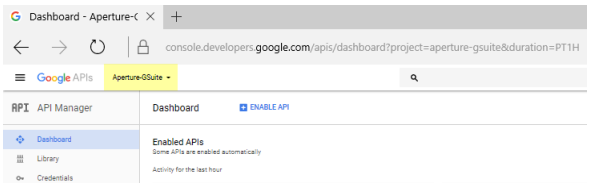
Item	Description
New Private Key	A P12 format private key certificate issued from your Google service account. This required certificate is uploaded on Prisma SaaS when adding the G Suite Marketplace app.
Private Key Password	The default password for the new private key.
Client ID	The client ID is entered when enabling G Suite domain-wide delegation, and on Prisma SaaS when adding the G Suite Marketplace app.
Google Administrator email	The email entered to create a service account in G Suite Marketplace, and on Prisma SaaS when adding the G Suite Marketplace app.

STEP 1 | Create a service account in Google for G Suite Marketplace.

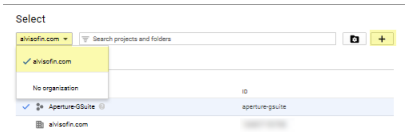
1. Log in to Google Developer Console as the G Suite administrator.

   If you have not used the Developer Console before, Agree to the Google Cloud Platform Terms of Service.

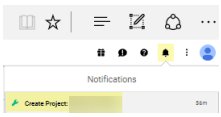
2. At the top of the screen next to your most recent project name, open your project list and then **Create a new project**.



3. Select your organization (domain) and add your new project.

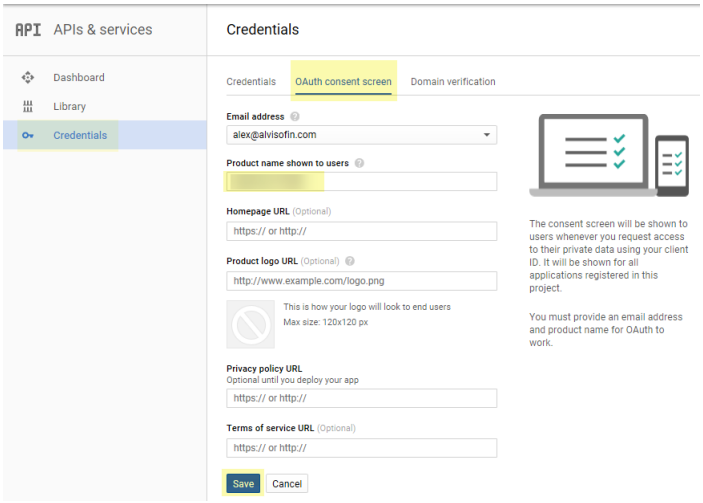


4. Name your project and **Create** the product.
5. Click **Notifications** and select **Create Project: <project name>**.

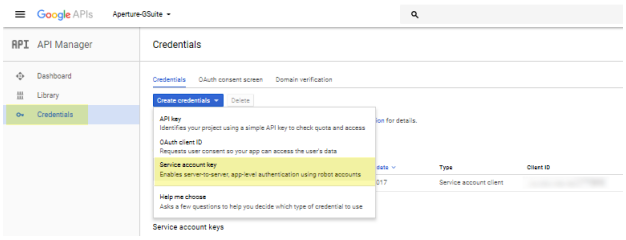


6. Search for **Credentials** and select **Credentials API Manager**.

7. Select **OAuth Consent** and enter your **<project name>** in **Product Name Shown to Users**, and **Save** the project.

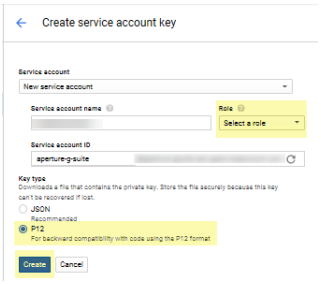


8. Select **Credentials** > **Create Credentials** > **Service Account Key**.



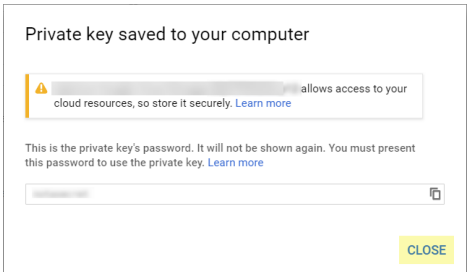
9. Select **P12** as the **Key Type** and **Create** the service account key.

Select Create Without Role if a warning message displays.

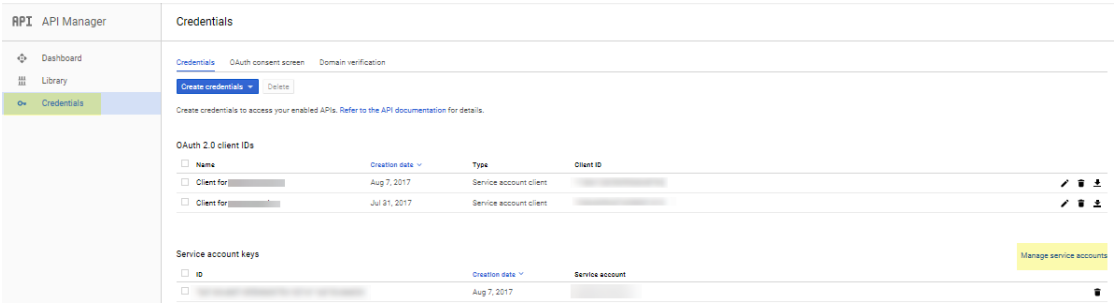


10. After a default password and new private key are issued, **Save** the new private key to your computer.

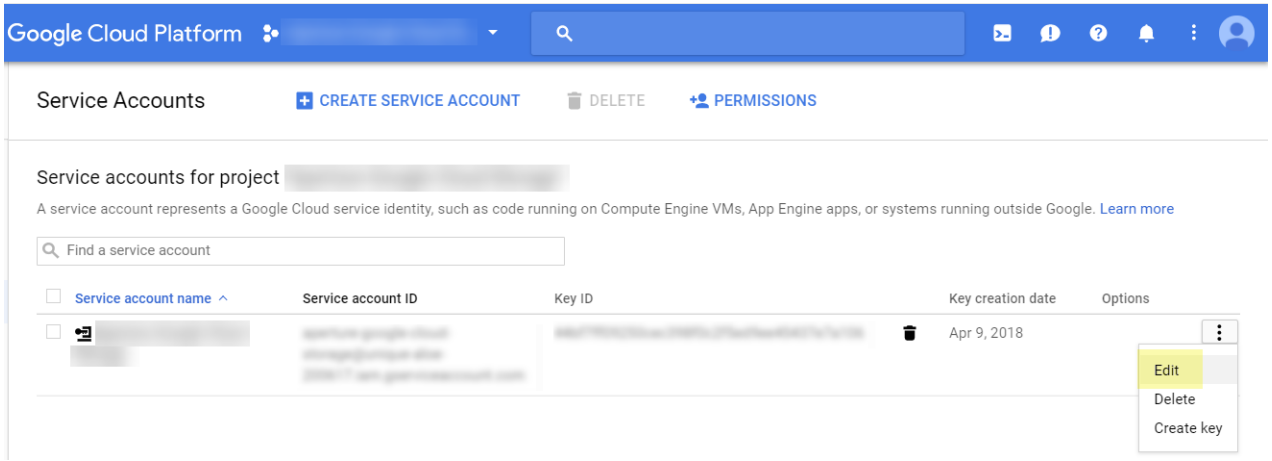
Store the private key securely as the key cannot be recovered if lost, and is required for adding the G Suite app on Prisma SaaS.



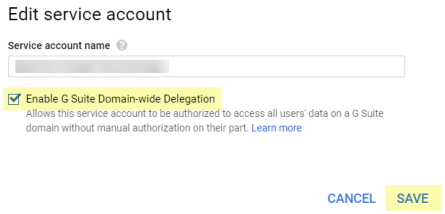
11. Select **Credentials** > **Manage Service Accounts**.



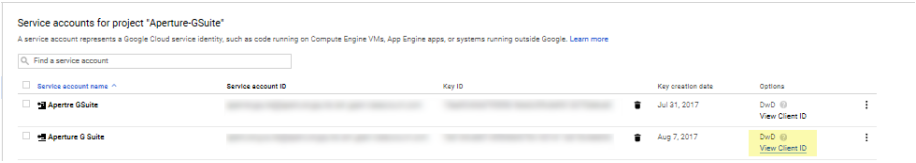
12. Click the three dots to the right of the service account and select **Edit**.



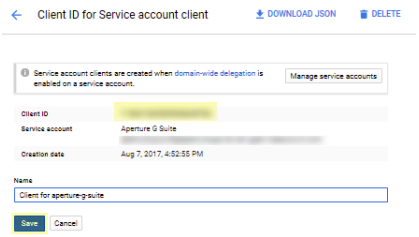
13. **Enable G Suite Domain-wide Delegation** and **Save**.



14. Click **View Client ID** for **<project name>**.

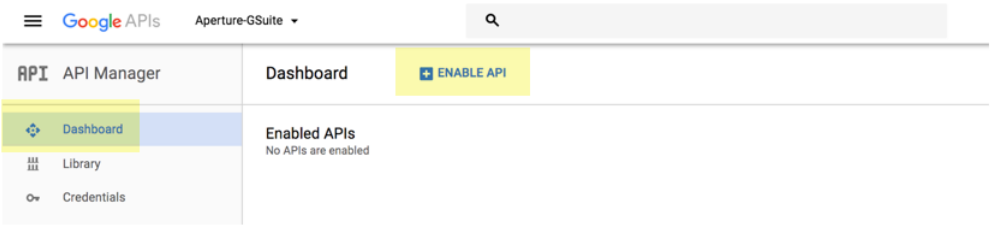


Note the value of the Client ID, and Save.

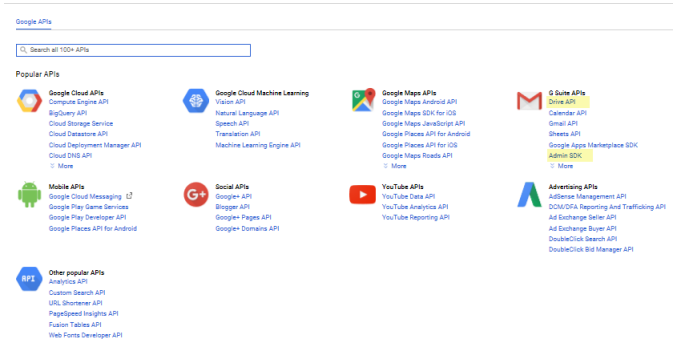


STEP 2 | Enable API Access in G Suite.

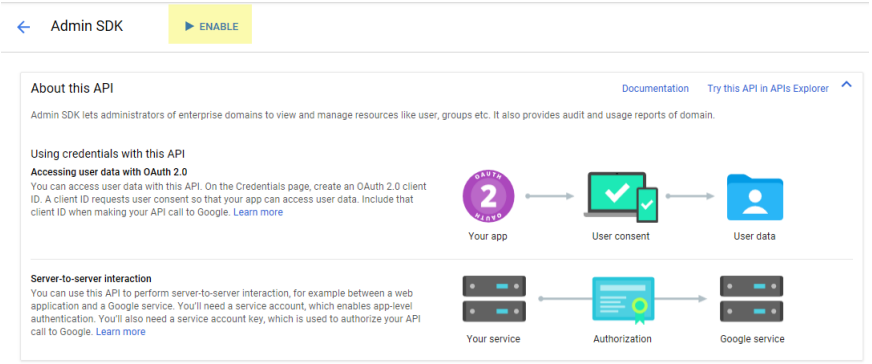
1. On your service account, select **Credentials** > **API Manager** > **Dashboard** > **Enable API**.



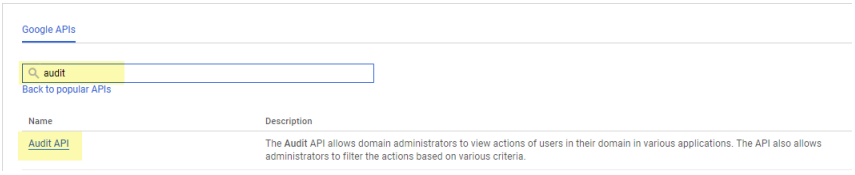
2. Click **Google APIs** and select **Drive API** and **Admin SDK** under G Suite APIs.



3. **Enable** the API.

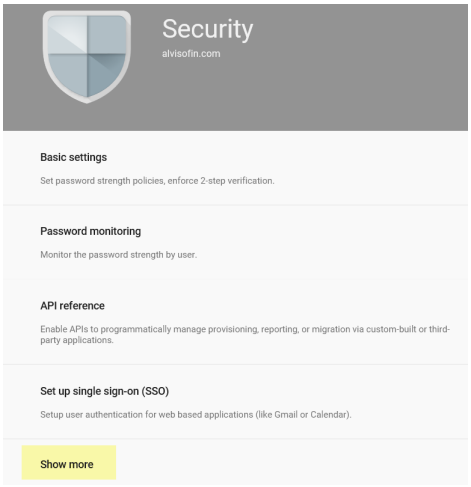


4. Return to **Dashboard** > **Enable API** > **G Suite APIs** and **Enable** the **Drive API**.
5. In **Google APIs**, **Search** for and **Enable** the **Audit API**.

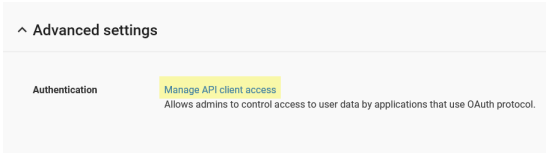


STEP 3 | Enable API Client access to G Suite.

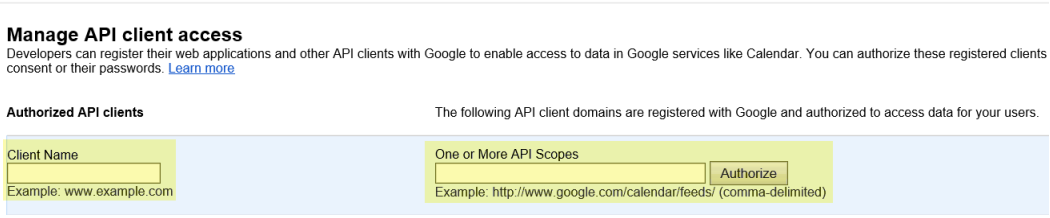
1. In a new browser window, log in to Google Admin Account as the G Suite Administrator.
2. Select **Security** > **Show more**.



3. Select **Advanced Settings** > **Manage API Client Access**.



4. Enter the **`Client ID`** previously noted in **Client Name**.

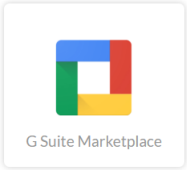


Copy and paste the following scope in **One or More API Scopes**, and then **Authorize** access to data in Google services.

```
https://www.googleapis.com/auth/userinfo.email,https://
www.googleapis.com/auth/userinfo.profile,https://www.googleapis.com/
auth/drive.apps.readonly,https://www.googleapis.com/auth/
admin.directory.user.readonly,https://www.googleapis.com/auth/
admin.directory.user.security,https://www.googleapis.com/auth/
admin.reports.audit.readonly
```

STEP 4 | Add the G Suite app.

1. On the Prisma SaaS **Dashboard**, **Add a Cloud App**.



2. Select **G Suite**, then **Click here to prepare your G Suite Account**.
3. Enter the **Google Administrator Email**, the **`Client ID`** you previously noted, click **Upload Certificate** to upload the P12 format private key certificate issued from your Google service account, and click **OK**.
4. **Connect to G Suite Account**.

Upon successful authentication, the new G Suite app is listed in Cloud Apps as G Suite *n,* where *n* is the number of G Suite app instances that you have connected to Prisma SaaS, for example G Suite 1.

5. Review and **Accept** the permissions for Prisma SaaS when scanning your assets on G Suite.

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for risks unique to any G Suite Marketplace apps.

STEP 6 | Add a New Setting for Third-Party Apps.

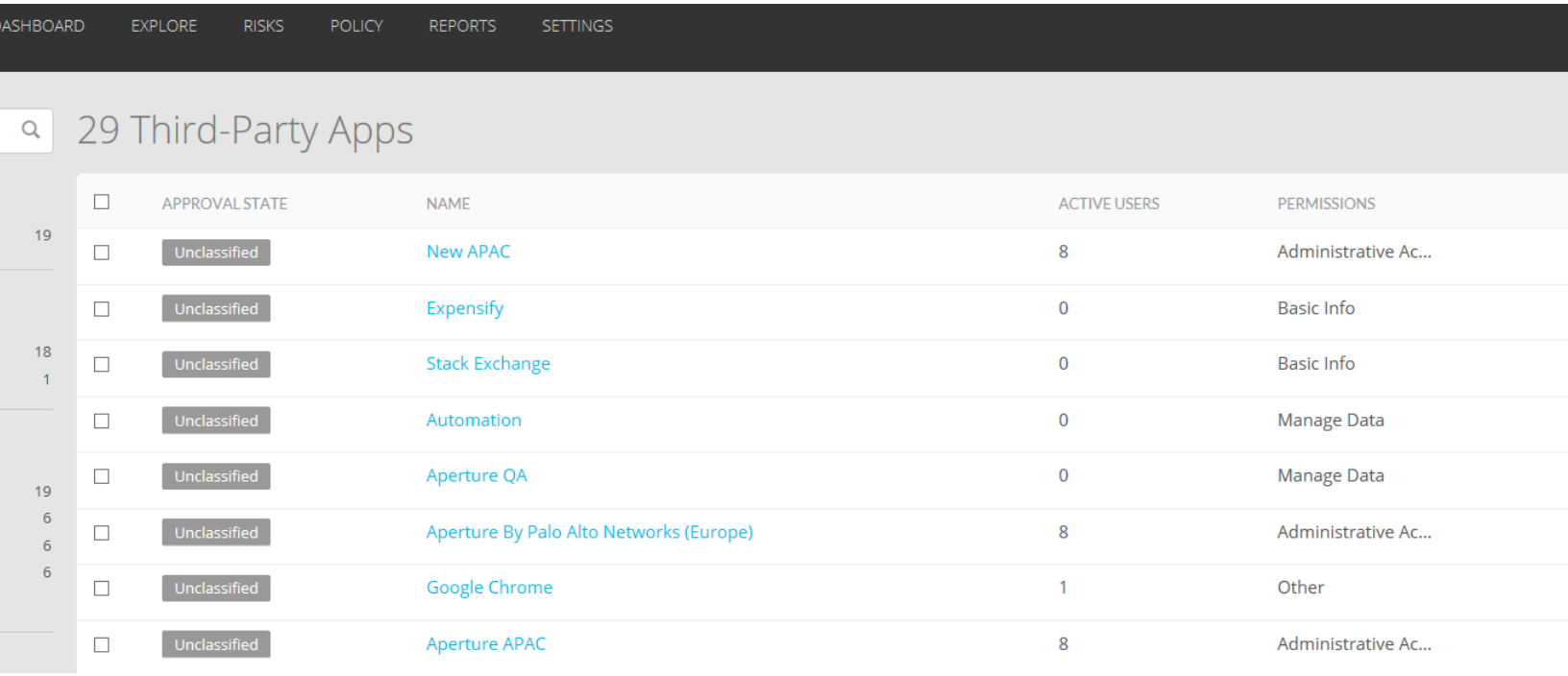
STEP 7 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against the settings, view the results by selecting **Explore** > **Third-Party Apps**. To assess and remediate the results:

- View Information for Third-Party Apps
- Remediate Third-Party Apps



Add a Jive App

To add a Jive app to Prisma SaaS:

- Install the Jive Add-On
- Begin Scanning a Jive App

Install the Jive Add-On

Before you can begin scanning a Jive app, you need to download and install a Jive client add-on. This add-on enables a secure OAuth 2.0 token and exchange authentication between the Jive app and Prisma SaaS.

STEP 1 | Download the Jive client add-on (**oauth**).

1. Log in to the Jive Software Developer website.
2. Enter a **Redirect URI/URL** for the add-on. The redirect you enter depends on the Prisma SaaS location:

   For North America, use:

   ```
   https://app.aperture.paloaltonetworks.com/auth/jive/callback
   ```

   For Europe, use:

   ```
   https://app.aperture-eu.paloaltonetworks.com/auth/jive/callback
   ```

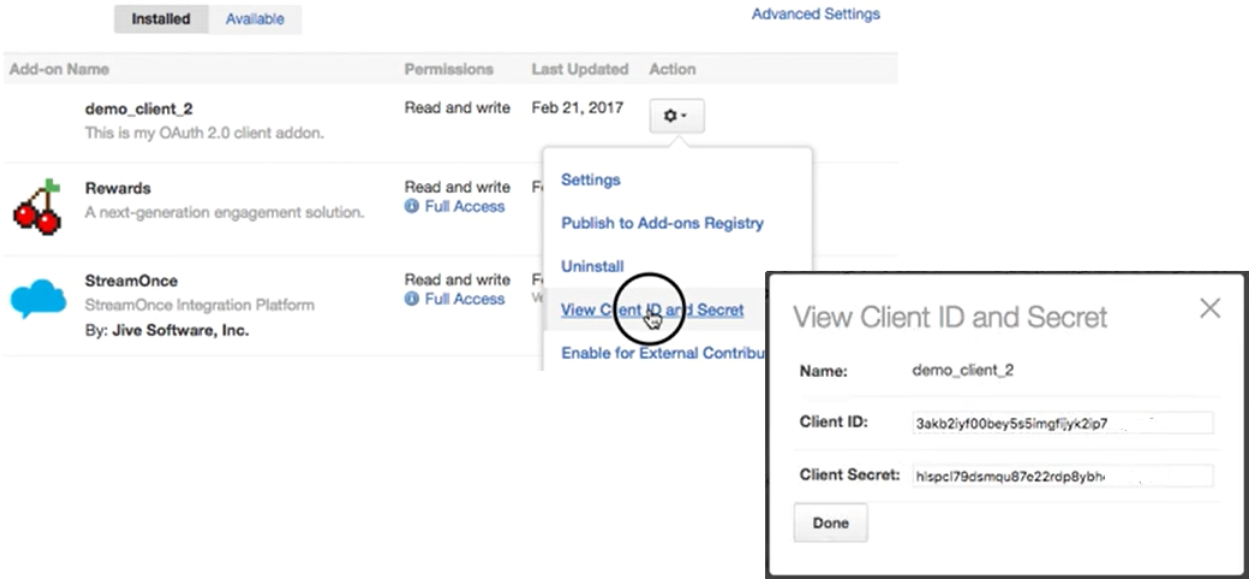
   For Asia-Pacific, use:

   ```
   https://app.aperture-apac.paloaltonetworks.com/auth/jive/callback
   ```
3. Enter a **Title** and **Description** for the add-on to identify the add-on in management settings on the Jive client.
4. Click **Download Add-On** to download to your computer.

STEP 2 | Install the Jive client add-on.

1. Log in to the Jive community console.

   You must be a Jive community administrator to install and configure the add-on for your Jive instance.
2. From Jive, select **Manage** > **Add Ons** to open the Jive Add-On management settings.
3. Select **All Add-ons** > **Upload Package** and browse to select the add-on package.
4. Click **Install Now**.
5. Once installation is complete, click **All Add-Ons**.
6. Open **Settings**, select **View Client ID and Secret**, and copy information to connect Jiva app on Prisma SaaS.



Begin Scanning a Jive App

To connect a Jive app to Prisma SaaS and begin scanning assets:

STEP 1 | Add the Jive app.

1. From the Prisma SaaS **Dashboard**, click **Add a Cloud App**, and select **Jive**.

2. Click **Connect to Jive Account**.

   You must be a Jive community administrator to add a Jive app to Prisma SaaS.
3. Add the **Jive URL** for your instance.
4. Add the **Client ID** and **Client Secret** copied from the Jive Add-On management settings page and click **OK**.
5. Click **Allow** to grant Prisma SaaS access to your Jive account.

   After authentication, the new Jive app is added to the list of Cloud Apps as Jive *n*, where *n* is the number of Jive app instances you have connected to Prisma SaaS. For example, if this is the second Jive app you have added, the name displays as Jive 2.

STEP 2 | (Optional) Give a descriptive name to this app instance.

1. Select the Jive *n* link on the Cloud Apps list and enter a descriptive **Name** to differentiate this instance from other instances, and click **Done**.

STEP 3 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 4 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically begins scanning the assets for possible policy violations. As a best practice, consider the business use and any associated risks and evaluate whether you want to Add a New Asset Rule to look for incidents unique to Jive.

STEP 5 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 6 | Start scanning Jive for possible policy violations and data exposure.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the Jive app you just added, select **Actions** > **Start Scanning**.

   Prisma SaaS scans the following assets in the associated Jive app — Discussions, Uploaded Files, Documents, Blog Posts, Events, and Ideas. Other asset types are not scanned. Depending on the number of Jive users and assets, it may take some time for Prisma SaaS to complete the scan. As soon as you begin to see information populate the Prisma SaaS dashboard, you can begin to Assess Incidents.

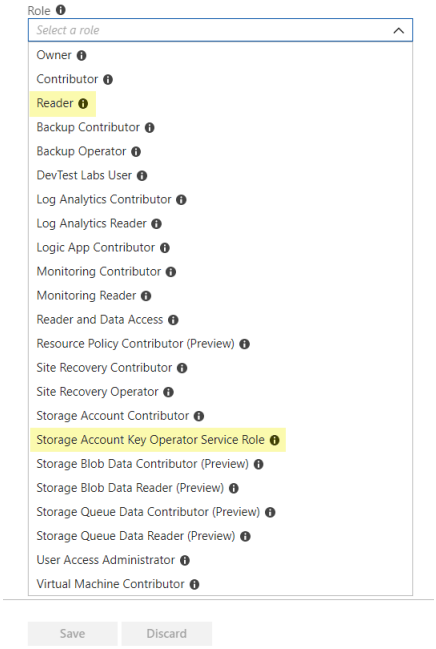
STEP 7 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard (Basic DLP) to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Microsoft Azure Storage App

Before you can begin scanning a Microsoft Azure Storage app, you must complete the following prerequisites:

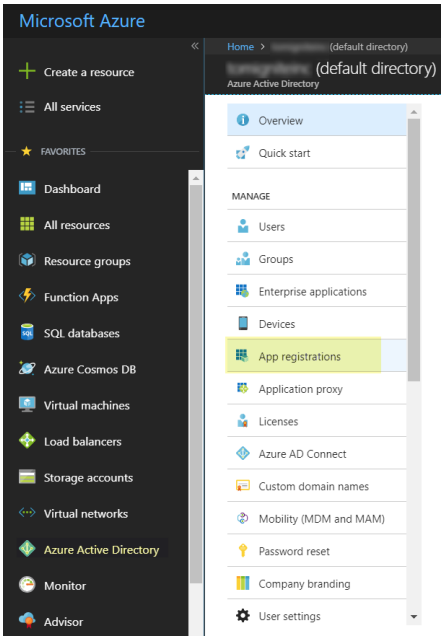
Item	Description
Ensure that you have the required permissions to create an application in Azure Active Directory (AAD).	**Check Azure Active Directory Permissions** in the Microsoft documentation.
Create an AAD Application. In a text editor (such as Notepad), and copy the Application ID and name of the application to use later in this procedure.	**Create an Azure Active Directory Application** in the Microsoft documentation.
Get the **Tenant ID**, which is the ID of the AAD directory in which you created the application. In a text editor (such as Notepad), copy the Directory ID to use later in this procedure.  *The Directory ID value is the tenant ID required to install Azure to Prisma SaaS.*	**Get Tenant ID** in the Microsoft documentation.
Assign **Reader Role** to the AAD Application on the subscriptions to scan.	**Assign Application to Role** in the Microsoft documentation.

Item	Description
Assign **Storage Account Key Operator Service Role** to the AAD Application on the subscriptions or storage accounts to scan.	
Enable roles required by the AAD Application. 	From your subscription select **Access control (IAM)** > **Add** > **Role**. Enable the following roles: • **Reader Role** (Subscription scans) — The reader role can view existing Azure resources and is required for monitoring subscriptions. • **Storage Account Key Operator Service Role** (Storage Account scans) — The storage account key operator role enables application identity and permissions. This role is required to list and regenerate storage account keys in the Azure key value application.

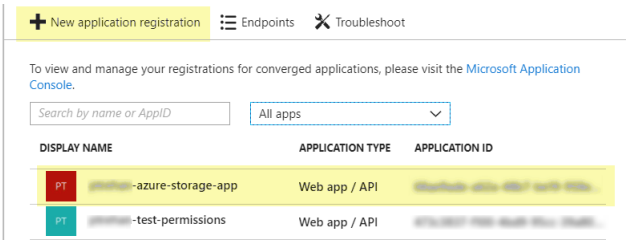
To begin scanning an Microsoft Azure Storage app:

STEP 1 | Prepare your Microsoft Azure Storage account to connect to Prisma SaaS.

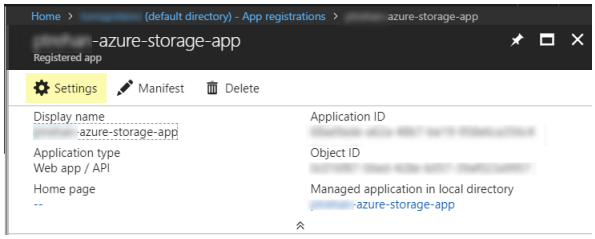
1. Select the application to register with the Azure AD tenant.
    1. Log in to Microsoft Azure.
    2. Select **Azure Active Directory** > **App registrations**.



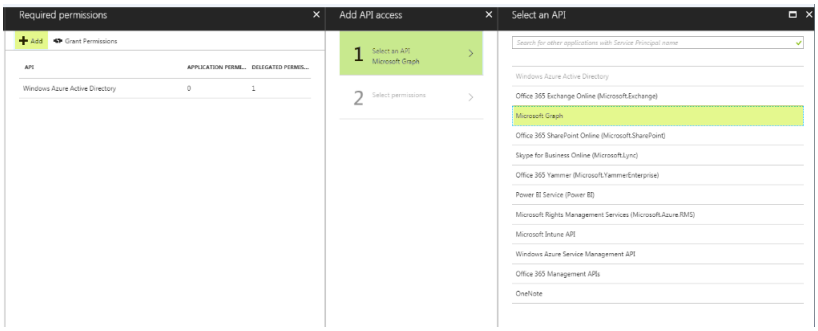
2. Register the application to provide secure sign-in and authorization for Prisma SaaS. You can add a **New application registration** or select an app that has already been registered by clicking on the app from the list.



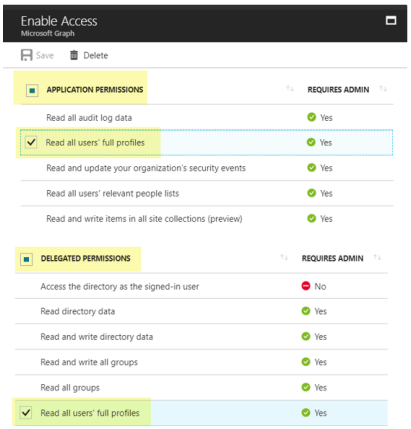
3. (Optional) Enter the application **Name**, **Application Type**, and **Sign-on URL** to **Create** a new application registration.
4. Enable the permissions API for Microsoft Graph.
    1. Click **Settings** for the registered app.



    2. Select **Required Permissions** > **Add** > **Select an API** > **Microsoft Graph**.



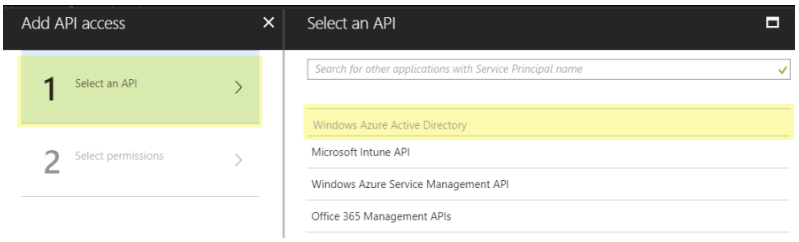
3. Add permissions, **Enable** > **Read all users' full profiles** in **Application Permissions** and **Delegated Permissions**.



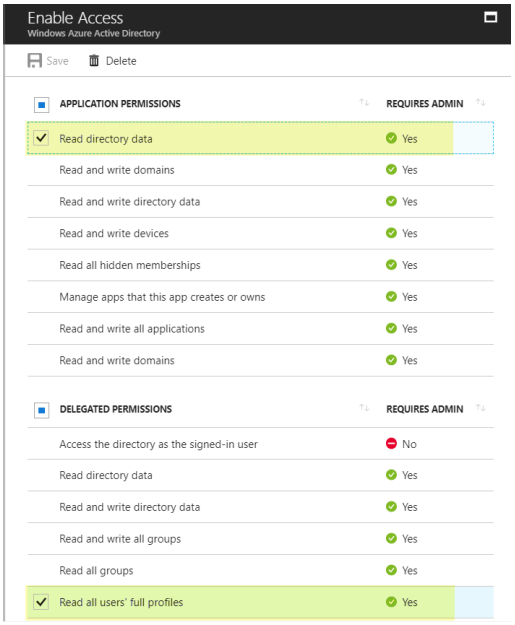
4. **Save** your Microsoft Graph API setting.

5. Enable the delegated permissions API for Windows Azure Active Directory.

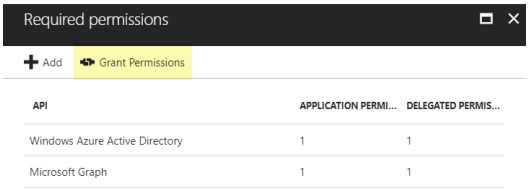
    1. Click **Settings** for the registered app.
    2. Select **Required Permissions** > **Add** > **Windows Azure Active Directory**.



    3. **Enable** > **Read directory data** in **Application Permissions** and **Read all users' full profiles** in **Delegated Permissions**.
    4. **Save** your Windows Azure Active Directory API setting.



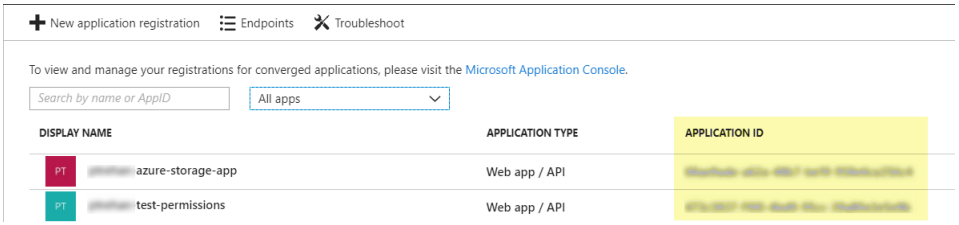
6. Grant application and delegated permissions.
    1. Click **Settings** for the registered apps.
    2. Select **Required Permissions** > **Grant Permissions**.



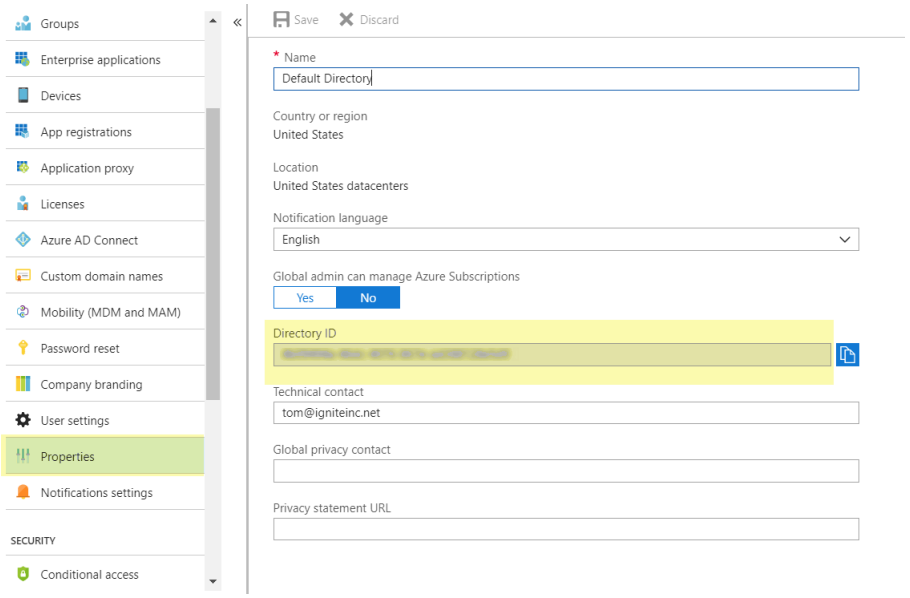
    A confirmation window will display to **Grant Permissions** for all accounts in the current directory. Select **Yes** to grant the permissions for the accounts.
7. You will need the **Application ID**, **Directory ID**, and **Application Key** for your registered application, as they are required to complete the setup of the Microsoft Azure Storage app on Prisma SaaS.

    For new applications that are not yet registered, set up an Application ID, Directory ID and Application Key on Azure Resource Manager.

    1. Log in to Microsoft Azure, select the registered app to view and copy the **Application ID** to enter during app installation.

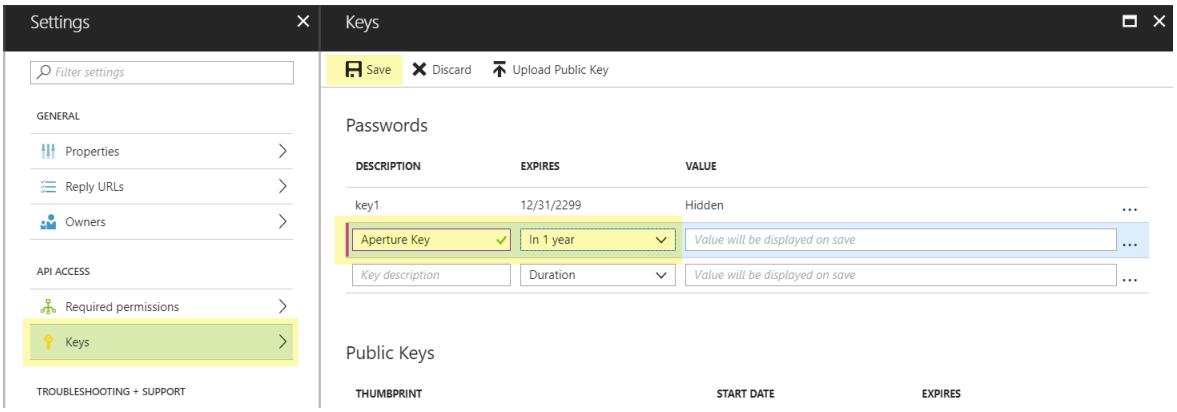


    2. Select **Azure Active Directory** > **Properties**. Copy the **Directory ID** to enter during app installation.

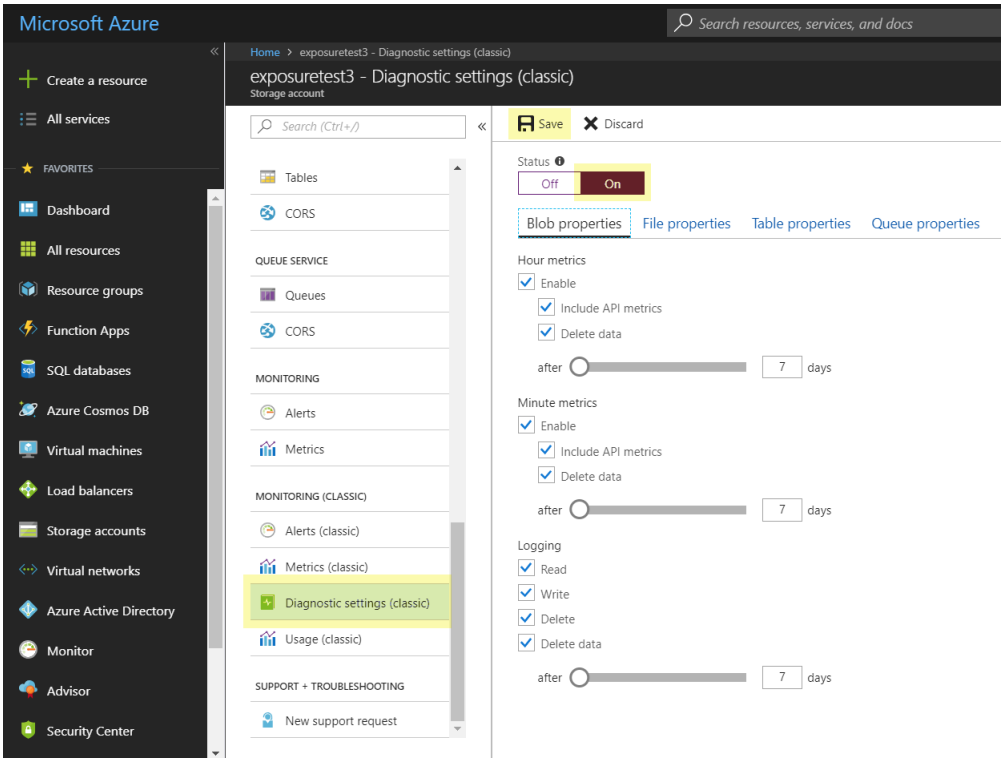


3. Click **Settings** > **Keys**. Provide a description of the key, and a duration for the key. **Save** the key.

The key value is the Application Key to enter during app installation. After saving the key, the value of the key is displayed. Copy this value because you are not able to retrieve the key later.



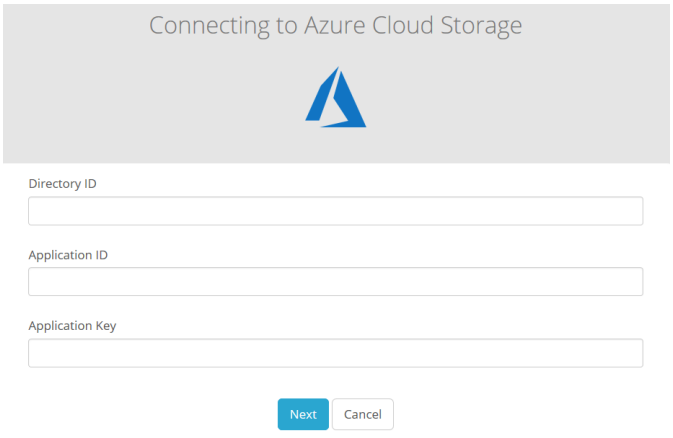
8. Prisma SaaS can continuously scan for Azure Storage subscriptions and accounts to identify and report any new accounts, activities, and events with the iterative scanning service. The service also scans and identifies users assigned to Subscriptions, Resources, Groups, Containers and Storage Accounts. To enable iterative scan on Prisma SaaS, you need to configure the diagnostic service settings in Azure for each storage account.
    1. Select the storage account to configure the diagnostic service settings and then select **Monitoring** > **Diagnostic Settings**. If not already, enable the settings by turning the status **On**.
    2. Select the type of **Metrics** and **Logging** data for each service you wish to monitor, and the retention policy for the data by moving the retention in days slider from 1 to 365. The default for new storage accounts is 7 days.
    3. **Save** your monitoring configuration.



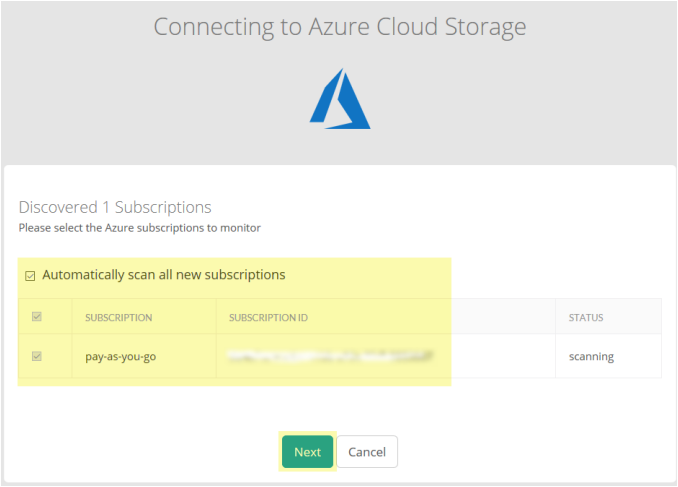
STEP 2 | Add the Microsoft Azure Storage app on Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Microsoft Azure Storage**.

3. Configure your Microsoft Azure Storage settings.
   1. Click **Connect to Account**.
   2. Enter the **Directory ID**, **Application ID**, and **Application Key** you recorded in the previous steps.
   3. Click **Next**.



4. Select the Azure subscriptions to monitor.
    1. Enable a **Subscription** to scan from the discovered list, or you can select **Automatically scan all new subscriptions**.
    2. Click **Next**.



5. Review initial scan discoveries and complete the Azure app installation. **View Details** on the discovered containers to review the discoveries and determine if you want to proceed with scanning:
    - To proceed scanning all discovered containers, enable **Scan all current and any new containers** and then **Save** your scan setting.
    - To proceed scanning individual containers and subscriptions, select the items to scan and then **Save** your scan setting.
    - If you do not want to proceed with scanning the discovered containers, select **Cancel** to abort the installation.
    - **Save** the Azure Cloud Storage app to the list of Cloud Apps.

STEP 3 | (Optional) Give a descriptive name to this app instance and specify an incident reviewer.

1. Select the Azure Cloud Storage link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Azure Cloud Storage app from other instances you are managing.

STEP 4 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of MS Azure Storage to determine whether you need to add new asset rules, security control rules, or user activity rules to look for risks unique to your enterprise.

STEP 6 | (Optional) Configure or edit a data pattern.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the new Azure Cloud Storage app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Azure Cloud Storage app, select **Actions** > **Start Scanning**.

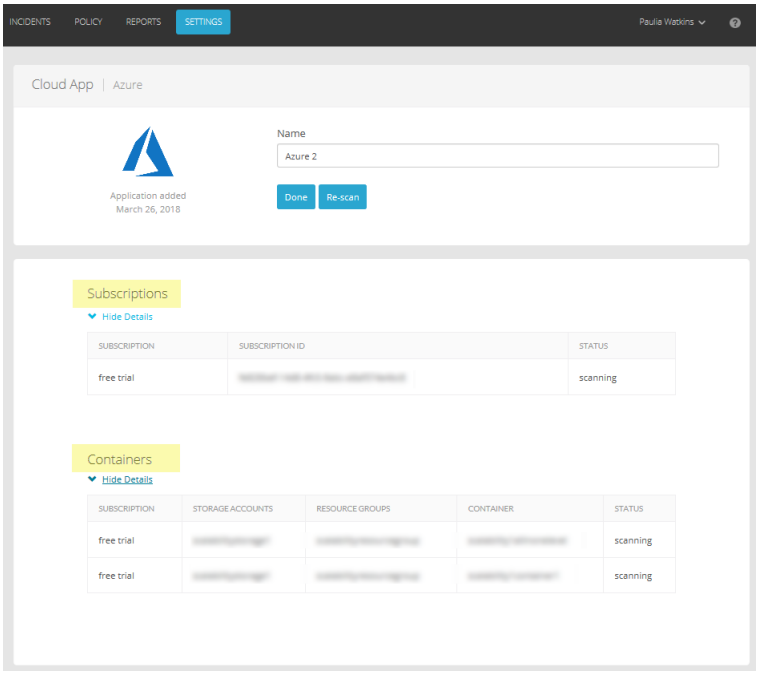
   The status changes to Scanning. Prisma SaaS starts scanning all assets in the associated Azure Cloud Storage app and begins identifying incidents. Depending on the number of Azure assets, it may take some time for service to complete the process of discovering all assets and users. However, as soon as you begin to see this information populating on the Prisma SaaS **Dashboard**, you can begin to Assess Incidents.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, Monitor Scan Results on the Dashboard to verify that your policy rules are effective.

Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

(Optional) To view the status of **Subscriptions** and **Containers** being scanned, select **Settings** > **Cloud App and Scan Settings**. Select an Azure app from the list of **Cloud Apps** and expand the **Subscriptions** and **Containers** to view the scan details.



Begin Scanning a Microsoft Exchange App

To begin scanning a Microsoft Exchange app:

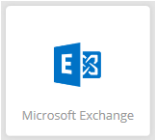
STEP 1 | Log in to Microsoft Exchange or Office 365 using an account with privileges that will enable communication between Prisma SaaS and the Microsoft Exchange app.

Before you can establish communication between Prisma SaaS and the Exchange app, you must:

- Go to http://portal.microsoftonline.com and log out of Exchange or Office 365.
- Log back in to Exchange or Office 365 using an account that has the Global Admin role prior to adding the Exchange app to Prisma SaaS.

STEP 2 | Add the Exchange app.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Microsoft Exchange**.



3. When prompted, enter the login credentials for the account with Global Admin role privileges on the Microsoft Online page to which you are redirected.
4. Review and **Accept** the changes that Prisma SaaS can perform on your assets in Exchange.

   When authentication succeeds, Prisma SaaS adds the new Exchange app to the list of Cloud Apps as Microsoft Exchange *n,* where *n* is the number of Exchange app instances that you have connected to Prisma SaaS, for example Exchange 1.

STEP 3 | (Optional) Give a descriptive name to this app instance.

1. Select the Exchange app instance from the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Exchange from other instances you are managing.
3. Click **Done** to save your changes.

STEP 4 | Add new domains and users to global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of Microsoft Exchange to determine whether you need to add new asset rules, security control rules, or user activity rules to look for risks unique to your enterprise.

STEP 6 | (Optional) Configure or edit a data pattern.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the new Exchange app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Exchange app, select **Actions** > **Start Scanning**.

The status changes to Scanning. Prisma SaaS starts scanning assets in the associated MS Exchange app and begins identifying incidents. All email attachments in Exchange are scanned based on defined policies. Email content is scanned based on defined policies only if the sender or receiver of the email is from an external domain. Scanning only starts on installation, and assets without risks are not stored.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, Monitor Scan Results on the Dashboard to verify that your policy rules are effective.

Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning Microsoft Office 365 Apps

To begin scanning Microsoft Office 365 apps:

STEP 1 | Add **`company.onmicrosoft.com`** as an internal domain.

See Define Your Internal Domains.

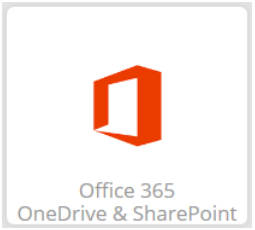
STEP 2 | Log in to Office 365 using an account with privileges that will enable communication between Prisma SaaS and the Microsoft Office 365 apps.

Before you can establish communication between Prisma SaaS and the Microsoft Office 365 SharePoint and OneDrive apps, you must:

- Go to http://portal.microsoftonline.com and log out of Office 365.
- Log back in to Office 365 using an account that has the Global Admin role prior to adding the Office 365 app to Prisma SaaS.

STEP 3 | Add the Office 365 app.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Office 365**.



3. Select one of the following:
   - **Connect to Office 365 Account**
   - **Using a custom configuration?**

   If you have a dedicated Office 365 account, select **Using a custom configuration?** and provide the URL for OneDrive and SharePoint that are part of your custom configuration.
4. Enter the login credentials for the account with Global Admin role privileges on the Microsoft Online page to which you are redirected.
5. Review and **Accept** the changes that Prisma SaaS can perform on your assets in Microsoft Office 365.

   Upon successful authentication, the new Office365 app is added to the list of Cloud Apps as Office365 *n*, where *n* is the number of Office 365 app instances that you have connected to Prisma SaaS, for example Office365 1.

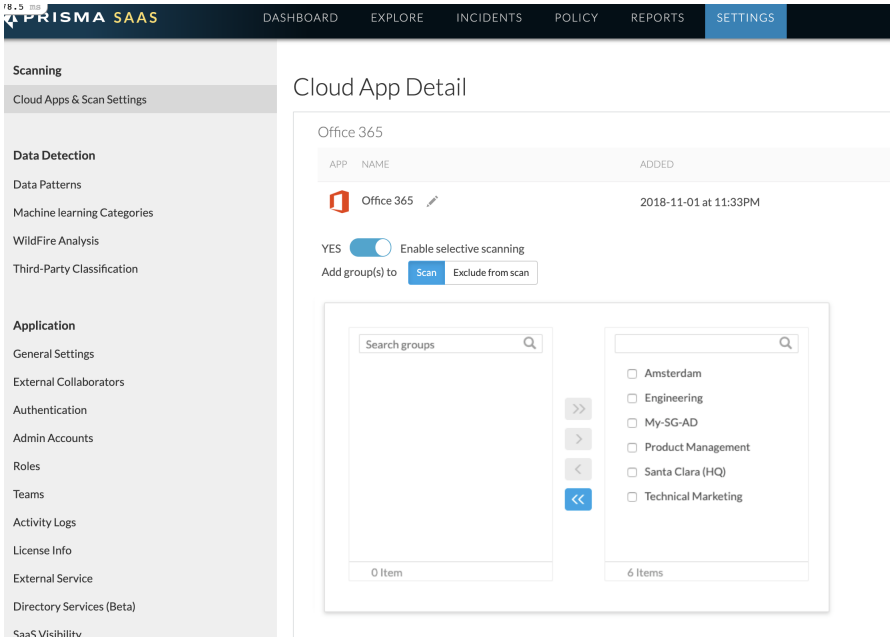
STEP 4 | (Optional) Choose the user groups whose assets and accounts you want to monitor.

Begin Selective Scanning Using Azure Active Directory Groups if you want Prisma SaaS to scan or not scan content for users who belong to specific groups. By default, selective scanning is not enabled. If you want to enable selective scanning later, you must delete the O365 instance and add it back so Prisma SaaS can discover all assets and events for all users. All assets and events previously stored will be deleted and incidents reported for users no longer included in the selected groups are automatically closed.

1. Select **Enable selective scanning** and choose the groups you want to include or exclude from scanning from the list of groups using >> to add all groups or > to add selected groups.

Prisma SaaS discovers metadata on all sites within SharePoint, however, it only scans or excludes from scan the assets (files and folders) that belong to users who are members of the groups you have selected in your selective scanning configuration.

If a group is edited or removed from selective scanning, it can take up to 7 days to remove assets or activities, and close any related incidents. Adding a group back to selective scanning will record new user activities but not old, previously removed user activities.



2. Select **Save** to continue.

STEP 5 | (Optional) Give a descriptive name to this app instance.

1. Select the Office365 *n* link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Office 365 from other instances you are managing.
3. Click **Done** to save your changes.

STEP 6 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your MS Office 365 to determine whether you want to add new asset rules, security control rules, or user activity rules to look for risks unique to your enterprise.

STEP 7 | (Optional) Configure or edit a data pattern.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 8 | Start scanning the new Microsoft Office 365 app for risks.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Office 365 app, select **Actions** > **Start Scanning**.

STEP 9 | Monitor the results of the scan.

As Prisma SaaS starts scanning files and matching them against enabled policy rules, Monitor Scan Results on the Dashboard to verify that your policy rules are effective.

Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Salesforce App

To begin scanning a Salesforce app:

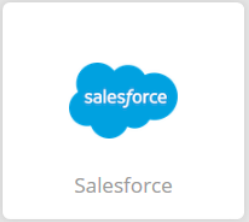
STEP 1 | Ensure that the Salesforce administrator account you plan to connect to Prisma SaaS has sufficient administrator privileges.

To configure the required permissions within Salesforce:

1. Under **Setup**, select **Manage Users** > **Users**.
2. Select the administrative user account and then click **System Permissions**.
3. Under **System**, enable the following permissions:
   - **API Enabled**
   - **Manage Chatter Messages** (required only if you use Chatter)
   - **Modify All Data**
   - **View All Data**
4. Under **Users**, enable the following permissions:
   - **View All Users**
   - **Manage Users** (required only if you have not enabled User Sharing)

STEP 2 | Add the Salesforce app to Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, click **Add a Cloud App**, and select **Salesforce**.



2. Choose the type of Salesforce application:
   - **Connect to Salesforce Account**—Adds your Salesforce production account to Prisma SaaS.
   - **Connect to Salesforce Sandbox**—Adds your Salesforce Sandbox account to Prisma SaaS. *Sandboxes* are special Salesforce accounts that are maintained separately from your product account and are useful for development, testing, and training.
3. Log in to Salesforce.

   After authentication, the new Salesforce app is added to the list of Cloud Apps as Salesforce *n*, where *n* represents the number of Salesforce app instances you have connected to Prisma SaaS.

STEP 3 | (Optional) Give a descriptive name to the Salesforce instance.

1. Click **Settings** and select the Salesforce *n* listed.
2. Enter a descriptive **Name** to differentiate this instance of Salesforce from other instances and click **Done**.

STEP 4 | (Optional) Adjust the maximum number of API calls allowed from Prisma SaaS to Salesforce.

By default, Prisma SaaS can send a maximum of 10,000 API calls to Salesforce.

STEP 5 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 6 | Add policy rules.

When you add a cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays any match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for incidents unique to Salesforce.

STEP 7 | Configure or edit a data pattern.

You can Configure Data Patterns (Basic DLP) to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 8 | Start scanning Salesforce for any possible policy violations or data exposure.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the Salesforce app you just added, select **Actions** > **Start Scanning**.

   Prisma SaaS scans all assets in the associated Salesforce app and identifies incidents. Depending on the number of Salesforce users and assets, it may take some time for Prisma SaaS to complete the process. However, you can Monitor Scan Results on the Dashboard and begin to Assess Incidents. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a ServiceNow App

To begin scanning a ServiceNow app:

STEP 1 | Register Prisma SaaS in the ServiceNow management console.

1. Log in to the ServiceNow management console as admin.
2. Select **System OAuth** > **Application Registry**.
3. Select **New** > **Create an OAuth API endpoint for external clients**.
4. Enter a unique **Name** for Prisma SaaS.
5. If you are using the Istanbul (or higher) release, enter a **Redirect URI/URL**. The redirect you enter depends on the Prisma SaaS location:

   For North America, use:

   ```
   https://app.aperture.paloaltonetworks.com/auth/servicenow/callback
   ```

   For Europe, use:

   ```
   https://app.aperture-eu.paloaltonetworks.com/auth/servicenow/callback
   ```

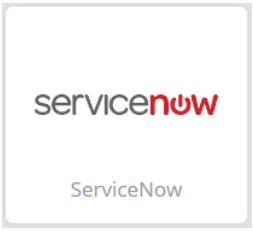
   For Asia-Pacific, use:

   ```
   https://app.aperture-apac.paloaltonetworks.com/auth/servicenow/callback
   ```

6. **Submit** your changes.

STEP 2 | Add the ServiceNow app on Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, click **Add a Cloud App**, and select **ServiceNow**.



2. Select one of the following:
   - **Connect to ServiceNow Account**—Select this option if you're using an earlier release of ServiceNow (Fuji, Geneva, or Helsinki).
   - **Istanbul or higher**—Select this option is you are using the ServiceNow Istanbul (or higher) release.
3. Log in to the ServiceNow app.
   - For Istanbul or higher, enter the **ServiceNow URL** (for example, **`https://acmecorp.service-now.com/`**), **Client ID**, and **Client Secret**.
   - For earlier releases (Fuji, Geneva, or Helsinki) enter the **ServiceNow URL** (for example, **`https://acmecorp.service-now.com/`**), **Client ID**, and **Client Secret**. Also, enter the **Username** and **Password** for your ServiceNow account.

   You can copy the client ID and client secret from the **System OAuth** > **Application Registry** page in the ServiceNow management console.
4. Click **OK**.
5. **Allow** Prisma SaaS access to the ServiceNow account.

   After authentication, the new ServiceNow app is added to the list of Cloud Apps as ServiceNow *n*, where *n* represents the number of ServiceNow app instances you have connected to Prisma SaaS. The instance displays a list of available tables but if you need to add any additional tables, contact Palo Alto Networks Customer Support.

STEP 3 | (Optional) Give a descriptive name to this app instance and specify additional app settings.

1. Go to **Settings** and select the ServiceNow *n* instance listed.
2. Enter a descriptive **Name** to differentiate this instance of ServiceNow from other instances.
3. Enter an **Admin UserName** (for example, **`admin@servicenow.com`**).

   As a best practice, create a separate administrator account and use that email address for Prisma SaaS. If you opt to use an existing admin account instead of a new account, the administrator activities are not tracked on Prisma SaaS. Creating a separate account enables you to monitor events generated by ServiceNow administrators on **Explore** > **Activities**.
4. Click **Done** to save your changes.

STEP 4 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want toAdd a New Asset Rule to look for incidents unique to ServiceNow.

STEP 6 | Configure or edit a data pattern.

You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning ServiceNow for possible policy violations or data exposure.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the ServiceNow app you just added, select **Actions** > **Start Scanning**.

   Prisma SaaS scans files and matches them against enabled policy rules, to verify that your policy rules are effective. Depending on the number of ServiceNow users and assets, it may take some time for Prisma SaaS to complete the process. However, you can Monitor Scan Results on the Dashboard and begin to Assess Incidents. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Slack for Enterprise App

To begin scanning a Slack for Enterprise app:

STEP 1 | Enable the privileges required for communication between Prisma SaaS and the Slack app.

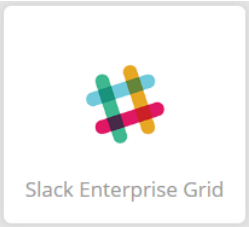
To establish communication, confirm the following:

- Application installation applies to enterprise customers only, and must occur at the top-level enterprise organization.
- The organization owner must contact exports@slack.com and request that the app is enabled for DLP API and integration with Prisma SaaS for successful cloud app connection.

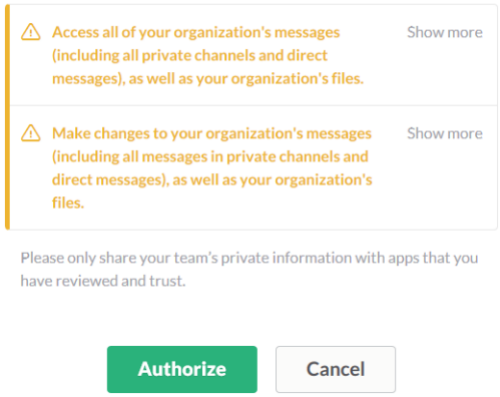
  Only an organization owner can install Prisma SaaS.
- The app is enabled for DLP API access. DLP API access provides visibility into the assets in Slack and allows Prisma SaaS to monitor the sharing of assets.

STEP 2 | Add the Slack app.

1. From the Prisma SaaS **Dashboard**, **Add a Cloud App**.
2. Select **Slack**.



3. **Connect to Slack Account**.
4. Enter your team's Slack domain and **Continue**.
5. **Sign in** with an email address and password for the Slack account with administrative privileges.
6. Review and **Authorize** the access and changes privileges for Prisma SaaS.



Upon successful authentication, the new Slack app is added to the list of Cloud Apps as Slack *n*, where *n* is the number of Slack app instances that you have connected to Prisma SaaS.

STEP 3 | (Optional) Give a descriptive name to this app instance.

1. Select the Slack *n* link on the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Slack from other instances.
3. Click **Done** to save your changes.

STEP 4 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 5 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want toAdd a New Asset Rule to look for risks unique to Slack.

STEP 6 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text that match a data pattern you specify.

STEP 7 | Start scanning the new Slack app for incidents.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Slack app, select **Actions** > **Start Scanning**.

STEP 8 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Begin Scanning a Workplace by Facebook App (Beta)

Before you can begin scanning a Workplace by Facebook app, you must configure a token that generates an app with specific user permissions enabled and a page, a type of bot for your Workplace community. The page name reflects the name of your custom integration, and the profile picture matches the icon you chose when creating the custom configuration. As you prepare the Workplace account, take note of the token

shown to you when creating your custom integration, since it is shown only once, and required to complete the setup of the Workplace app on Prisma SaaS and to read and write posts on your page.

To begin scanning a Workplace by Facebook app:

STEP 1 | Prepare to connect your Workplace by Facebook account to Prisma SaaS.

1. Log in to the Workplace by Facebook console as an administrator.
2. In your company dashboard, select **Integrations** > **Create Custom Integration**.
3. Choose a relevant name and description for the app and click **Create**.
4. (Optional) Select an icon for the app by clicking **Update** to display any time the app is seen, such as in a group posting.

STEP 2 | Each Workplace app comes with unique **Permissions** to control the information being read or written to by that app. Grant the following permissions:

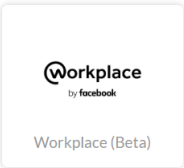
Permission	Description
Read Group Content	Read posts, comments, and member profiles in selected groups.
Read Security Logs	Access details of security events, including login attempts and password requests.
Read user email	Access any group member's email address.
Read all messages	Access messages sent to anyone in the community.
Read user timeline	Read all posts made by group members on a user's timeline
Manage Group Content	Manage posts and comments in selected groups.
Manage Groups	Edit or remove selected groups and their members.
Impersonate Account	Post and comment in groups and read messages from any user account.

STEP 3 | Click **Create Access Token** and **understand** the token terms. Click **Done** and **Save** the configuration.

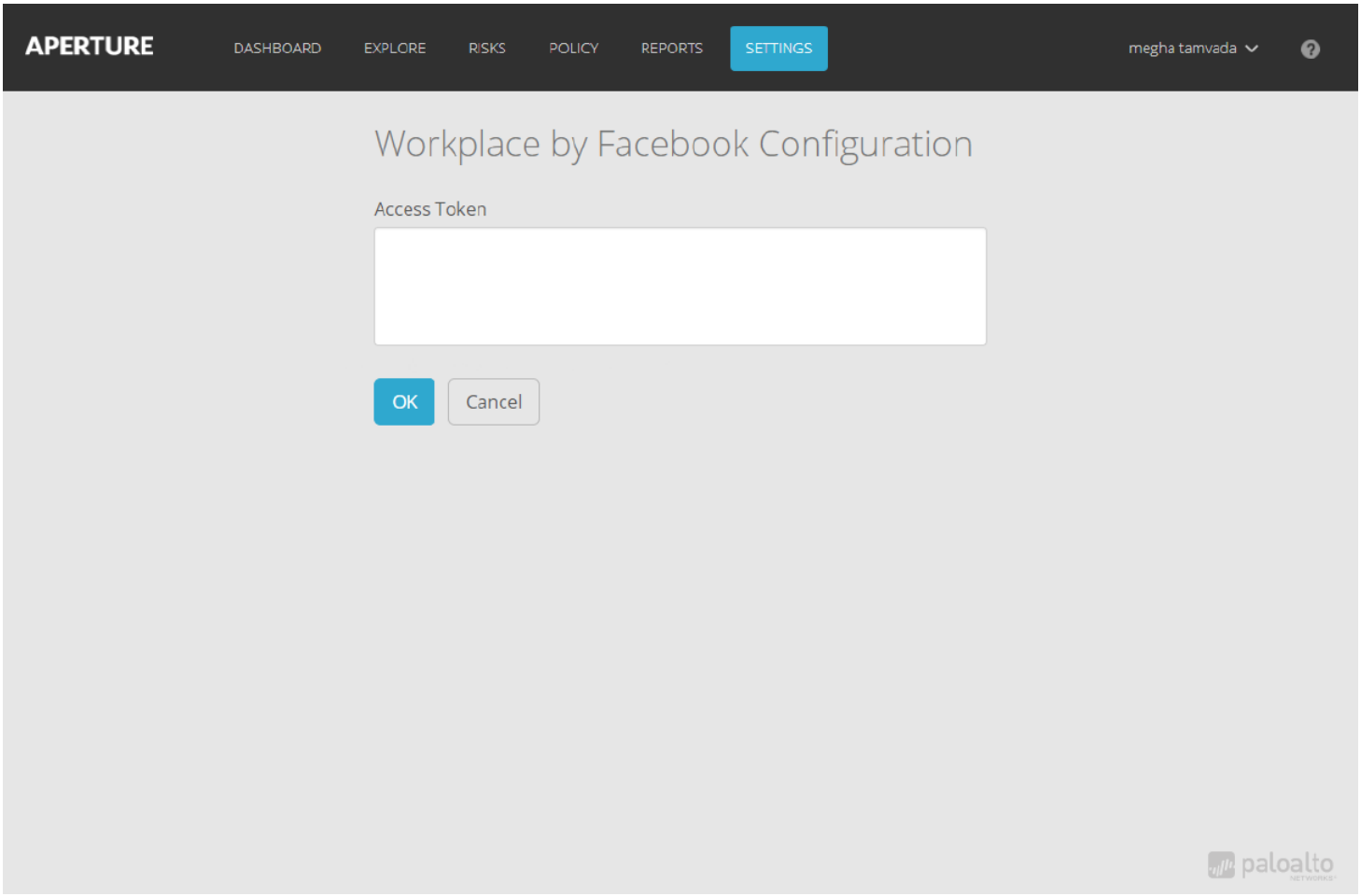
Copy and safely store the access token shown to you, as you will need the token to setup your account on Prisma SaaS and make API calls. As a system administrator, it is important to make sure that you only share access tokens with trusted developers within your organization and Facebook-approved third-party developers.

STEP 4 | Add the Workplace by Facebook app to Prisma SaaS.

1. From the Prisma SaaS **Dashboard**, click **Add a Cloud App**, and select **Workplace by Facebook**.



2. Select **Connect to Account**.
3. Paste the **Access Token** copied in the previous step and click **OK**.



STEP 5 | (Optional) Give a descriptive name to this app instance and specify an incident reviewer.

1. Select the Workplace by Facebook in the Cloud Apps list.
2. Enter a descriptive **Name** to differentiate this instance of Workplace by Facebook from other instances.

STEP 6 | Define global scan settings.

- Define Your Internal Domains
- Define Untrusted Users and Domains
- Enable Data Masking

STEP 7 | Add policy rules.

When you add a new cloud app, Prisma SaaS automatically scans the app against the default data patterns and displays the match occurrences. As a best practice, consider the business use of your app to determine whether you want to Add a New Asset Rule to look for incidents unique to Workplace by Facebook.

STEP 8 | (Optional) Configure or edit a data pattern.

You can Configure Data Patterns to identify specific strings of text, characters, words, or patterns to make it possible to find all instances of text or information to match a data pattern you specify.

STEP 9 | Start scanning the new Workplace by Facebook app for incidents.

1. Select **Settings** > **Cloud Apps & Scan Settings**.
2. In the Cloud Apps row that corresponds to the new Workplace by Facebook app, select **Actions** > **Start Scanning**.

   Prisma SaaS scans all assets in the associated Workplace by Facebook app and identifies incidents. Depending on the number of assets, it may take some time to complete the process. However, as soon as you begin to see this information populating on the Prisma SaaS **Dashboard**, you can begin to Assess Incidents.

STEP 10 | Monitor the results of the scan.

As Prisma SaaS scans files and matches them against enabled policy rules, you can Monitor Scan Results on the Dashboard to verify that your policy rules are effective. Monitoring the progress of the scan during the discovery phase allows you to Fine-Tune Policy to modify the match criteria and ensure better results.

Add Unsanctioned Device Access Control to Prisma SaaS

You can control unmanaged and employee-owned device access to your sanctioned SaaS applications by configuring the Prisma SaaS as your SAML proxy. Unsanctioned device access control utilizes SAML redirection by proxy by redirecting traffic through your next generation firewall, decreasing vulnerability to data exfiltration and malware propagation. When an employee needs to access a SaaS app on an unmanaged computer or mobile device, the authorization request is sent through the Prisma SaaS SAML proxy and authenticated by your identity provider. Once authenticated, the user is redirect through the firewall allowing visibility into access and control of corporate resources on your SaaS app.

There are several options available for an identity provider (IDP) and service provider (SP) but an integration with Okta as the Identity Provider and G Suite as the SaaS application (Service Provider) are used in this example. Other identity providers supported are Google IDP, Ping, Azure AD, and ADFS.

Configure Unsanctioned Device Access Control by following these steps:

Step	Details
1.	A Prisma SaaS application integration with the IDP allows you to authenticate requests to sanctioned SaaS applications from unmanaged devices.
2.	Configure the IDP on Prisma SaaS to authenticate access using SAML Proxy 2.0.
3.	A SaaS app (SP) integration with the IDP authenticates user requests before granting access to SaaS application resources. An app integration for each SaaS application must be created on the IDP.
4.	Configure the SaaS application on Prisma SaaS to authenticate the user and redirect traffic to your firewall. Each SaaS application you want to control access to must be configured on Prisma SaaS.
5.	Configure the IDP on the SP to establish a trusted relationship to identify a user, grant access and authenticate a Prisma SaaS session to redirect the traffic through the next generation firewall.
Configure your Clientless VPN.	Configure Prisma SaaS on your Clientless VPN to redirect the remote users' authentication request and application traffic through the firewall.
7.	Configure the firewall portal settings on Prisma SaaS to create a trusted relationship between the firewall and Prisma SaaS. The portal settings can also be configured to use your domain, IP address, combination of domains or IP addresses, or Prisma Access.

Configure Unsanctioned Device Access Control

To control unmanaged and employee-owned device access to your sanctioned SaaS applications, add application integration on your Identity Provider for Prisma SaaS and each application to authenticate SAML 2.0 access. Configure Prisma SaaS by adding your IDP SSO URL and configure each application with the same SSO URL for a transparent and seamless experience. After your IDP, service providers, and Prisma SaaS are configured, add your next generation firewall on Prisma SaaS. For visibility and control of unsanctioned devices, Prisma SaaS offers the flexibility of adding your clientless VPN portal that your host yourself or is on your Prisma Access infrastructure.

You must be a Super Admin or Admin to configure SAML Proxy on Prisma SaaS.

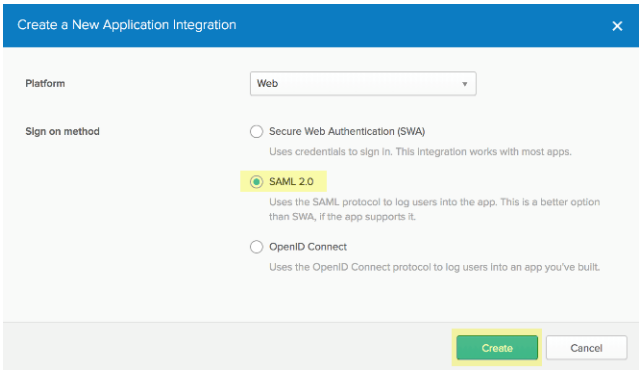
This document details an example integration with Okta as the identity provider and G Suite as the service provider but you can configure Google IDP, Ping, Azure AD, and ADFS as the identity provider.

STEP 1 | Create a Prisma SaaS app on your Identity Provider.

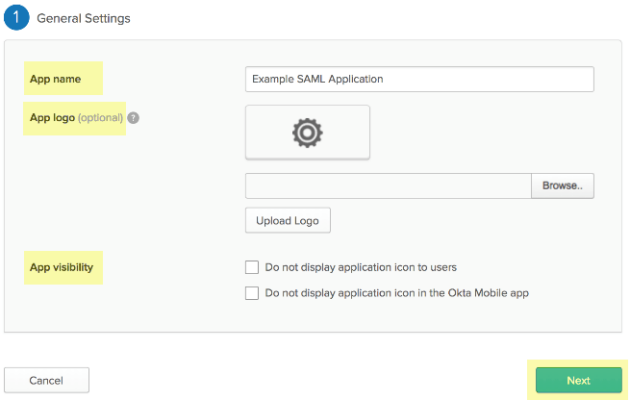
By creating an application integration for Prisma SaaS with your Identity Provider, you can control access to SaaS applications on unmanaged devices on external networks using SAML 2.0 protocol.

1. Log in to your Okta organization using an account with administrative privileges.

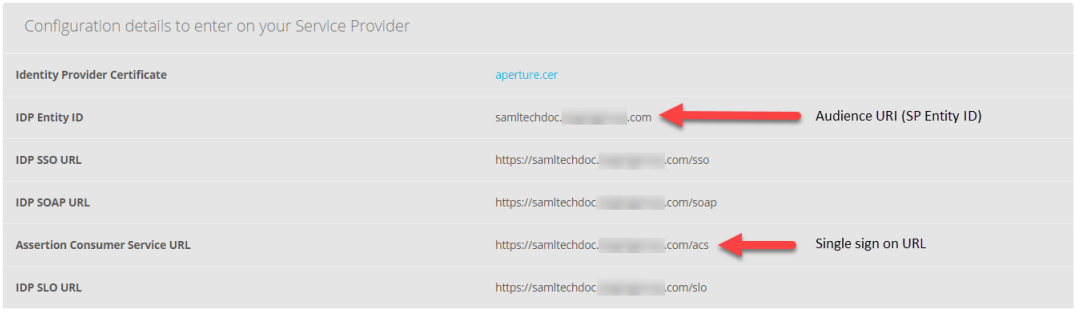
   If you don't have an Okta organization, you can create a free Okta developer edition organization.
2. Create a new application integration by selecting **Admin** > **Add Applications** > **Create New App** > **SAML 2.0** > **Create**.
3. Select **SAML 2.0** and **Create** the application integration.



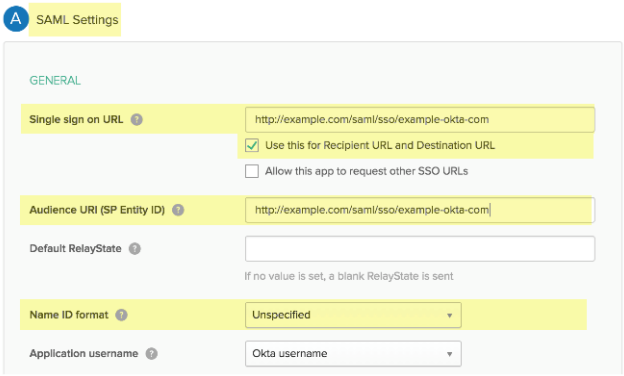
4. Enter an **App name** for Prisma SaaS.
5. (Optional) Upload an image for the **App logo** and select **App visibility**.
6. Click **Next**.



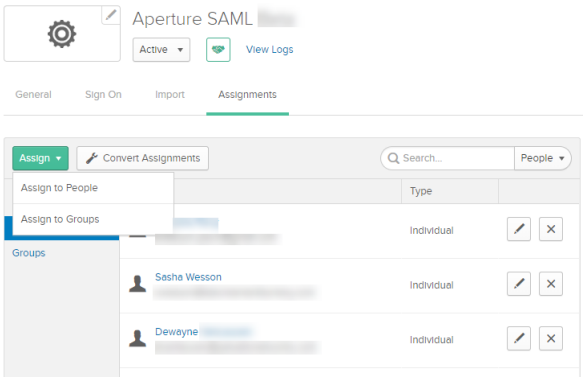
7. Log in to Prisma SaaS, select **Settings** > **SAML Proxy**, and enable the feature.
8. Click **Add Identity Provider** to gather the IDP configuration details.



9. On the Okta SAML Settings screen, enter the Prisma SaaS **Assertion Consumer Service URL** for **Single sign on URL**.
10. Enter the Prisma SaaS **IDP Entity ID** for **Audience URI (SP Entity ID)**.
11. Configure the **Default RelayState**, **Name ID format**, and **Application username**, and click **Next**.



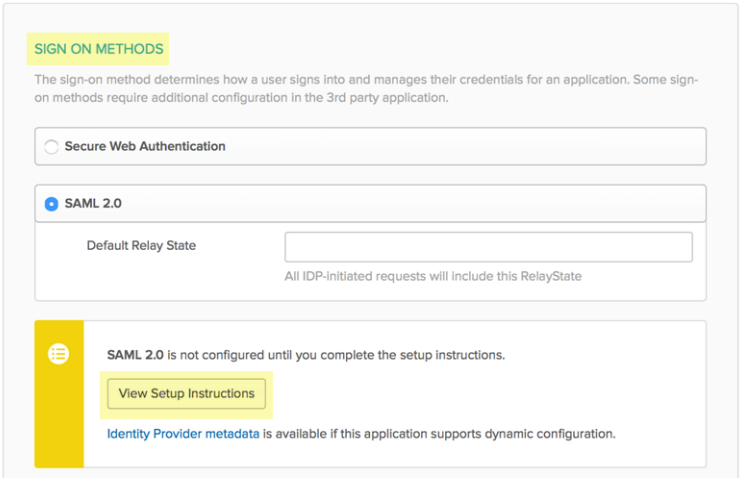
12. Answer Okta Support questions and click **Finish**.
13. Select **Assignments** > **Assign** to add and manage people or groups.



STEP 2 | Add your identity provider on Prisma SaaS.

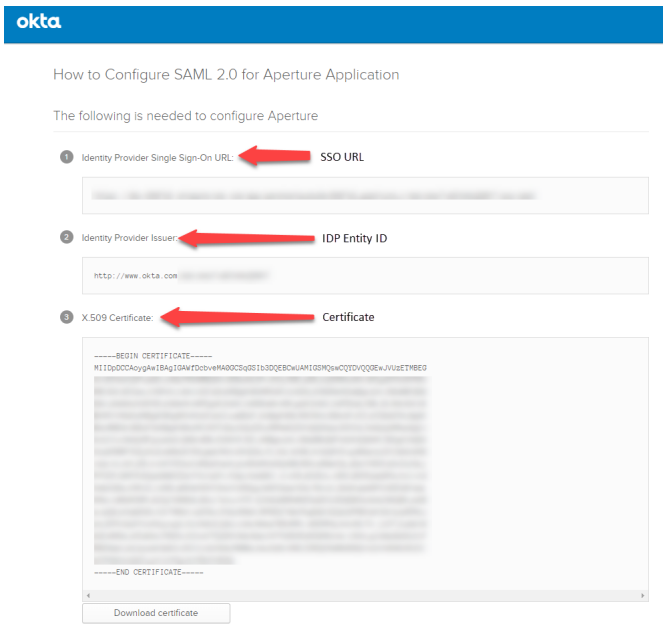
Configure the IDP on Prisma SaaS to authenticate the user before redirecting access through the firewall and to the SaaS application. Use the IDP SSO URL, Identity Provider Issuer and Certificate from Okta to configure the identity provider settings on Prisma SaaS.

1. Log in to Okta, select **Admin** > **Applications** and select your Prisma SaaS SAML 2.0 application.
2. Select **Sign On** > **View Setup Instructions**.

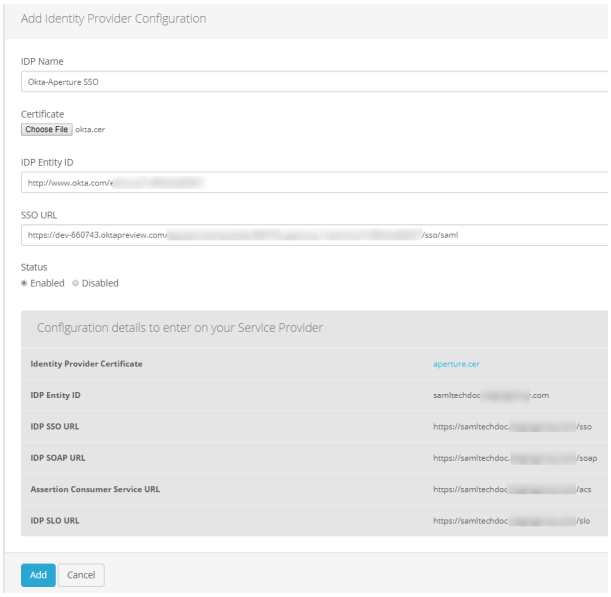


3. Locate the Okta SSO URL, IDP Entity ID and download the certificate to configure Prisma SaaS.

   When downloading the Okta X.509 certificate, you must change the CERT extension to either CER or CRT file extension.



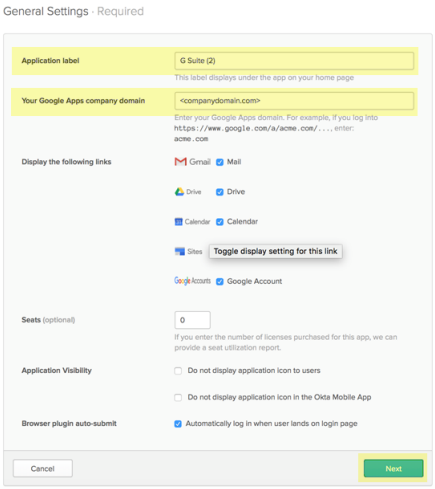
4. Log in to Prisma SaaS, and select **Settings** > **SAML Proxy** > **Add Identity Provider**.
5. Enter an **IDP Name**.
6. Click **Choose File** and upload the Okta **X.509 Certificate**.
7. For **IDP Entity ID**, enter the Okta **Identity Provider Issuer**.
8. For **SSO URL**, enter the Okta **Identity Provider Single Sign-On URL** and **Add** the Identity Provider on Prisma SaaS.



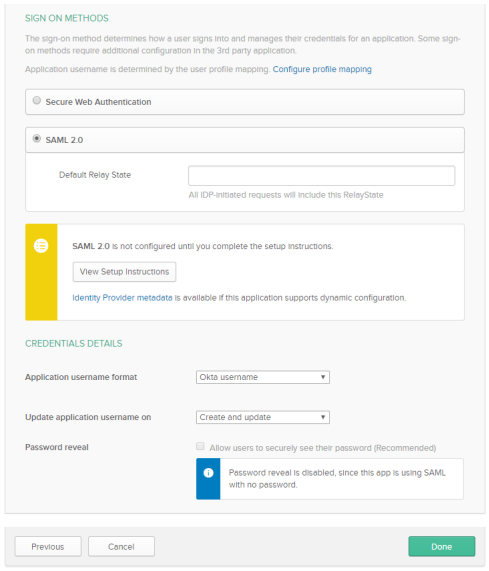
STEP 3 | Create a Service Provider app on your Identity Provider.

Configure the SSO URL on your IDP for your SaaS app and IDP when you add an application integration, providing a transparent experience. When you add the SaaS application to your IPD, access is authenticated through the Prisma SaaS SAML proxy before redirecting traffic through the firewall. You need the Identity Provider Sign-in URL to direct users to sign in and the certificate from the IDP to validate SAML signatures when using SSO. Each SaaS application must be configured on your Identity Provider to control unmanaged device access.

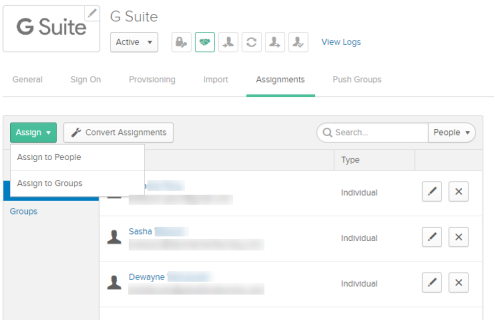
1. Log in to Okta, select **Admin** > **Add Applications**, and search for **G Suite**.
2. Select G Suite and click **Add**.
3. Enter an **Application label**.
4. Enter **Your Google Apps company domain** and click **Next**.



5. Select **SAML 2.0** and click **Done**.



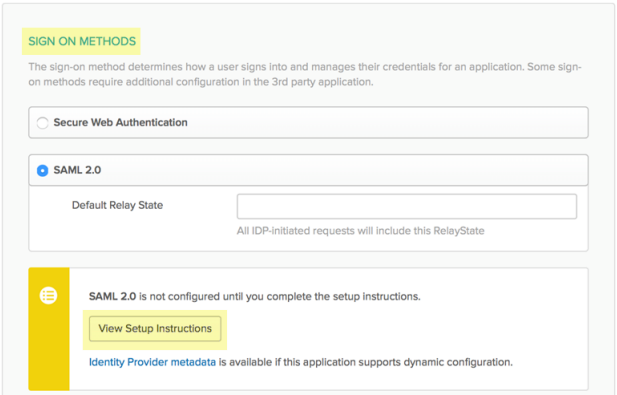
6. Select **Assignments** > **Assign** to add and manage people or groups.



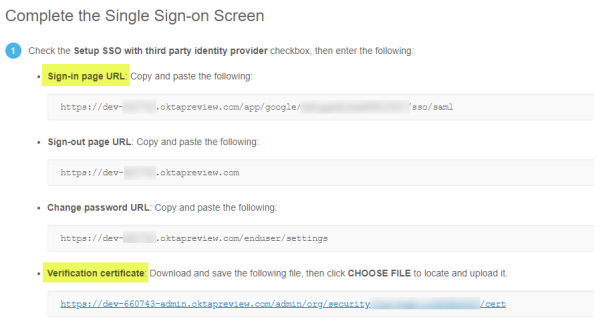
STEP 4 | Add the Service Provider on Prisma SaaS.

Each SaaS application must be configured on Prisma SaaS to grant access using the same IDP SSO URL and redirect traffic to the SaaS application through the firewall. You need the Okta Single Sign-on URL and Verification Certificate for the SaaS application, and the Entity ID and ACS URL from Prisma SaaS to configure the SaaS application on Prisma SaaS.

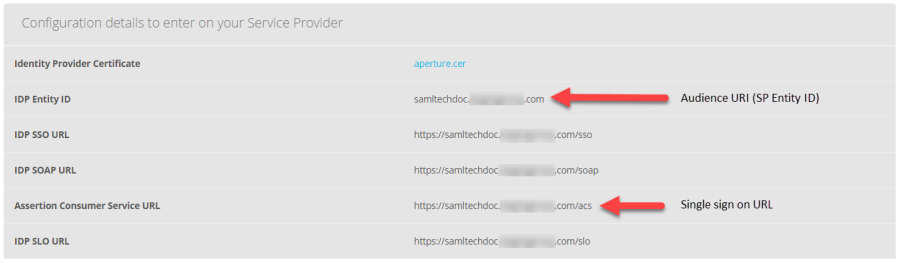
1. Log in to Okta, select **Admin** > **Applications** and select your G Suite application to gather the SaaS details.
2. Select **SAML 2.0** and click **View Setup Instructions**.



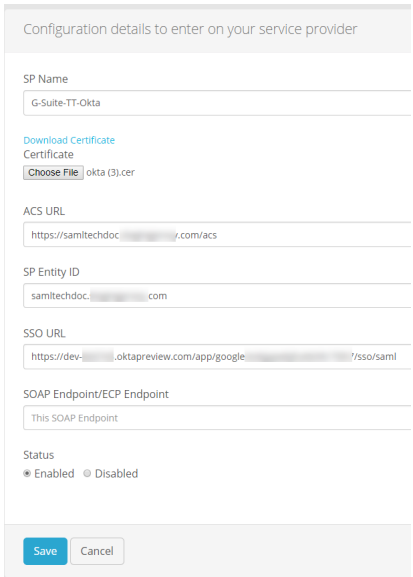
3. Locate the Single Sign-On Screen information for G Suite, download the verification certificate and copy the **Sign-in page URL**.



4. On Okta, click **Applications**, and select the Prisma SaaS SAML 2.0 application.
5. Click **Sign On** > **View Setup Instructions**
6. Log in to Prisma SaaS, select **Settings** > **SAML Proxy** > **Identity Provider Settings** > **Edit** to locate the **ACS URL**, and **SP Entity ID**.



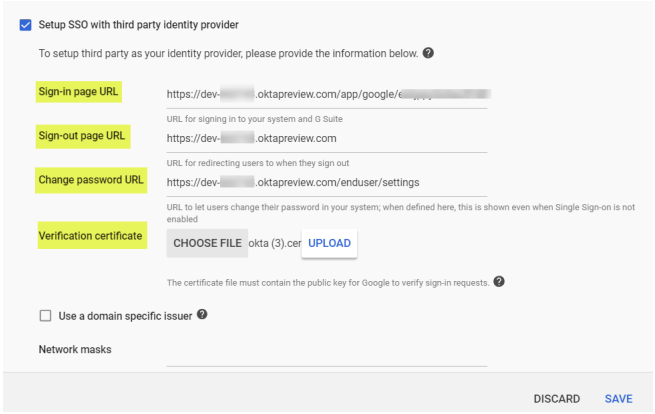
7. On Prisma SaaS, select **Settings** > **SAML Proxy** > **Add Service Provider**.
8. Enter a **SP Name**.
9. Upload the Okta **Verification Certificate** to Prisma SaaS.
10. For the **ACS URL**, enter the Prisma SaaS **Assertion Consumer Service URL**.
11. For the **SP Entity ID**, enter the Prisma SaaS **IDP Entity ID**.
12. For the **SSO URL**, enter the Okta **Sign-in page URL**.
13. (Optional) Configure the **SOAP Endpoint/ECP Endpoint** on Prisma SaaS to enable communication in HTTP and its XML language as the mechanisms for information exchange. The endpoint is URL where your service can be accessed by a client application.
14. **Add** the Service Provider configuration on Prisma SaaS.



STEP 5 | Configure the Identity Provider on the Service Provider.

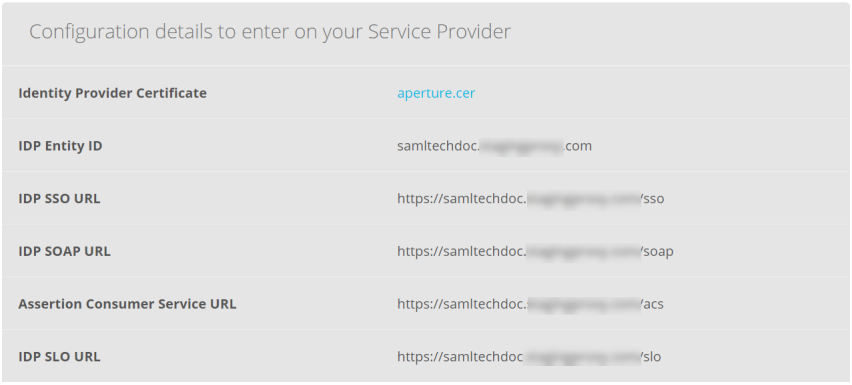
Configure the SaaS application to consume an assertion from the Identity Provider to grant the user access after being authenticated.

1. Log in to Okta, select **Admin** > **Applications** and select your G Suite application.
2. Select **SAML 2.0** and click **View Setup Instructions**.
3. Locate the **Single Sign-On Screen section**.
4. Log in to the G Suite admin console.
5. Click **Security** > **Set up single sign-on (SSO)** and select **Setup SSO with third party identity provider**.
6. Enter the setup SSO information from Okta, upload the Verification certificate, and click **Save**.



STEP 6 | Log in to Prisma SaaS and select **Settings** > **SAML Proxy** > **Identity Provider Settings** > **Edit** to locate the details required to Configure Your Clientless VPN.

When you configure your Clientless VPN, Prisma SaaS will intercept the authentication request and redirect the application traffic through the clientless rewriter on the firewall.

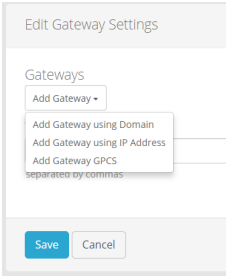


STEP 7 | Configure your Gateway Settings on Prisma SaaS.

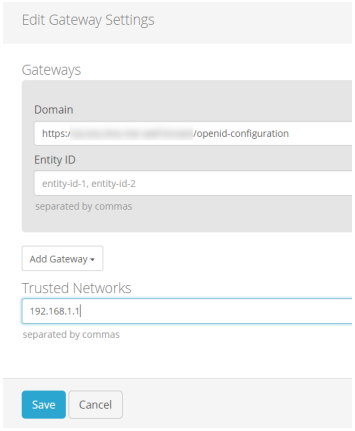
Prisma SaaS uses the gateway settings to whitelist your trusted networks. Any sanctioned SaaS application traffic that originates from your trusted networks is not redirected to the clientless VPN portal on the firewall. To secure all traffic that is not from a trusted network, Prisma SaaS creates a trust relationship between the clientless VPN (self-hosted or Prisma Access) and Prisma SaaS to offer a transparent experience when a user accesses a sanctioned SaaS application on an unmanaged device.

To whitelist IP addresses, you have two options. If your clientless VPN gateway is self-hosted you must specify a domain or IP address; if it is hosted on Prisma Access, you must provide the API key to fetch the IP addresses dynamically.

1. Log in to Prisma SaaS, select **Settings** > **SAML Proxy** > **Gateway Settings** > **Edit** to add your gateway settings.



2. Choose one of the following:
   - Select **Add Gateway using Domain** or to enter your **Domain** URL and **Entity ID**. Enter the IP addresses of your **Trusted Networks** and **Save**.



   - Select **Add Gateway using IP Address** to enter the IP address and (Optional) **Entity ID**. Enter the IP addresses of your **Trusted Networks** and **Save**.
   - If you are using a clientless VPN Gateway hosted on Prisma Access, the trusted networks IP addresses are retrieved dynamically using the API. Select Add Gateway using GlobalProtect Cloud Service to enter your **GlobalProtect Cloud Service Gateway URL** and **GlobalProtect Cloud Service API Key**.

Reauthenticate to a Cloud App

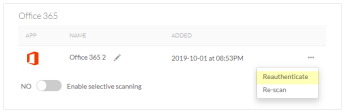
When you connect Prisma SaaS to one of your sanctioned SaaS applications, you must provide login credentials that enable the service to establish a secure connection with the cloud app. Prisma SaaS and the app maintain this secure connection (in most cases using token-based authentication). In some cases, you might need to reauthenticate to a cloud app when:

- There is a network connectivity issue between the two services.
- You change the password associated with the login account.
- The administrative user associated with the login account changes credentials to those associated with a different administrator.

If you encounter authentication errors when you retrieve a token for Prisma SaaS, see Authentication Errors.

STEP 1 | Select **Settings** > **Cloud Apps & Settings**.

STEP 2 | Select the cloud app from the list and click **Reauthenticate**.



STEP 3 | Follow the same process to log in to the app that you did when you first added the app. See the specific app section in Add Cloud Apps to Prisma SaaS for details on what privileges are required for each app and for specific steps to successfully authenticate.

STEP 4 | To begin scanning the app after you successfully reauthenticate, select **Actions** > **Start Scanning**.

Stop Scanning a Managed Cloud App

If you want to exclude or stop scanning a cloud app, you can remove it from Prisma SaaS. Keep in mind that, to secure an app, Prisma SaaS builds a database of all assets and users associated with that app so the process of deleting an app takes some time to complete.

STEP 1 | Select **Settings** > **Cloud Apps & Settings**.

STEP 2 | Select **Actions** > **Delete Cloud App** in the row that corresponds to the cloud app instance you want to stop scanning.

Rescan a Managed Cloud App

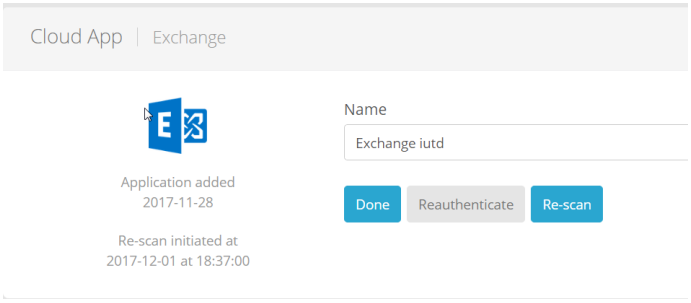
When you Configure Data Patterns, all connected cloud apps are automatically scanned to detect sensitive content that match on these patterns. If you add or modify a data pattern, Prisma SaaS matches content going forward and does not look for matches on previous scan results. To find matches for content that has already been scanned, you can **Rescan** a specific cloud app or exclude a cloud app from all scans by Stop Scanning a Managed Cloud App.

The rescan is a resource intensive and time consuming process, depending on the volume of assets in your cloud app the rescan may take a long time to complete.

STEP 1 | Select **Settings** > **Cloud Apps & Settings**.

STEP 2 | Select the cloud app instance name and **Re-scan**.

The Re-scan option is available for the cloud app if the option is displayed, and rescans are limited to once every three days. A re-scan timestamp indicates when you initiated it.



Manage Prisma SaaS Policy

Policy in Prisma SaaS is simple and aims to create an awareness of user actions and minimize the risks associated with the use of SaaS and IaaS applications. Prisma SaaS policy allows you to monitor and enforce responsible use of assets (files or other data) and protect against malware, malware propagation, regulatory non-compliance, and data leaks that are caused by human errors, such as promiscuous or inadvertent sharing, and sharing content using links without establishing an expiration date. When Prisma SaaS detects a policy violation, it generates an alert to notify you of an active incident related to malware, a security breach, or a compliance violation and, if configured, takes automatic action to remediate the incident.

Prisma SaaS Policy

Prisma SaaS policy gives you the controls to manage assets, user activity, third-party apps and security controls across the different cloud SaaS and IaaS applications that the service supports. The different types of policy rules that you can configure are:

- **Asset Rules**—Asset policy allows you to identify issues with data governance. To know about what type of content is stored in the cloud app and who has access to it, content security rules use data patterns and match criteria to automatically discover activity in your sanctioned SaaS applications and remediate incidents around data segregation, personal and financial information, intellectual property, malware, data breaches, and sensitive documents in your organization. See Configure Prisma SaaS Asset Rules
- **User Activity Rules**—User activity policy allows you to identify abnormal behavior. To know about unusual user activity or compliance violations, you can use match criteria to monitor activity such as downloading or exporting data out of the SaaS application, set the activity threshold that triggers a policy violation, and track the IP address where the activity was initiated. See Configure Prisma SaaS User Activity Rules
- **Security Control Rules**—Security controls policy allows you to define rules that monitor email activity in SaaS applications and proper configuration in IaaS applications to prevent data exfiltration and exposure. These rules unlike the content security policy focus on administrators of an application instead of users. See Configure Prisma SaaS Security Control Rules
- **Third-party apps Rules**—Third-Party Apps policy allows you to detect and remediate any non-compliant third-party apps to prevent data exfiltration or unauthorized access. See Configure Third-Party App Settings

For a list of file types that the service can scan for issues, see Supported File Types, and see Supported SaaS Applications to learn what type of content is scanned for each application and what actions are available.

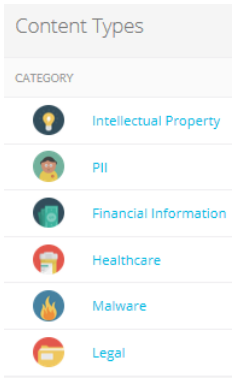
As Prisma SaaS starts scanning your cloud apps, use the **Dashboard** to review information about the assets, content types, incidents, users, policy violations, collaborators, and domains that the service discovers during the scan. See Monitor Scan Results on the Dashboard.

Configure Data Patterns (Basic DLP)

Prisma SaaS offers the following data pattern types:

- **predefined** data patterns—the service automatically activates after a scan to match on keywords, which you can modify, and pre-tested strings.

  Prisma SaaS includes several predefined data patterns that automatically begin scanning content and detecting incidents as soon as you Add Cloud Apps to Prisma SaaS. Predefined data patterns are grouped into six categories by content type:



- **custom** data patterns—you create from scratch to match on keywords and strings of text, such as particular characters, words, or patterns of characters and make it possible to find all instances of text that match a certain pattern, or return a value if the pattern is not found.
- **file property** data patterns—you create from scratch to match on file metadata.

  If you assign classification tags or labels as metadata to files, with the file property data pattern you can specify any custom or extended file property as a name-value pair to match in policy rules.

After you're familiar with the predefined data patterns and how they work, you can modify the predefined data patterns as desired or define your own new data pattern. You can then view and filter incidents to determine if the matched content to your configured data patterns poses a risk to your organization.

- Modify a Predefined Data Pattern (Basic DLP)
- Create a Custom Data Pattern (Basic DLP)
- Add a File Property Data Pattern
- View and Filter Data Pattern Match Results (Basic DLP)
- Prisma SaaS Predefined Data Patterns
- Configure a Machine Learning Data Pattern
- Configure a WildFire Analysis Data Pattern
- Configure Regular Expressions
- Enable or Disable a Data Pattern (Basic DLP)

Prisma SaaS Predefined Data Patterns

Prisma SaaS provides predefined data patterns that enable you to discover sensitive content and how that content is being shared or accessed in your managed cloud applications. The service automatically scans your cloud applications when you Add Cloud Apps to Prisma SaaS using predefined data patterns, classifies all documents using machine learning, and checks hash on all Microsoft Office documents, PDF, and portable executable files against WildFire rules without requiring you to create any policies.

As the service displays incidents that match the predefined data patterns, you can explore and filter the results to determine if the content that the service reported poses a risk to your organization. Then, you can do any of the following to prevent future violations:

- Create a custom data pattern.
- Remediate issues.
- Modify a predefined data pattern.
- Modify a policy rule.

Prisma SaaS categorizes predefined data patterns as follows:

Content Category	Scans for
Intellectual Property 	Scans files for RSA and AWS secret keys and confidential documents that are at risk of being stored or shared in a way that could result in a loss of intellectual property. You can specify **File Extensions to Exclude**. Excluding files that are unlikely to have intellectual property information that is public and not at risk of being exposed or shared in non-compliant ways helps minimize false positives.
Personally Identifiable Information (PII)	Scans for PII data, such as U.S., Canadian, and international social security numbers. It also scans for Tax IDs from the U.S., Australia, Canada, Germany, and the UK for both the Unique Tax Payer ID, (UTR) and National Insurance Number (NINO) formats.

Content Category	Scans for
	For each type of PII Prisma SaaS scans for, you can specify the minimum number of occurrences required to trigger a match. As the number of violations for a specific asset exceeds the specified threshold, the severity of the risk increases.
Financial Information 	Scans for financial data including credit card numbers, credit card magnetic stripe data, international bank account numbers, financial accounting, bank statements, personal finance, invoices, and other financial documents. By default, Prisma SaaS performs strict checking on credit card numbers to reduce false positives.
Healthcare Information 	Scans healthcare documents for exposure to sensitive or confidential information, related to Clinical Laboratory Improvement Amendments (CLIA) number, Drug Enforcement Administration (DEA) number, and other healthcare documents. Prisma SaaS uses machine learning algorithms to classify information and to detect sensitive information.
Legal Information 	Scans legal documents for exposure to sensitive or confidential information related to bankruptcy filings, lawsuits, business agreements, mergers and acquisition information, patents, and other legal documents. Prisma SaaS uses machine learning algorithms to classify information and to detect sensitive information.
Malware 	Scans files using WildFire Analysis to detect and protect against malicious portable executables (PEs), Microsoft Office Files, Adobe Portable Document Format (PDF) files, and known threats based on file hash. A hash is a unique fingerprint of a file. It is string of letters and digits that is generated as a result of running a file through a cryptographic hash function. By default, Prisma SaaS automatically submits portable executable files to the WildFire service for analysis (**Windows executables**).

Proximity Keywords

Keywords reduce false positives, and improve accuracy. Prisma SaaS assigns an asset a higher accuracy probability if:

- **50-byte distance**—keyword is within a 50-byte distance of the expression. If a document has **<16 digit number>** immediately followed by **Visa:**, that's more likely to be a credit card number. But if **Visa** is the title of the text and the 16-digit number is on the *last* page of the 22-page document, that's less likely to be a credit card number.
- **Keyword group**—More than one keyword in your keyword group appears within 50#bytes of the expression.

Modify a Predefined Data Pattern (Basic DLP)

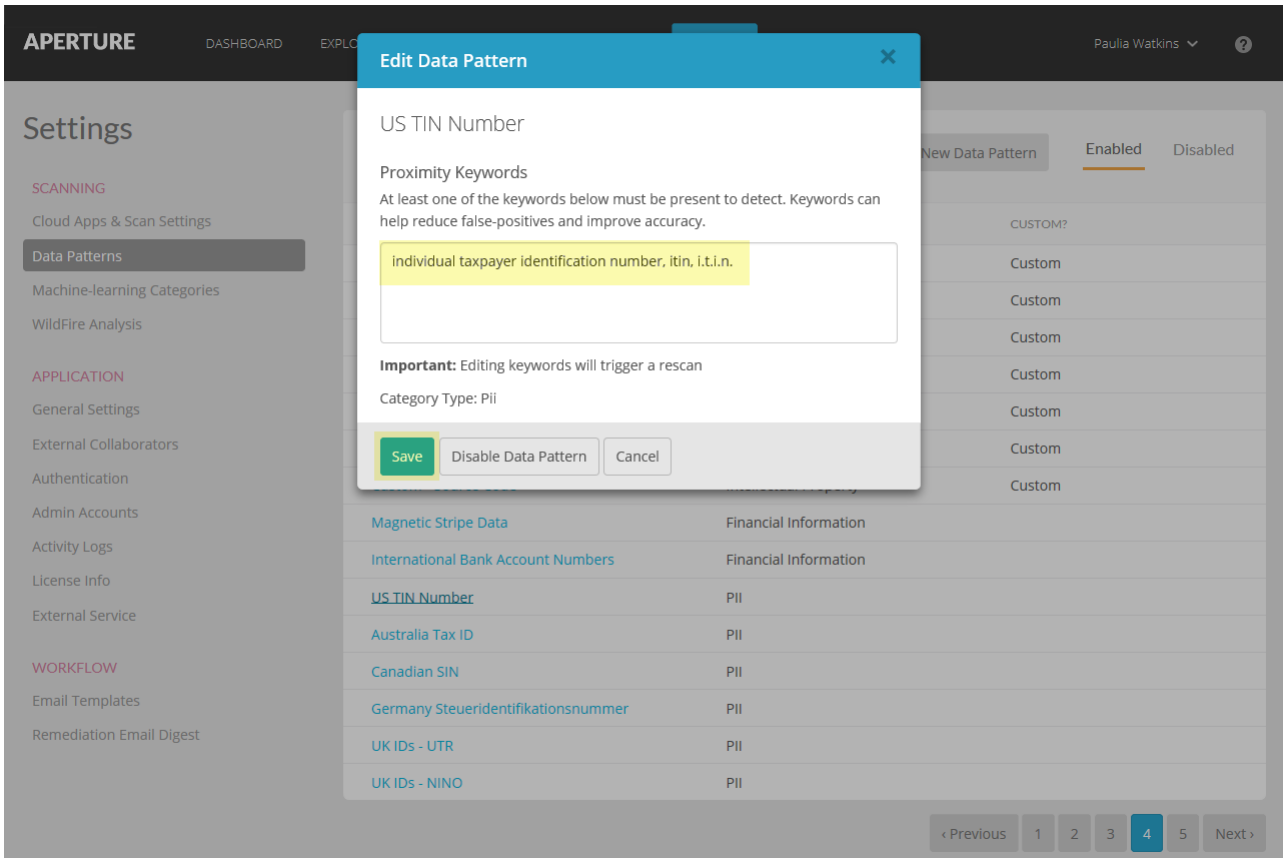
Prisma SaaS provides predefined data patterns that automatically scan for matches against the default rules for Data Leak Prevention (DLP) and Threat Prevention as soon as you Add Cloud Apps to Prisma SaaS. You can edit the proximity keywords for any predefined data pattern to narrow the match results, reduce false positives, and improve accuracy.

Select the predefined data pattern to edit.

1. Select **Settings** > **Data Pattern**.
2. Select a predefined data pattern by **Name** from the list.

For easy identification, the predefined data patterns do not have Custom in the title.

3. Enter the new proximity keywords for the predefined data pattern and click **Save**.



Prisma SaaS will immediately begin scanning and display the match results in **Explore** > **Assets** from this view, you can View and Filter Data Pattern Match Results.

Add a File Property Data Pattern

For data governance and protection of information, if you use classification labels or embed tags in MS Office and PDF documents to include more information for audit and tracking purposes, you can create a file property data pattern to match on the metadata or attributes that are a part of the custom or extended properties in the file. Regardless of whether you use an automated classification mechanism such as Titus or require users to add a tag, you can specify a name-value pair to match on a custom or extended property embedded in the file.

For example, you can define a file property data pattern to create an incident when a user on your network uploads a file labeled as Customer Data to a folder that has external collaborators.

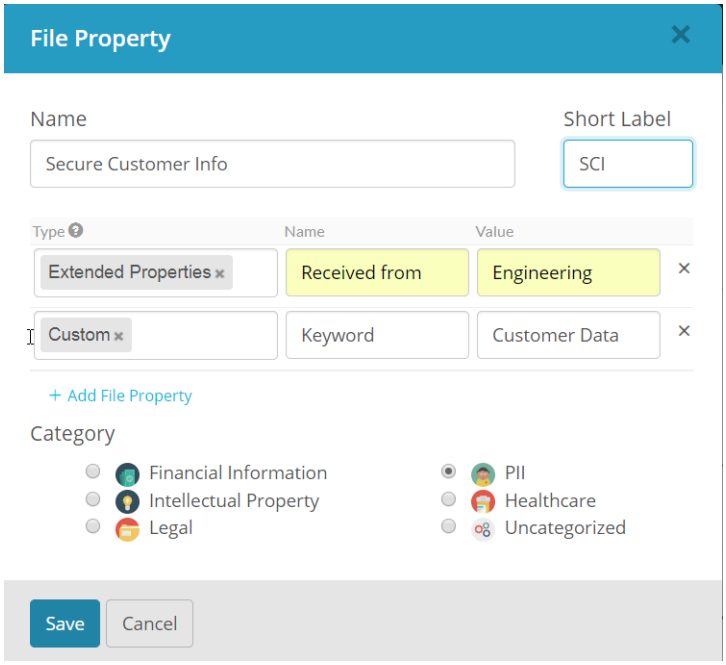
STEP 1 | Select **Settings** > **Data Patterns** > **Add New** > **Add New File Property**.

Prisma SaaS supports file property data patterns in MS Office and PDF documents. Both the OLE (.doc/.ppt) or XML (.docx/.pptx) formats of MS Office are supported.

STEP 2 | Enter a **Name** and a **Short Label** for the file property data pattern.

STEP 3 | Select the **Custom** or **Extended Properties** that you want to include as match conditions.

Enter the name-value pair for the property that you want to look for. You can add as many file properties as you'd like. When you later reference the file property data pattern in an asset rule in Step 6 below, a boolean OR match is used in the match criteria.



STEP 4 | Select the predefined category with which you want to associate this file property.

STEP 5 | **Save** the file property data pattern.

STEP 6 | Add a New Asset Rule and add your new file property data pattern as match criteria.

In the match criteria, you can decide whether you want to look for any property, or more than or fewer than a specified number of properties that you've included in the file property data pattern.

Create a Custom Data Pattern (Basic DLP)

Prisma SaaS offers various data pattern types, and each type has unique advantages. Use a custom data pattern to build a data pattern from scratch.

Custom data patterns cannot be disabled, they can only be deleted.

Data patterns use a combination of content analysis techniques to identify the content and rate it with a low to high confidence score:

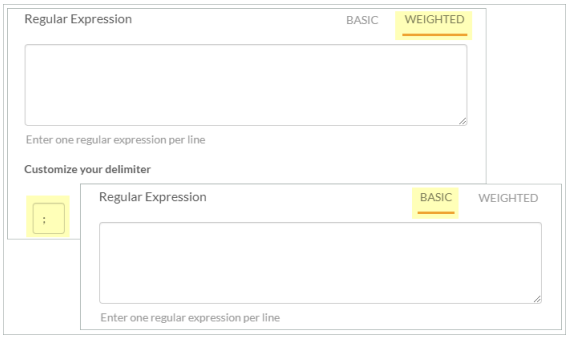
- regular expressions
- machine learning
- proximity keywords
- check sum

STEP 1 | Select **Settings** > **Data Patterns** > **+Add New** > **Add New Custom Data Pattern**.

STEP 2 | Name the data pattern.

1. Enter a **`Data Pattern Name`** for the data pattern.
2. Enter a **`Short Label`** description for the data pattern that is 12 characters or less.

STEP 3 | Define the regular expression, including whether you want a **Basic** or **Weighted** regular expression.

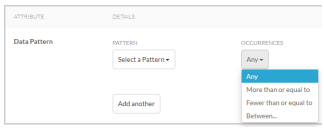


STEP 4 | Select a **Category** to scan, then **Save**.

If you select uncategorized category, Prisma SaaS scans all assets in your sanctioned cloud apps to locate a match for the expressions, and such a scan takes longer to return results than if the service only scanned a specific category.

STEP 5 | (Optional) Enable the custom data pattern.

STEP 6 | Modify a policy rule or add a new asset rule to use the new data pattern as match criteria.



Configure a Machine Learning Data Pattern

Prisma SaaS uses supervised machine learning algorithms to sort sensitive documents into Financial, Legal and Healthcare top-level categories for document classification and categorization. These top-level categories may contain documents that also classify into sub-categories, such as a financial accounting document classifies as a sub-category to the financial top-level category.

The Palo Alto Networks Data Science team collects large numbers of documents for each category that serve as the foundation for classification. The labeled data is then split into train, test, and verify data sets. The training data set is used to learn the classification model, the testing data set was used to tune the model, and the verification data set was used to evaluate the model.

Preprocessing the labeled training data generates features and the feature text is tokenized into n-gram words for processing to remove stop words, special characters, punctuations, etc. The classifier converts the features using a vector space model and generates a high-dimension document-feature matrix that

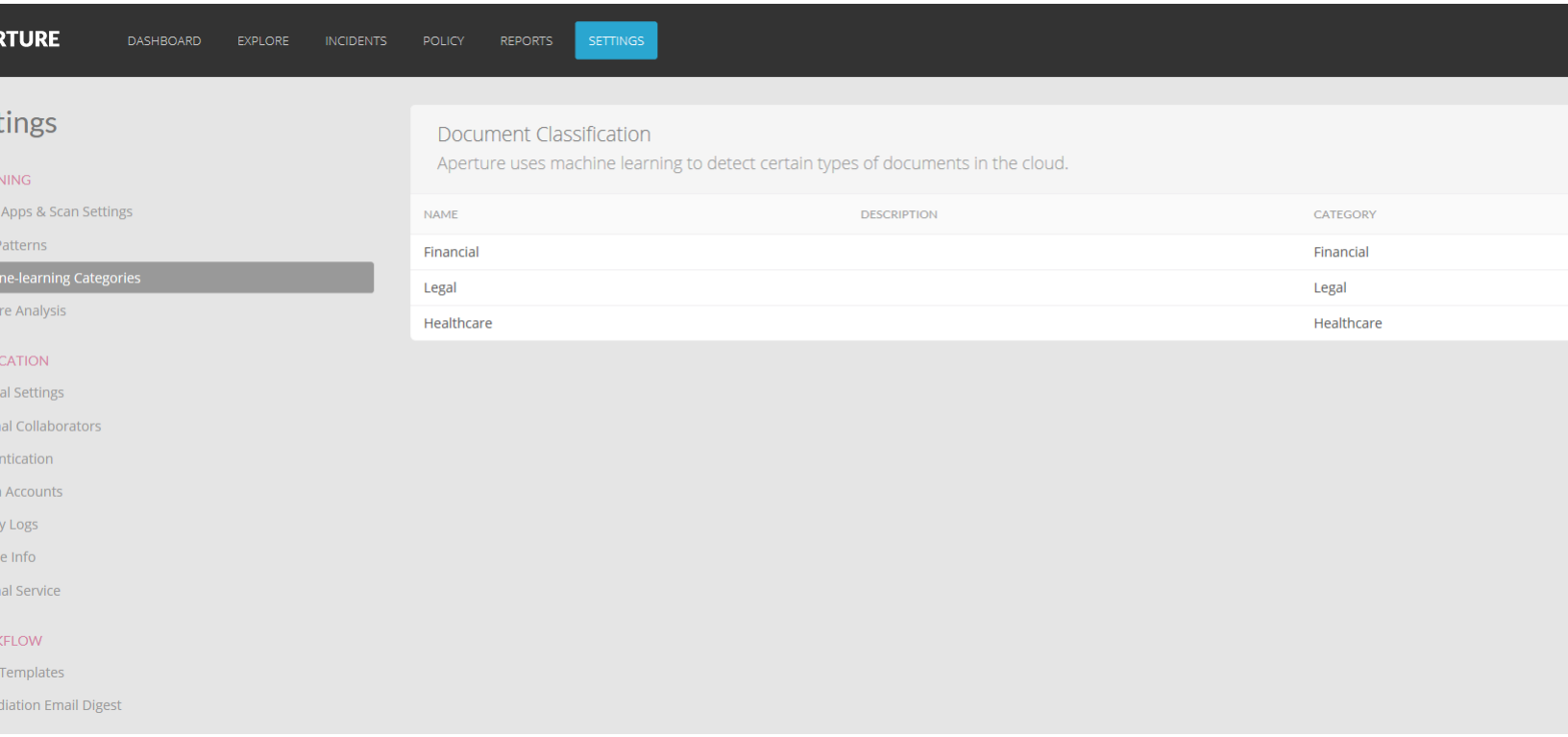
identifies significant features to reduce the matrix dimension. For each significant feature, Prisma SaaS computes a term frequency-inverse document frequency (TF-IDF) weight, and the weight is normalized to remove the effects due to different document lengths. At the end of the data preprocessing, labeled documents then transform into labeled feature vectors for feeding into supervised machine learning algorithms.

To improve detection rates for sensitive data in your organization, you can define the machine learning data pattern match criteria to identify these sensitive assets in your cloud apps and protect them from exposure. By default, the machine learning category is always enabled and is applied to all your cloud apps. To change this setting, you must be an administrator with a Super Admin role or an Admin with access to All Apps.

Enable or disable the machine learning data pattern.

By default, the machine learning data pattern is always enabled. If you have Super Admin account or an Admin account with access to All Apps, you can disable a machine learning data pattern in Settings.

1. Select **Settings** > **Machine-learning Categories**.
2. Enable the data pattern by clicking the on/off toggle.



3. **Save** your setting.

Configure a WildFire Analysis Data Pattern

The predefined data pattern service in Prisma SaaS uses WildFire analysis to detect known and unknown malware by file type. By default, Prisma SaaS automatically submits Windows executables, Microsoft Office files, and Portable Document Format (PDF) files to the WildFire service for analysis, classification and reporting as follows:

- WildFire reports the file information, including the hash, file, type, and size.
- WildFire static analysis leverages the machine learning capabilities of WildFire to display samples that contain characteristics of known malware.

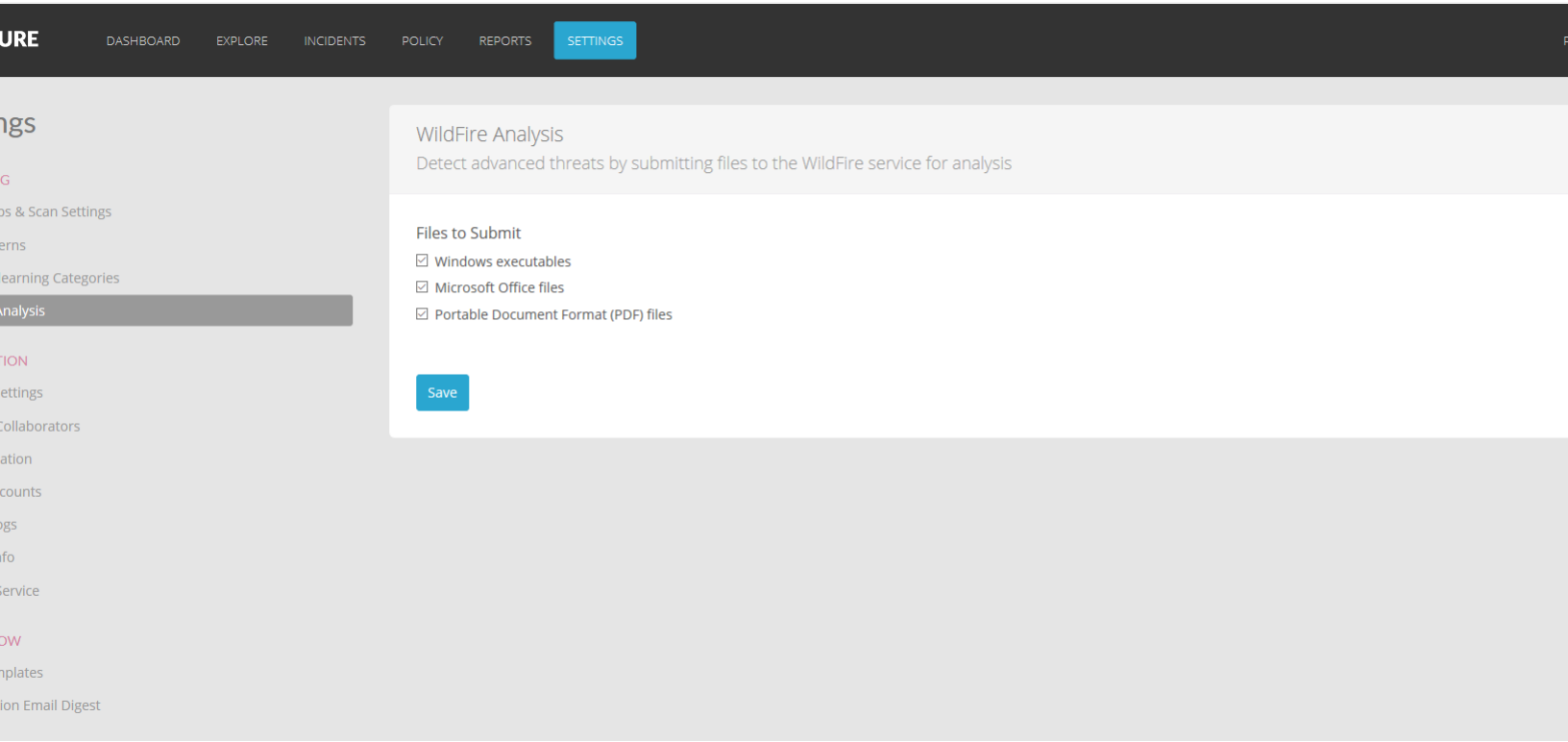
- WildFire Dynamic Analysis displays the details about the malicious host and network activity the file exhibited in the different WildFire sandbox environments.

You can configure the WildFire match criteria to select the cloud apps to scan and exposure settings in policy rules. For assets that match the WildFire analysis rule, you can Use the WildFire Report to Track Down Threats.

Enable or disable the WildFire analysis data pattern.

By default, the WildFire analysis data pattern is always enabled. You can disable a WildFire analysis data pattern in Settings.

1. Select **Settings** > **WildFire Analysis**.
2. Enable the data pattern by clicking the on/off toggle.
3. Select the **Files to Submit**, such as **Windows executables**, **Microsoft Office files**, and **Portable Document Format (PDF) files**.
4. **Save** your setting.



Configure Regular Expressions

The regular expression builder in Prisma SaaS provides an easy mechanism to configure regular expressions (regex for short), which you define when you create a custom data pattern. You can use the regular expression builder to construct a data pattern expression, view matches, filter occurrences and weight thresholds, and assess match results to determine if the content poses a risk to your organization.

There are two types of regular expressions:

- **basic expression** —searches for a specific text pattern. When a pattern match is found, the service displays the match occurrences.
- **weighted expression** —assigns a score to a text entry. When the score threshold is exceeded, such as enough expressions from a pattern match an asset, the service returns a match for the pattern.

To reduce false-positives and maximize the search performance of your regular expressions, you can assign scores using the weighted regular expression builder in Prisma SaaS to find and calculate scores for the information that is important to you. Scoring applies a match threshold, and when a threshold is exceeded, such as enough words from a pattern are found in a document, the document will be indicated as a match for the pattern.

Use Case: calculating a weighted regular expression

For example, Joe is an employee at a water treatment plant and needs to compile use data on a proprietary pH additive that is used when source water arrives at the plant. If Joe initiated a regular expression search with just the term "tap water" thousands of match results display, as the matched tap water documents list the additive, but Joe is really searching for the first use of the additive, not every document the additive is listed in, making it difficult for Joe to find the usage data he needs.

To get more accurate results, Joe can initiate a weighted regular expression to assign weight and occurrence scores to the expression, or indicate the information to exclude by assigning a negative weight value.

Joe enters a negative weight value to exclude tap water and higher values to source water and the proprietary water additive. The results are filtered and counted to a more manageable list, meaning that a document containing 10 occurrences of water counts as one when all files and folders are scanned. This enables Joe to view the match results, adjust the totals for weight and occurrences, and calculate an adjusted score to determine if the content poses a risk to his organization.

Example weighted regular expression scoring:

Weighted Regex Item	Occurrence	Adjusted Occurrence Score	Adjusted Total
Water; 1	50	50 (1 Occurrence X 1)	110 minus 100 for tap water = 10 regex weight
IP pH; 2	30	60 (30 occurrences X 2)	
Tap Water; -10	100	-100 (10 occurrences x -10)	

STEP 1 | Consider the best practices for using regular expression matches.

- **Use predefined data patterns instead of regular expressions**. Use Prisma SaaS predefined data patterns instead of regular expressions where possible. Data patterns are more efficient than regular expressions because the predefined data patterns are tuned for accuracy and the data is validated. For example, if you want to search for social security numbers, use the US Social Security Number (SSN) data pattern instead of a regular expression.
- **Use regular expressions sparingly**. Regular expressions can be computationally expensive. If you add a regular expression condition, observe the system for one hour for efficient performance. Make sure that the system does not slow down and there are no false positives.
- **Test regular expressions**. If you implement regular expression matching, consider using a third-party tool to test the regular expressions before you enable the policy rules. The recommended tool is RegexBuddy. Another good tool for testing your regular expressions is RegExr. If your expression is incorrect, the service cannot match or will match incorrectly.

STEP 2 | Understand expression terminology.

Expression Terminology:

Term	Description
Literal	A literal is any character you use in a search or matching expression, for example, to find dlp in Prisma SaaS, "dlp" is a literal string - each character plays a part in the search, it is literally the string we want to find.
Metacharacter	A metacharacter is one or more special characters that have a unique meaning and are NOT used as literals in the search expression, for example, the character < > (caret) is a metacharacter.
Regular Expression	This term describes the search expression data pattern that you will be using to search in Prisma SaaS.
Escape Sequence	An escape sequence is a way of indicating that you want to use one of the metacharacters as a literal. In a regular expression an escape sequence involves placing the metacharacter \ (backslash) in front of the metacharacter that you use as a literal, for example, if you want to find (dlp) in Prisma SaaS then use the search expression \(dlp \), and if you want to find \\file in the target string c:\\file then you would need to use the search expression \\\\file (each \ to search for a literal (there are 2) that is preceded by an escape sequence \).

STEP 3 | Understand expression constructs.

Prisma SaaS implements the Java regular syntax for policy condition matching. Prisma SaaS provides some common reference constructs for writing regular expressions to match or exclude characters in content.

Regular expression constructs:

Construct	Description
.	A dot, any single character, except newline (line ending, end of line, or line break) characters.
\	Escape the next character (the character becomes a normal/literal character.)
\d	Any digit (0-9.)
\s	Any white space.
\W	Any word character (a-z, A-Z, 0-9.)
\D	Anything other than a digit.
\S	Anything other than a white space.

Construct	Description
[ ]	Elements inside brackets are a character class (for example, [abc] matches 1 character [a. b. or c.]
^	At the beginning of a character class, negates it (for example, [^abc] matches anything except (a, b, or c.)
$	At the end of a character class, or before newline at the end.
+	Following a regular expression means 1 or more (for example, \d+ means 1 more digit.)
?	Following a regular expression means 0 or 1 (for example, \d? means 1 or no digit.)
*	Following a regular expression means any number (for example \d* means 0, 1, or more digits.)
(?i)	At the beginning of a regular expression makes it case-insensitive (regular expressions are case-sensitive by default.)
( )	Groups regular expressions together.
(?u)	Makes a period (.) match to even newline characters.
|	Means OR (for example, A|B means regular expression A or regular expression B.)

STEP 4 | Understand expression qualifiers.

Quantifiers can be used to specify the number or length that part of a pattern should match or repeat. A quantifier will bind to the expression group to its immediate left.

Regular expression quantifiers:

Quantifier	Description
*	Match 0 or more times.
+	Match 1 or more times.
?	Match 1 or 0 times.
{n}	Match exactly n times.
{n, }	Match at least n times.
{n, m}	Match at least n but not more than m times.

STEP 5 | Enter one regular expression per line, up to 100 lines of expressions.

STEP 6 | (Weighted expressions only): Assign a regular expression for each line entry between **-9999** (lowest importance) to **9999** (highest importance) by entering the regular expression, the delimiter, and the weight score. You must enter a weight threshold score of one (1) of more.

STEP 7 | (Optional) Customize your delimiter.

By default, the delimiter for all weighted regular expressions is semicolon (;). You can customize your delimiter to copy and paste existing expressions instead of entering them manually. A delimiter is used to specify separate strings of data when configuring regular expressions. For example, you can configure a weighted regular expression using a delimiter to separate the string of text you are matching from the weight threshold value. If you have large amounts of existing expressions to match, you can customize your delimiter to copy and paste the expressions instead of entering them manually. A delimiter can be any non-alphanumeric, non-backslash, non-whitespace character.

Regular expression delimiters:

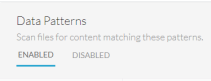
Delimiter	Note
;	Semicolon — If the delimiter is not customized, the semicolon is the default delimiter in Prisma SaaS.
:	Colon.
|	Pipe.
/	Forward Slash — If the delimiter needs to be matched inside the pattern it must be escaped using a backslash (\ ). If the delimiter appears often inside the pattern, it is a good idea to choose another delimiter to increase readability.
+	Plus — Include phrase for matching.
-	Minus — Ignore phrase for matching.
#	Hash — Can be used to denote a number.
~	Tilde
{ } Curly	Brackets are used to find a range of characters. Bracket style delimiters do not need to be escaped when they are used as meta characters within the pattern, but they must be escaped when they are used as literal characters.
[ ] Square	
( ) Parenthesis	
< > Caret	

Enable or Disable a Data Pattern (Basic DLP)

By default, the data pattern is enabled when you save it. Any disabled data pattern can be enabled. If you do not see the enable or disable links, you do not have the privilege necessary to modify the data pattern.

STEP 1 | Select **Settings** > **Data Pattern**.

STEP 2 | Filter the data pattern list to view the **Enabled** or **Disabled** data patterns.



STEP 3 | Select the data pattern to edit, and either **Enable** or **Disable** the data pattern.

For enabled data patterns, Prisma SaaS will immediately begin scanning and display the match results in **Explore** > **Assets**. To scan a disabled data pattern, you must enable it.

View and Filter Data Pattern Match Results (Basic DLP)

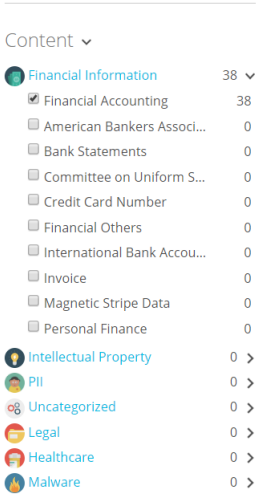
When you Configure Data Patterns, you define the criteria that the policy rule uses when Prisma SaaS scans for matches. The service compares all the information it discovers against the enabled data pattern and identifies match occurrences. From the match results, you can focus on a match to filter and determine if the number of occurrences meets an incident threshold.

Filter data pattern match results with occurrence match counting.

WildFire and machine learning data patterns do not have occurrences to specify in Match Criteria.

1. Select **Explore** > **Assets** > **Content** to configure occurrence match counting to view pattern match results and adjust the threshold.
2. Select the content **Category** to view.
3. Enter the numerical value in **Occurrences** in the selected category, and click **Enter** to view the filtered results.

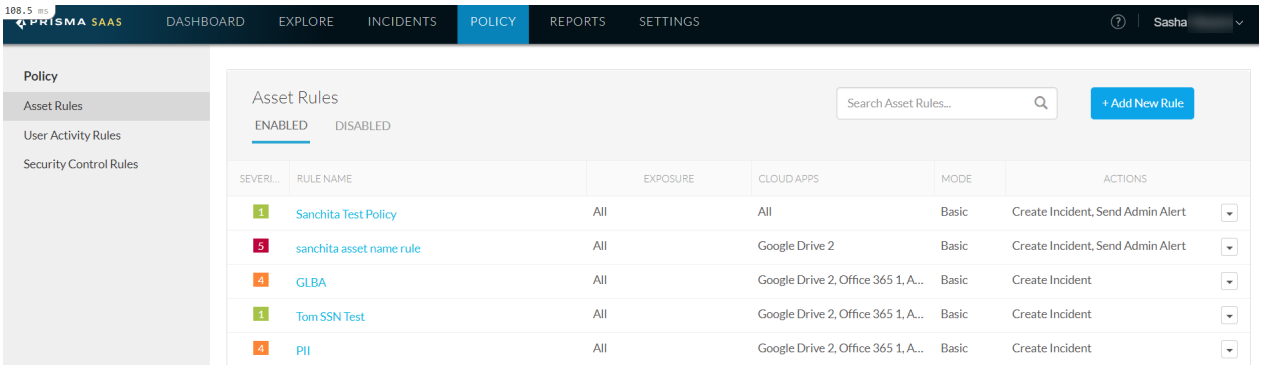
For basic data patterns, you can Assess Incidents and remediate the occurrences. For weighted data patterns, you can calculate the unique occurrence against the weight threshold to determine a score. See Configure Regular Expressions.



Configure Prisma SaaS Asset Rules

In addition to the predefined data patterns and asset rules already configured on Prisma SaaS, you can add your own asset rules for ever greater comprehensive coverage. For example, you can create a rule that creates an incident and when an a file is shared internally. Asset rules have a large set of match criteria options that allow you to precisely define how Prisma SaaS should monitor your sanctioned SaaS applications.

- Add a New Asset Rule
- Building Blocks in Asset Rules
- Match Criteria for Asset Rules (Basic DLP)
- View Asset Details



Add a New Asset Rule

To add a new rule for scanning assets (content) stored on your sanctioned SaaS applications:

STEP 1 | Select **Policy** > **Asset Rules** > **Add New Rule**.

STEP 2 | Enter a **Rule Name** and an optional **Description**.

STEP 3 | Select a **Severity** for the rule.

STEP 4 | Verify that the **Status** is **Enabled**.

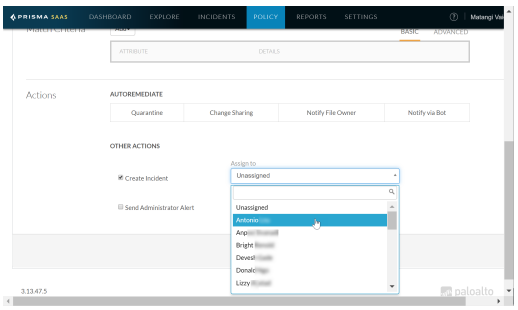
STEP 5 | Specify the Match Criteria for Asset Rules (Basic DLP).

Review information in Building Blocks in Asset Rules.

Sensitive documents are identified as a policy rule violation only if the exposure level is violated. For example, you can configure a policy rule to trigger a an alert for a sensitive document that has a Public or External exposure. To specify the exposure level for which to flag a sensitive document as an incident:

STEP 6 | Select an **Action** for the new asset rule.

Automatic remediation is a powerful tool and can modify a large number of assets in a short amount of time. Make sure you perform a test run first (using one policy rule and a small set of assets) before including these actions on additional policy rules.



1. For most policy rules, verify that **Actions** setting is **Create Incident**. By default a new incident is not assigned to an administrator. If you have Connect Prisma SaaS to Directory Services (Beta), you have the option to **Assign to** a specific administrator who has context to triage the incident and address

the potential risk. Then, after you uncover specific issues that are high-compliance risks on your network, you can modify the rule or add a new rule that triggers Automatic Remediation:

Quarantine—Automatically moves the compromised asset to a quarantine folder.

Change Sharing—Automatically removes links that allow the asset to be publicly-accessed.

Notify File Owner—Sends an email digest to the asset owner that describes actions they can take to fix the issue.

Notify via Bot—(Only for Cisco Webex Teams) Uses a machine account that you created to send a direct message to the asset owner who triggered the policy match.

2. Select **Send Administrator Alert** only for compliance issues for which you need to take immediate action, such as policy rules that are high-risk or sensitive. Prisma SaaS can send up to five emails per hour on matches against each Cloud App instance.

Enable email alerts only after Prisma SaaS completes the initial discovery scan so that you are not inundated with emails when historical assets are scanned.

STEP 7 | Save your new policy rule.

Save your changes.

Prisma SaaS starts scanning files against the policy rule as soon as you save the changes. After the scan starts, you can start to Assess New Incidents and Fine-Tune Policy.

Building Blocks in Asset Rules

An asset (or content) rule has the following information:

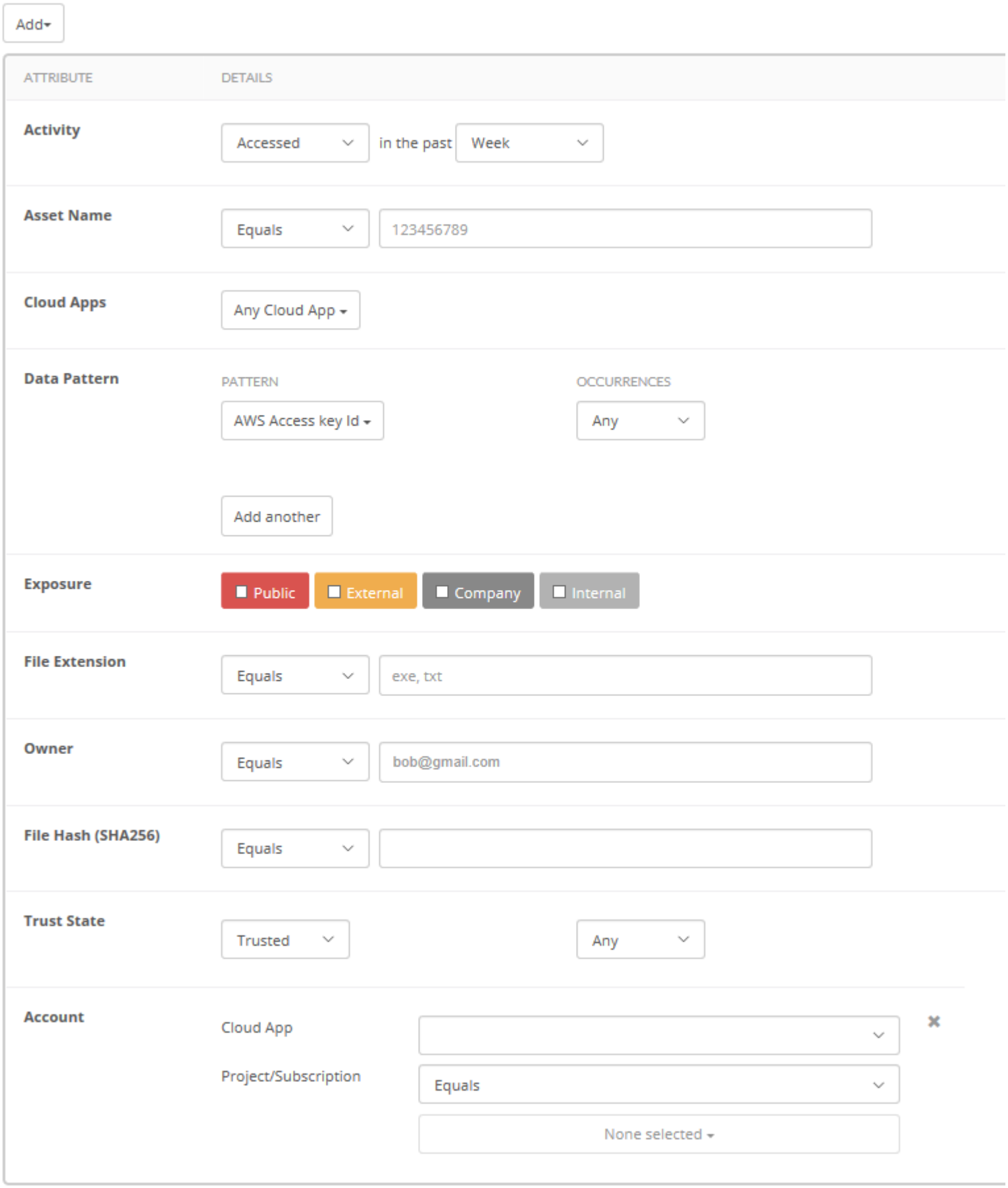
Field	Description
Rule Name	A name for the policy rule.
Description	A description that explains the purpose of the rule.
Severity	Specify a value to indicate the impact of the issue. The value can range from 1 to 5, with 5 representing the highest severity.
Status	A rule can be in the enabled or disabled state. The predefined data patterns provided by Prisma SaaS are automatically enabled. After you Configure Data Patterns, you must enable the pattern.
Match Criteria	Specifies what the rule scans for and the number of occurrences or frequency required to trigger an alert. See Match Criteria for Asset Rules (Basic DLP) for details about each rule type. When you change the match criteria settings, you automatically trigger a rescan of all assets for the corresponding SaaS application. Prisma SaaS uses the updated settings in the policy rule configuration to rescan assets and identify incidents.

Field	Description
Actions	Allows you to specify whether Prisma SaaS should trigger one of the following actions to carry out Automatic Remediation or if it should simply log the event as a incident. • **Quarantine**—Automatically moves the compromised asset to a quarantine folder. For **User Quarantine**, you can send the asset to a quarantine folder in the owner's root directory for the associated cloud app. For **Admin Quarantine**, you can send the asset to a special Admin quarantine folder which only an Admin can access. When the asset is quarantined, you can send the asset owner an email that describes the actions that were taken. • **Change Sharing**—Automatically removes links that allow the asset to be publicly-accessed. For **Direct Links** you can remove the direct link on the asset only. For **Public Links on Parent Folders** you can also remove links that expose the asset due to inheritance from the parent folders. • **Notify File Owner** —Sends an email digest to the asset owner that describes actions they can take to fix the issue. • **Notify via Bot**— Sends a message using the Cisco Webex bot that you configured in Begin Scanning a Cisco Webex Teams App (Beta). • **Apply Classification**—Automatically applies the classification and priority labels to the third party classification data pattern match criteria. • **Create Incident**—Automatically changes incident status to **Open** and the incident category to **New** so the administrator can Assess Incidents. • **Send Admin Alert**—Select send admin alert for compliance issues that need immediate action, such as policy rules that are high risk or sensitive. Sends an email digest to the asset administrator that describes actions they can take to fix the issue. View which autoremediate options are supported for each sanctioned SaaS application.

Match Criteria for Asset Rules (Basic DLP)

When you Add a New Asset Rule or you Modify an Asset Rule, you define the match criteria that the asset rule uses when Prisma SaaS scans for matches. The service compares all of the information it discovers against the enabled asset rules and identifies incidents and exposures in every asset across all your monitored SaaS applications. Match criteria is critical for successful discovery of risks in SaaS application usage across your organization so, when you set the match criteria, you must carefully consider the thresholds, types of information, and risks associated with how assets are shared. Use match criteria to enforce compliance with your corporate acceptable use policy.

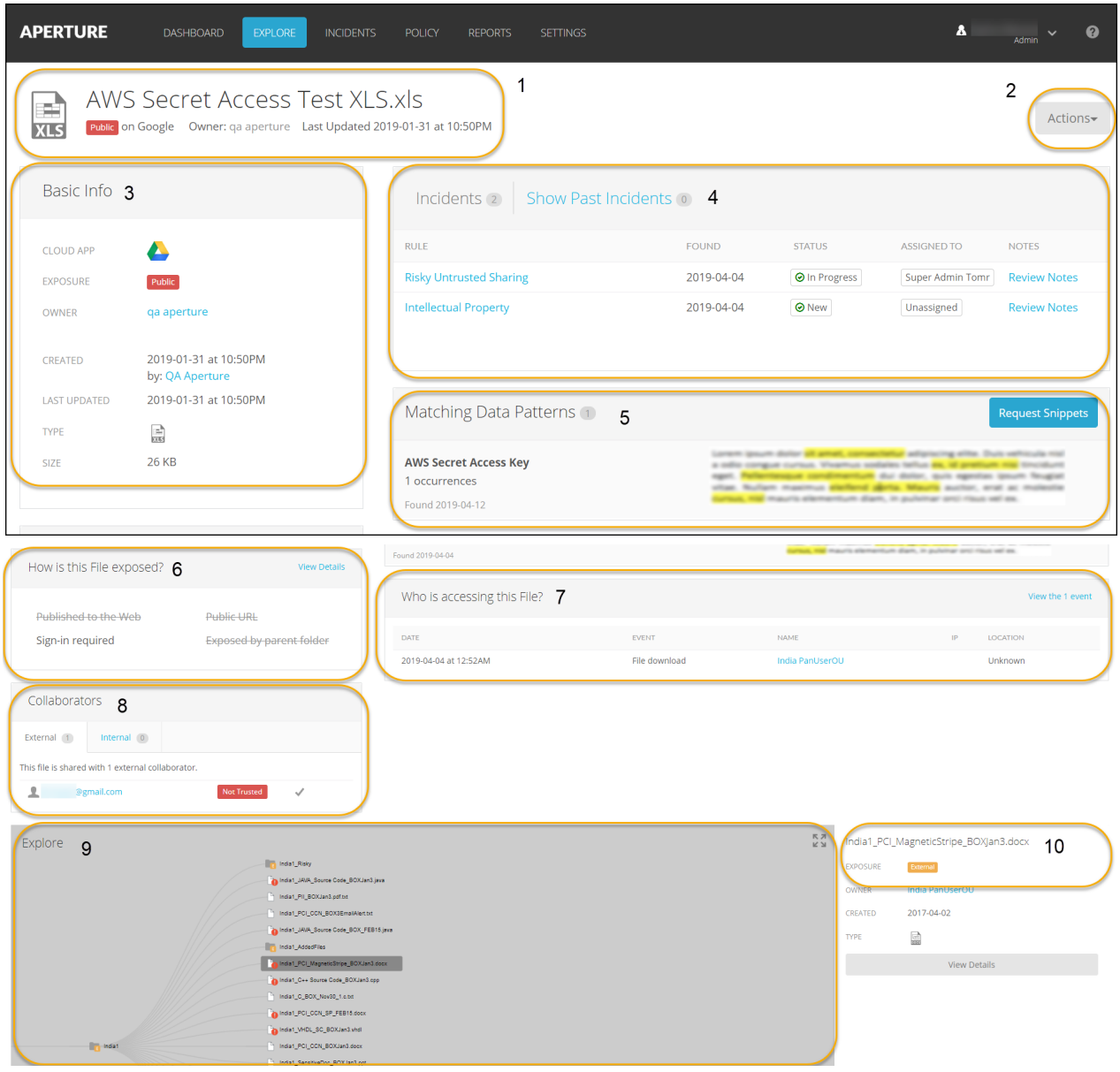
Match Criteria	Description
Activity	Select the asset access and modification activities within a selected time frame to match. For example, activities can include **Accessed**, **Not Accessed**, **Modified**, and **Not Modified**. Time frames include **in the past week**, **in the past month**, and **in the past 6 months**.
Asset Name	Enter the **Asset Name** to include or exclude in the match results. Select either **Equals** to match the asset, or **Does not Equal** to exclude the asset from matching.
Cloud Apps	Select the managed applications to scan and match. By default, all cloud apps you added to Prisma SaaS are scanned, but you can Rescan a Managed Cloud App.
Data Pattern	Select the available data patterns to match including predefined or custom data patterns or a file property you defined when you Create a Custom Data Pattern (Basic DLP). Enter the number of **Occurrences** required to display a data pattern match.
Exposure	Select the match conditions for how the asset is shared (Public, External, Company, or Internal). The ideal exposure level that you specify depends on the asset you're want to protect.
File Extension	Enter the **File Extension** to include or exclude in the match results. Select either **Equals** to match the asset file extension, or **Does not Equal** to exclude the asset file extension from matching.
File Owner's Group	To enforce group-based policy using **File Owner's Group**, you must Connect Prisma SaaS to Directory Services (Beta). Select either **Equals**, or **Does not Equal** and the Azure Active Directory Group to which the file owner must belong. You can also select **Not Available** if you want to enforce an action for any users who are not identified either because the email address is unavailable or because they belong to an AD group that is not being scanned by Prisma SaaS.
Owner	Enter the email address for the asset **Owner** to **Include** or **Exclude** in the match results. You can add one or more Directory groups
File Hash	Files are scanned using WildFire analysis to detect and protect against malicious portable executables (PEs) and known threats based on file hash. Enter the **Hash** (SHA256) details of the file to match. Select **Equals** (include in matching), or **Does not Equal** (exclude in matching).
Trust State	When you Define Untrusted Users and Domains or if you are matching on an assets trust state, all assets shared with a user in the selected **Trusted**, **Untrusted**, or **Anyone Not Trusted** users list are detected as a match. Specify the number of occurrences (such as **Any**, **More than**, **Fewer than**, or **Between** with whom a file must be shared to trigger a match.
Account	Select the **Cloud App** and the **Project/Subscription** in the storage **Account** to include in the match results.



View Asset Details

As Prisma SaaS scans your managed cloud apps and discovers content, you can view the details on **Explore** > **Assets**. This page provides context into the findings so you can Assess Incidents across these applications. The details for each incident vary depending on the associated cloud app, whether the asset is a file or a container (for example, a folder or a repository), the policy rule violated, and how the asset is shared.

Asset Detail Description



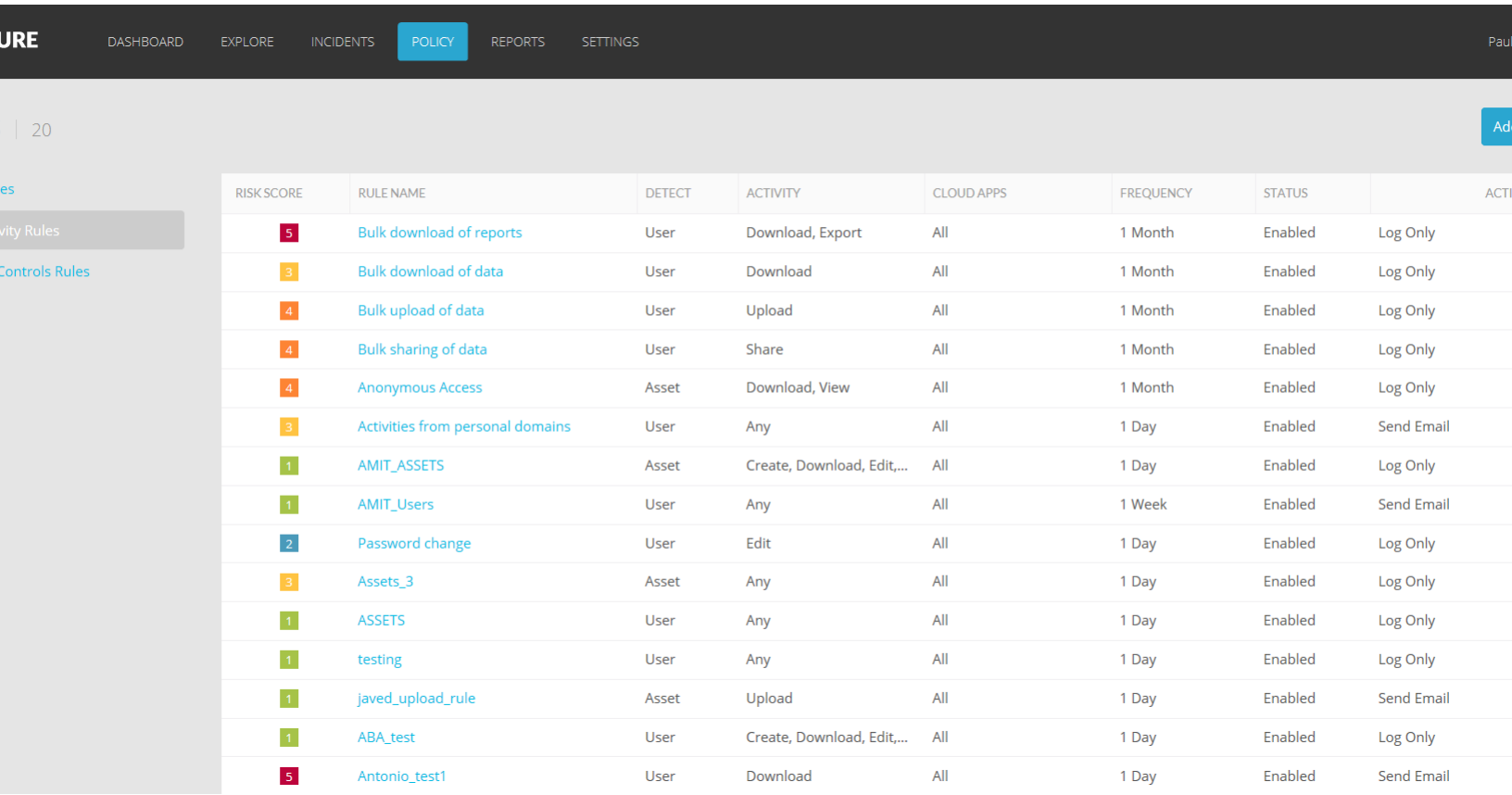
1	Asset Summary	Summarizes asset file name, file type, exposure on cloud app, owner, and last updated timestamp.

Asset Detail		Description
2	Actions	Lists available actions for an asset, such as Apply Classification or Quarantine, depending on the cloud app and admin role permissions.
3	Basic Info	Displays metadata about the asset including cloud app, data attachment, exposure, owner, creation date, file type, and size.
4	Incidents	Displays which policy rule or rules that an asset violates, the date Prisma SaaS identified the incident, the status of the incident, and whether there have been previous incidents associated with the asset.
5	Matching Data Patterns	Displays the data pattern that the asset matched, number of occurrences, and date found. Admins with a Super Admin or Admin role may **Request Snippets** to view any available details about the asset matching the data pattern. For assets that match the WildFire Analysis rule, you can Use the WildFire Report to Track Down Threats.
6	How is this File exposed?	Details how the asset is exposed (Published to the web, accessible by a public URL, if sign-in is required, or the asset is exposed by a parent folder). You can **View Details** to access the asset URL, if available.
7	Who is accessing this File?	Lists the timestamp, type of access (for example, whether the user downloaded the file), user name, IP address, and location of the user. You can **View the event** details to investigate whether there is malicious or inappropriate access to the file.
8	Collaborators	Lists **Internal** and **External** collaborators for the asset. This section appears only if the asset has an **External** exposure level. Additionally, if the collaboration settings are defined at the asset level, you can change the trust settings and remove collaborators. If the asset inherits a collaborator from a parent folder, you must change these settings from the parent folder.
9	Explore	Displays the asset in context of the hierarchy (one level above and one level below) to help you investigate the scope and source of the risky behavior and identify indirect or inherited exposures. In this view, a red exclamation point denotes any asset with associated risks. Select an object in the hierarchy (either a folder, repository, or individual file) to display information about that object, including the creation date, file type, exposure, owner, and policy violation (if applicable).
10	Exposure Level	Displays the exposure level of the asset (Internal, External, Company, or Public).

Configure Prisma SaaS User Activity Rules

In addition to data patterns, you can add user activity rules for comprehensive coverage. Similar to asset rules, user activity rules include a robust set of match criteria that allow you to precisely define which user activities are threats to your organization.

- Add a New User Activity Rule
- Match Criteria for User Activity Rules
- Examples of User Activity Rules
- View Policy Violations for User Activity



RISK SCORE	RULE NAME	DETECT	ACTIVITY	CLOUD APPS	FREQUENCY	STATUS	ACTI
5	Bulk download of reports	User	Download, Export	All	1 Month	Enabled	Log Only
3	Bulk download of data	User	Download	All	1 Month	Enabled	Log Only
4	Bulk upload of data	User	Upload	All	1 Month	Enabled	Log Only
4	Bulk sharing of data	User	Share	All	1 Month	Enabled	Log Only
4	Anonymous Access	Asset	Download, View	All	1 Month	Enabled	Log Only
3	Activities from personal domains	User	Any	All	1 Day	Enabled	Send Email
1	AMIT_ASSETS	Asset	Create, Download, Edit,...	All	1 Day	Enabled	Log Only
1	AMIT_Users	User	Any	All	1 Week	Enabled	Send Email
2	Password change	User	Edit	All	1 Day	Enabled	Log Only
3	Assets_3	Asset	Any	All	1 Day	Enabled	Log Only
1	ASSETS	User	Any	All	1 Day	Enabled	Log Only
1	testing	User	Any	All	1 Day	Enabled	Log Only
1	javed_upload_rule	Asset	Upload	All	1 Day	Enabled	Send Email
1	ABA_test	User	Create, Download, Edit,...	All	1 Day	Enabled	Log Only
5	Antonio_test1	User	Download	All	1 Day	Enabled	Send Email

Add a New User Activity Rule

User activity rules enable you to track user activities that compromise your organization. For example, you can create a rule that sends an email alert or creates a log entry when a user downloads a large number of reports, or when a user tries to access an SaaS application from a malicious IP address. For additional examples, refer to Examples of User Activity Rules.

STEP 1 | Add a new rule.

1. Select **Policy** > **User Activity Rules** > **New Rule**.

STEP 2 | Define the basic settings.

1. Enter a **Name** for the rule.
2. (Optional) Enter a **Description** for the rule.
3. Specify a **Severity** for the rule ranging from 1 to 5, with 5 representing the highest risk type of incident.

STEP 3 | Specify the **Items to Detect**.

1. Select one of the following:
   - **Users**—Applies the policy rule to users.
   - **Assets (such as files or folders)**—Applies the policy rule to assets.
2. (Optional) **Manage Exceptions** for the rule. Enter the users or assets you want to exclude from the rule. For example, you might want to exclude Prisma SaaS administrators from user activity monitoring.

STEP 4 | Specify the match criteria for the activity.

See Match Criteria for User Activity Rules.

STEP 5 | Verify that an action is enabled.

Choices include:

- **Log Only** (default)—Log the policy violation.
- **Send admin alert**—For policy violations that require immediate action, send an email alert. Prisma SaaS can send up to five emails per hour on matches against each policy rule.

STEP 6 | Verify that the policy rule is enabled.

In **Basics**, verify that the **Status** is **Enabled**. A rule can be in the enabled or disabled state. After you add a new rule, you must enable the rule.

STEP 7 | Save your new policy rule.

Save your changes.

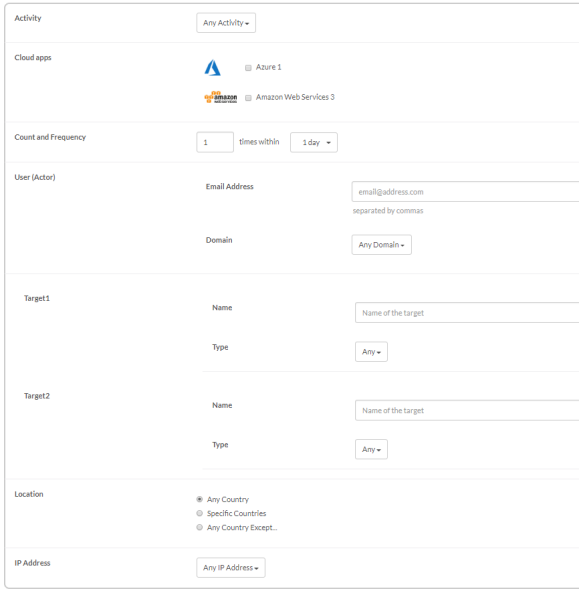
Prisma SaaS starts scanning files against the policy rule as soon as you save the changes. After the scan starts, you can start View Policy Violations for User Activity.

Match Criteria for User Activity Rules

The following table lists the match criteria for user activity rules.

Match Criteria	Description
Activity	List of activities to monitor. For example, activities can include **Create**, **Edit**, **Delete**, **Authorize**, **Upload**, **Join**, or more. You can include multiple activities in a rule.
Cloud Apps	List of accessible applications to scan. By default, all cloud apps you added to Prisma SaaS are scanned, but you can restrict scans to specific apps.
Count and Frequency	The count and frequency of the activity that will trigger a policy violation. For example, ten (or more) times a week, or two (or more) times per day.
User (Actor)	Users whose perform the activities. By default, all users in all domains are included. Alternatively, you can: • **Email Address**— Include an email addresses for each user to monitor. Use commas to separate each address in the list. • **Domain**—Include (or exclude) a subset of users based on domains. Use commas to separate each domain in the list.

Match Criteria	Description
Target	The **Name** and **Type** of target for the user activity. For example, a target could be any user activity that impacts a **Super Admin** (target name) **Password** (target type). Or, any user activity associated with a **Client List** (target name) **Report** (target type). You can **Add a Target** to include multiple targets in a policy rule. For example, activities that add **Users** (target) to **Teams** (target), or activities that share **Links** (target) with **Users** (target) would include two targets in the rule.
Location	The location where the activity occurs. Choices include: • **Any Country** (default)—Activities in all countries. • **Specific Countries**—Activities in specific countries. You can select multiple countries from the list. • **Any Country Except**—Activities in all countries, except the ones you select.
IP Address	The IP address where the activity was initiated. Choices include: • **Any IP Address**—Activities initiated from any IP address. • **Specific IP Addresses**—Activities initiated from specific IP addresses. • **Any IP Address Except**—Activities initiated from all IP addresses, except the ones you specify. Use commas to separate multiple IP addresses.



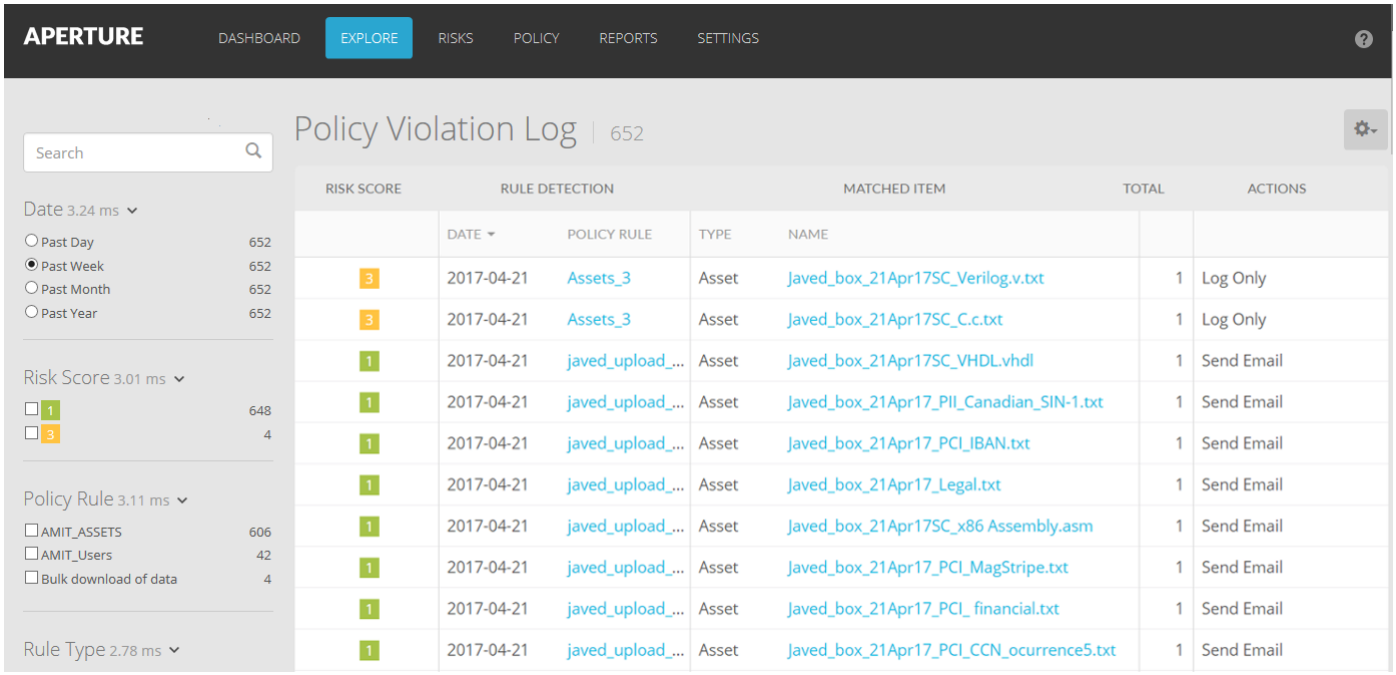
Examples of User Activity Rules

The following are some examples of how to configure user activity rules.

Objective	Criteria	Value
Send an alert if any user downloads more than 500 files in a day.	Activity Count/Frequency Target Type Action	Download 500, 1 day File Send Admin Alert
Send an alert for failed logins on Salesforce.	Activity Cloud Apps Action	Failed Login Salesforce Send Admin Alert
Log any activity from a malicious IP address.	Activity IP Address Action	Any Activity 127.31.52.12 Log only
Send an alert if a user outside of paloaltonetworks.com uploads an executable file.	Activity Domain Target Name Target Type Action	Upload Any Domain Except paloaltonetworks.com *.exe File Send Admin Alert
Log an activity when users change their passwords.	Activity Target Type Action	Edit Password Log only

View Policy Violations for User Activity

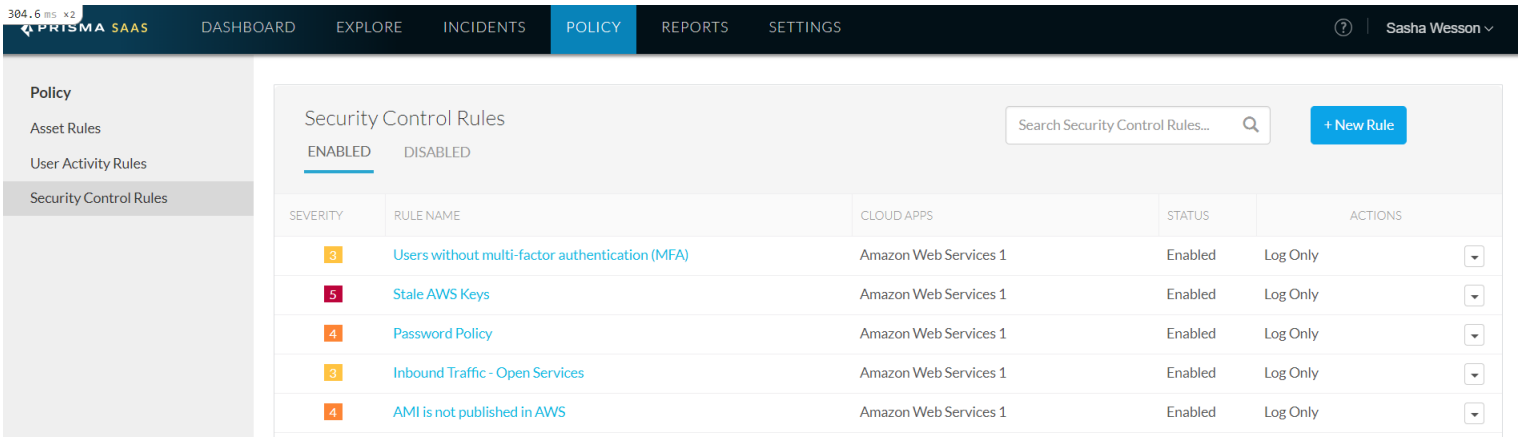
Prisma SaaS starts scanning files and matching them against enabled policy rules as soon as you save a new rule or modify an existing rule. The default action is to generate a log when a policy violation occurs but if you enabled email alerts for high-risk issues, you will also receive an automatic email notification. To view policy violations for user activities, select **Explore** > **Policy Violations**.



Configure Prisma SaaS Security Control Rules

Prisma SaaS Security Control Rules allow you to define and enforce policy rules for monitoring settings and activities so you can automatically detect and remediate risks around data exfiltration, exposure, or risky user behavior. For example, you can create a policy that sends an email alert or creates a log entry when a user forwards a corporate email to a personal email address or when a security key pair rotation does not follow defined policies. Security Control Rules include a robust set of match criteria that allow you to precisely define which settings and activities to track.

- Add a New Security Control Rule
- View Policy Violations for Security Controls



Prisma SaaS supports the following types of security controls:

Security Control Setting Type	Action
Administrative Access of End Users Inbox	Identifies administrators who have access to an end users inbox. The **Admin Email** lists the email address of the administrator and the **User**

Security Control Setting Type	Action
	Email lists the email address of the user whose inbox can be accessed by the administrator.
Email Forwarding Rule	Identifies Corporate emails that are forwarded to personal email domains. **Rule Name** identifies the email forwarded and the email address is listed in **Forwarded Email Address**.
Email Public Folder	Identifies exposed public folders that users can access within the Enterprise, and **Folder Name** and **Folder Owner** to exclude.
Email Retention	Identifies user-generated email retention settings that vary from the Corporate Administrator policy settings.
Inbound Accessible Services	Identifies Inbound Security Groups that have access to specific services and ports that are scanned in AWS.
Key Rotation	Sends an alert for keys that have not been rotated within a specific time frame such as one week, one month, three months, or one year.
Multi-Factor Authentication	Identifies users and sends an alert when they log in to the SaaS application without multi-factor authentication.
Non-Standard Amazon Web Services EC2 Appliance (AMI)	Identifies AMIs that are not trusted by the organization and sends an alert on non-standard AMIs.
Outbound Accessible Services	Identifies Outbound Security Groups that have access to specific services and ports that are scanned in Amazon Web Services.
Password Policy	Checks the password (such as complexity, reuse, or expiration) against the password policy and sends an alert when there is a discrepancy.
Unencrypted Storage	Identifies and alerts on Elastic Block Storage (EBS) storage volumes that are not encrypted.

Add a New Security Control Rule

To add a new security control rule:

STEP 1 | Add a new rule.

1. Select **Policy** > **Security Control Rules** > **New Rule**.

STEP 2 | Define the basic settings.

1. Enter a **Name** for the rule.
2. (Optional) Enter a **Description** for the rule.
3. Specify the **Severity** for the rule. Severity ranges from 1 to 5, with 5 representing the highest risk.
4. Enable or disable the **Status**.
5. Select a **Setting Type**, **Cloud apps**, if applicable, and the **Setting Options**.

Setting Type	Setting Options
Administrative Access of End Users Inbox	Enter the **Admin Emails to Exclude**, and **End User Emails to Exclude**.
Email Forwarding Rule	List the **Risky Domain**, **Email Addresses of Users to Exclude**, and **Rule Names to Exclude**.
Email Public Folder	Enter the **Folder Names** and **Email Addresses of the Folder Owners to Exclude**.
Email Retention	Enter the **Email Addresses of the Users to Exclude**.
Inbound Accessible Services	Enter the **Source IP Address**, **Service to Exclude**, **Security Groups to Exclude**, **VPCs to Exclude** and **ELBs to Exclude**.
Key Rotation	Select a time frame in **Keys not rotated within**, list the **Keys to Exclude from Key Rotation Check**, and **Roles to Exclude from Key Rotation Check**.
Multi-Factor Authentication (MFA)	List the **Exclude MFA Check User**, and **Exclude MFA Check for User with Role**.
Non-Standard Amazon Web Services EC2 Appliance (AMI)	List the **Exclude AMIs**.
Outbound Accessible Services	List the **Destination IP Address**, **Service to Exclude**, **Security Groups to Exclude**, **Virtual Private Cloud (VPC) to Exclude** and **Elastic Load Balancing (ELB) to Exclude**.
Password Policy	Flag if password does not follow password policy rules.
Unencrypted Storage	List the **Exclude Volumes**, **Exclude Volumes attached to EC2**, and **Exclude Volumes in VPC**.
Actions	Allows you to specify whether Prisma SaaS should trigger one of the following actions to automatically remediate incidents or log the event as a risk. • **Send Admin Alert** • **Log Only**

Setting Options with **Exclude** are Optional.

6. **Save** your new security control rule.

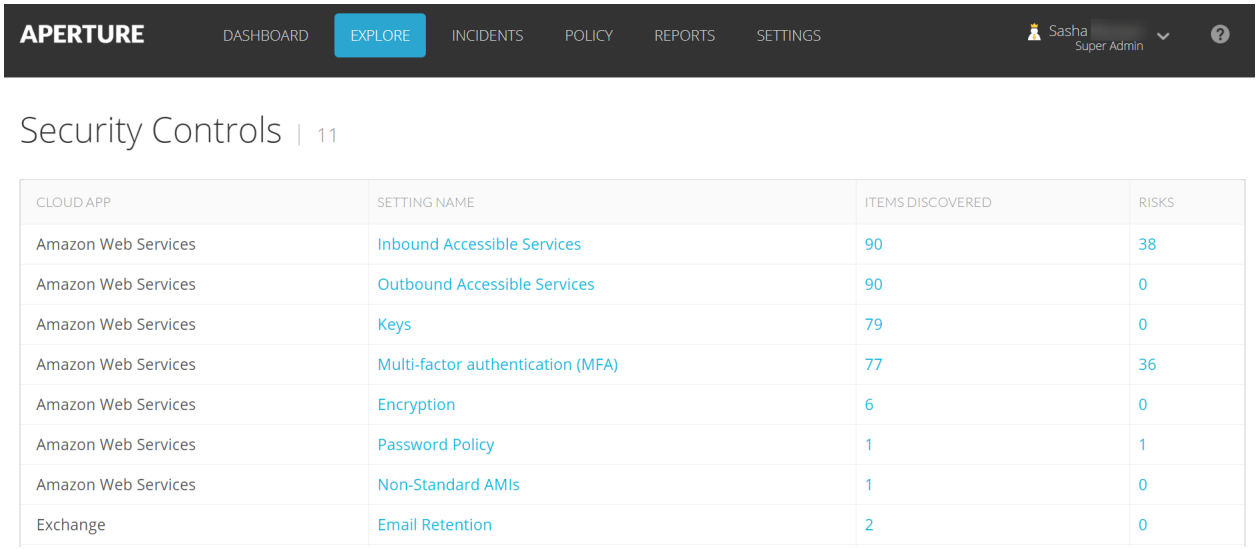
STEP 3 | Verify the Security Control rule is enabled.

After saving, the rule will be listed on the **Security Control Rules** under **Enabled** or **Disabled**. Prisma SaaS starts scanning files against the policy rule as soon as you save the changes. After the scan starts, you can start to View Policy Violations for Security Controls.

View Policy Violations for Security Controls

After connecting to a SaaS application such as Gmail, Microsoft Exchange, or AWS, Prisma SaaS begins scanning and matching activities and settings against enabled security control rules. The default action for a Security Control Rule is to generate a log for a discovered violation but you can configure Prisma SaaS to send administrator alert as an action instead.

To view policy violations for security controls, select **Explore** > **Security Controls** and investigate further by the reported violations under **Risks**.



Configure Third-Party App Settings

Prisma SaaS third-party app settings gives you the controls to monitor third-party apps added by end users to an application ecosystem. Prisma SaaS policy enables you to detect and remediate any non-compliant third-party apps to prevent data exfiltration or unauthorized access. For example, you can create a policy that blocks access to a third-party app from a malicious IP address that also automatically emails users who try to install the blocked app.

- Add a New Setting for Third-Party Apps
- Configure Classification Labels for Third-Party Apps
- View Information for Third-Party Apps

Add a New Setting for Third-Party Apps

To add a new setting for third-party apps:

STEP 1 | Add a new setting.

1. Select **Explore** > **Third-Party Apps** > **Settings & Policy**.

STEP 2 | Define the **Block by Default**settings.

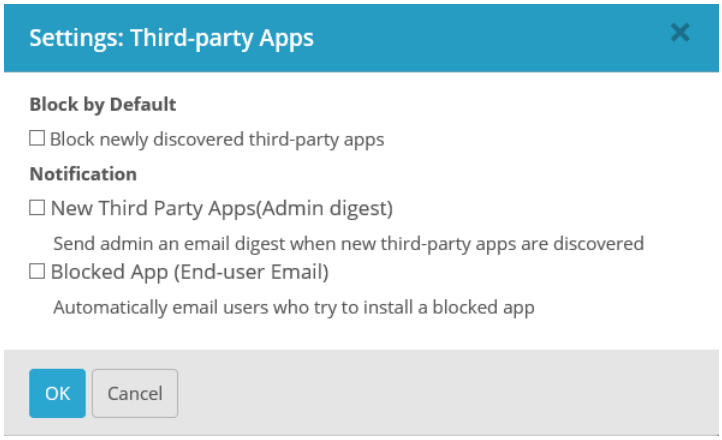
1. To automatically block third-party apps, select **Block by Default** and then **Block newly discovered third-party apps**.
2. Third-party apps are classified as either **Registered** or **Unregistered** to the app marketplace. Based on registration classification, select either **Block unregistered apps by default** or **Block all apps by default**.

STEP 3 | Define the **Notification** setting.

1. To send an email **Notification** to the admin when new apps are discovered, select **New Third Party Apps (Admin digest)**.

   Set the admin email digest **Frequency** to either **Daily** or **Weekly**. Enter the admin email address to receive the email digest in the **To** field.
2. To automatically email users who try to install a blocked app, select **Blocked App (End-user Email)**.

STEP 4 | Click **OK** to save your settings and Prisma SaaS starts scanning third-party apps against your new settings.



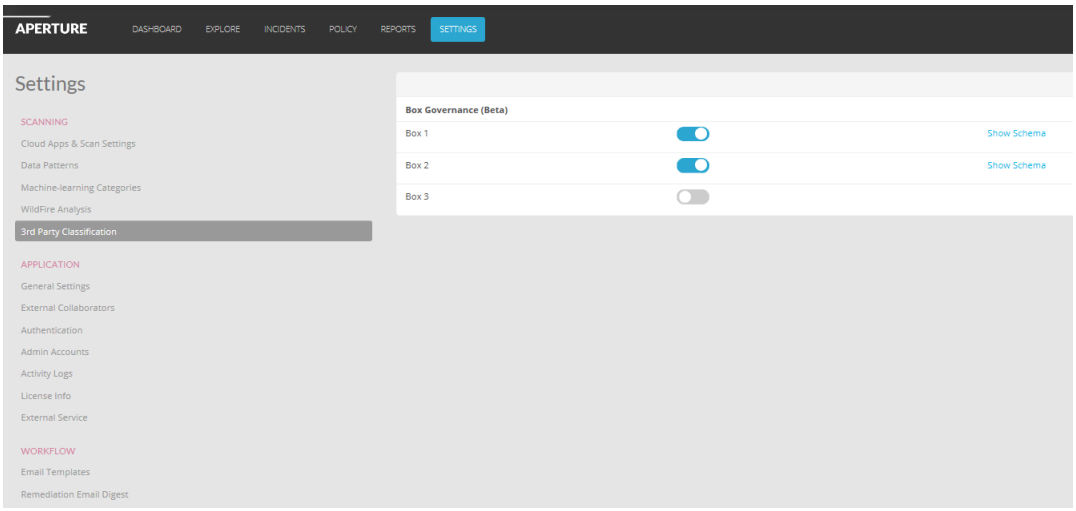
STEP 5 | When scanning is complete, you can View Information for Third-Party Apps.

Configure Classification Labels for Third-Party Apps

Prisma SaaS extends its governance and protection capabilities to automatically secure your sensitive third-party app content before it is shared through the data classification label service. To better secure your sensitive file content, you can configure the data classification labels for the files in your third-party apps to control data sharing, prevent data exfiltration, and any future violations.

STEP 1 | Enable the classification for third-party apps.

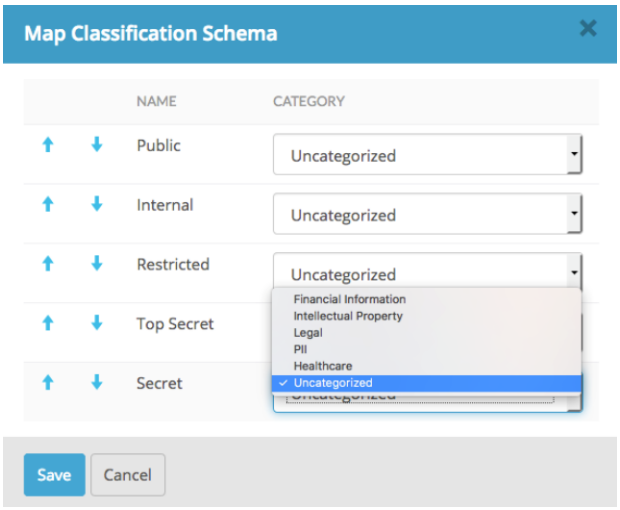
1. Select **Settings** > **Third Party Classification**.
2. Enable the classification setting.
3. **Save** your setting.



STEP 2 | (Optional) If third-party governance is enabled for the selected cloud app, configure the **Map Classification Schema**.

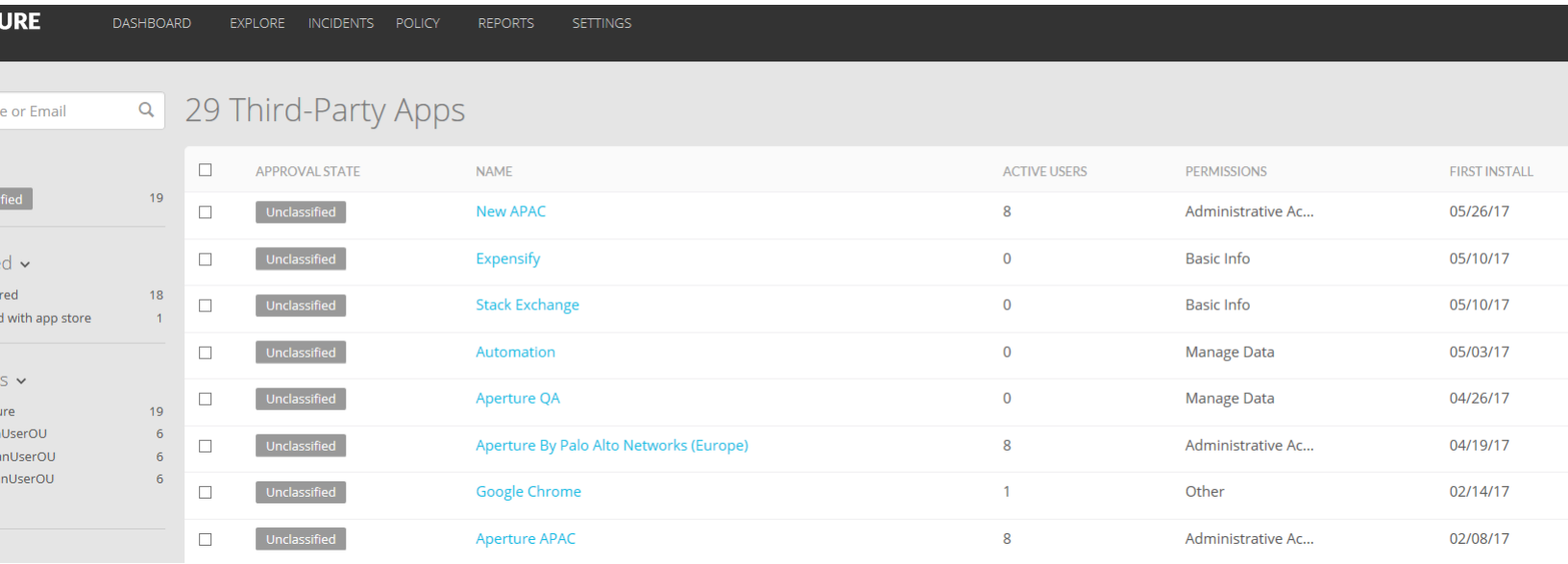
1. Click **Show Schema** and select the **Category** from the list of available content types.
2. Apply the content labels in **Name** and use the up and down arrows to set the content priority.
3. **Save** your map setting.

A data pattern will automatically be generated based on the classification schema mapping you defined. You can then configure Match Criteria for Asset Rules (Basic DLP) or User Activity Rulesand View and Filter Data Pattern Match Results (Basic DLP) for this data pattern.



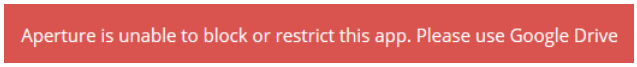
View Information for Third-Party Apps

Prisma SaaS starts scanning third-party apps and lists all discoveries in the third-party apps log. The default action is to log all new discoveries as **`Unclassified`** until admin assessment is completed. To view information for third-party apps, select **Explore** > **Third-Party Apps**.



Click **Name** to view third-party app details These details can include some or all of the following information:

Item	Description
Active Users	Lists the number of users who have installed the third-party app.
Cloud App	Lists the cloud app where the third-party app was discovered.
Description	Displays a brief description of the third-party app services or actions. For example, an electronic signature app would be displayed as: *Send docs for electronic signature, or add your own signature in minutes. Sign PDFs directly from Google Drive or Gmail.*
First Install	Lists the first date the third-party app was installed.
Last Install	Lists the last date the third-party app was installed.
Link	Lists the marketplace where the third-party app is installed.
Manage User Permissions	Lists the number of active and inactive users by name, current status, install date, and approval state. You can approve, block or email the user. **View User Details** by clicking on the **User name**.

Item	Description
Published	Lists the publication URL of the third-party app. For example, an electronic signature app would be displayed as *docusign.net*.
Scope	Lists the permissions to areas the application has requested or been granted.
Unblockable Apps	Certain applications that cannot be blocked. The following type of message will display for unblockable apps: 
User Details	Displays an **Overview** with metadata about the user including active risks, owner, collaborator and number of email messages sent. Lists **Personal Info** including name, email address, and alternate email addresses. Details the **Top Risks** associated with the user and the **Cloud Apps** that the user has added or attempted to add.

Fine-Tune Policy

Fine tuning policy for a managed application in Prisma SaaS provides visibility into the data sharing and collaboration activities of your users. This allows you to flag non-compliant behavior so you can manage user activity, govern application usage, secure corporate data, and prevent data loss due to malicious or inadvertent user actions.

Prisma SaaS includes six Predefined Data Patterns that are automatically applied when Prisma SaaS scans the assets in the connected applications, but you can modify or disable policy rules to better suit your security needs.

- Modify a Policy Rule
- Disable a Policy Rule

Modify a Policy Rule

When you modify a policy rule, Prisma SaaS scans all content against the newly defined criteria to assess incidents.

STEP 1 | Click **Policy**, select the Policy type, and choose the rule you wish to modify.

STEP 2 | Modify the following options as required:

1. Edit the **Rule Name**.
2. Update the **Description**.
3. Set the **Severity** for the policy rule.
4. Verify the policy rule is **Enabled**.
5. Select **Users** or **Assets** for User Activity Rules or **Setting Type** for Security Control Rules.
6. Edit the Match Criteria for Asset Rules (Basic DLP) and User Activity rules.
7. Select what **Actions**, if any, you want to select for Automatic Remediation.
8. **Save** your changes.

Disable a Policy Rule

You can disable a rule if you no longer need it, but as a best practice, do not disable a policy rule until you have reviewed any associated incidents.

Disable a policy rule.

1. Select **Policy**, select the Policy type, and find the rule you want to disable.
2. Click on the rule and set the **Status** to **Disabled**.
3. **Update** the rule.

   The disabled rule is now listed under **Disabled** for the Policy type.

Prisma SaaS Supported File Types

Prisma SaaS extracts metadata and textual content for more than 100 file formats including the following commonly used formats:

- Hyper Text Markup Language—HTML, XHTML
- XML and derived formats—OOXML
- Microsoft Office document formats—complete list including both the OLE-based and XML-based formats (for example DOC and DOCX)
- Source code
- Mail formats—including MS Exchange, MS Outlook, PST, and RFC 822
- Executable programs and libraries—windows executables and Linux/BSD binaries
- Open Document Format
- iWorks document formats—Numbers, Pages and keynote
- Portable Document Format—PDF
- Electronic Publication Format—ePub
- Rich Text Format—RTF
- Compression and packaging format—tar, rar, zip, 7zip
- Text formats
- Feed and Syndication formats
- Help formats—chm
- Java class files and archives—jar
- Font formats

Visit Apache Tika to view a complete list of supported file types by Prisma SaaS.

Languages Supported for Scanning Assets

Prisma SaaS can scan content in the following languages to detect and prevent data exposure:

- English
- German
- Japanese
- Spanish
- Italian
- French
- Dutch
- Portuguese

Assess Incidents

When you first add a new SaaS application, Prisma SaaS goes through a discovery phase where it compares the enabled data patterns and active policy rules against the information about all users associated with your assets. The service also gathers metadata for the assets (folder, repository, and table names and information about the files, such as the owner and collaborators) and the actual contents of the files. The service monitors changes in all of your monitored cloud apps and adds new incidents after it scans the assets. How soon Prisma SaaS can identify incidents depends on a variety of factors including the volume of users and assets on your SaaS application, and the SaaS application provider's process for queuing and throttling calls to their API.

What is an Incident?

An incident is a record you can use to track a policy violation in a managed SaaS application. Prisma SaaS identifies incidents when it finds a violation of Asset rules or Security Control rules against default policy rules and any custom rules you have defined. It detects these incidents by scanning all assets in your managed SaaS applications and matching the file and folder metadata, associated collaborators, and the content of the files against your active policy rules or the configuration.

For each incident, you can determine whether it indicates a regulatory non-compliance, or if it compromises the security of your proprietary data or intellectual property.

Some examples of incidents include:

- AWS keys that have not been rotated in 3 months.
- Files WildFire has classified as malware.
- Passwords that do not meet the minimum complexity requirements.
- A document or folder containing sensitive data (such as credit card or social security numbers, secret code names, or source code) shared with an external user or contains a public link.
- Assets users have shared with external domains or collaborators or are directly accessible through a public link or vanity URL.
- Forwarding a corporate email containing sensitive data to a personal email domain.

Prisma SaaS provides the following default **Open** and **Closed** categories:

You cannot delete, or rename default or custom categories.

State	Incident Category
Open	Prisma SaaS automatically assigns all incidents as **New** and needs assessment. You cannot manually assign an incident from another state to New.
	The incident has been **Assigned** to another administrator. To Assign Incidents to Another Administrator, select an admin from **Assigned To**.
	The incident investigation is **In Progress**, but not closed. The assigned administrator is actively working to assess and resolve the incident.
	Pending action to take place before you can assess or investigate the incident.
Closed	**No Reason** found for the reported incident.
	Business Justified for incidents such as testing, any Prisma SaaS demonstrations, and training.
	Misidentified as a data pattern match or policy violation.

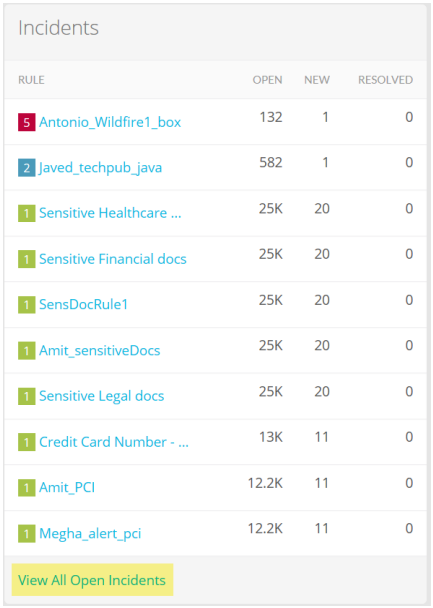
State	Incident Category
	Automatic Remediation resolved this incident **In the Cloud**. You cannot manually assign an incident from another state to **In The Cloud**.

See Assess New Incidents for information on how to review and resolve these issues.

Assess New Incidents

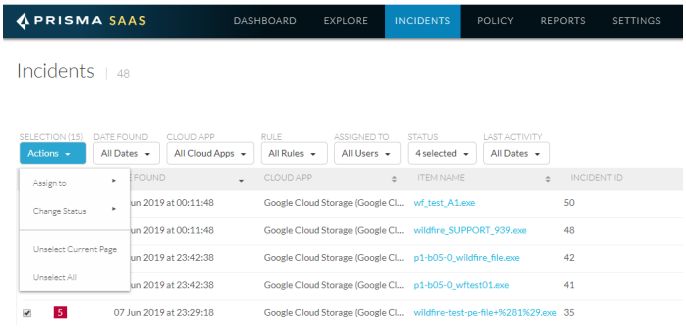
Prisma SaaS compares all information it discovers against the enabled data patterns and active policy rules and identifies all violations and exposures for every asset across all cloud apps. The service then sorts the violations by severity so you can assess and either close or address them. After the initial discovery and remediation process, you should never see the same incidents again.

STEP 1 | Select **Dashboard** and view open **Incidents** to see a summary of policy rules with the number of open violations, any new incidents discovered in the last seven days, and the number of resolved incidents.

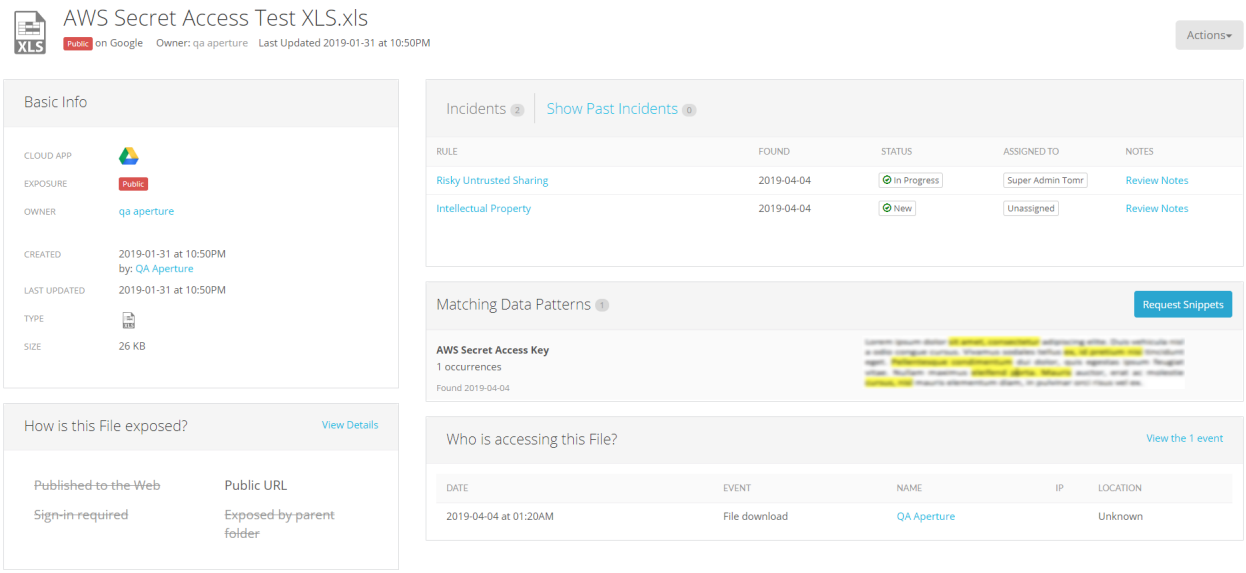


STEP 2 | Drill down into the incidents associated with a policy rule by clicking the corresponding link or **View All Open Incidents**, which takes you to a list of all open incidents where you can narrow your search results further or edit multiple incidents at once.

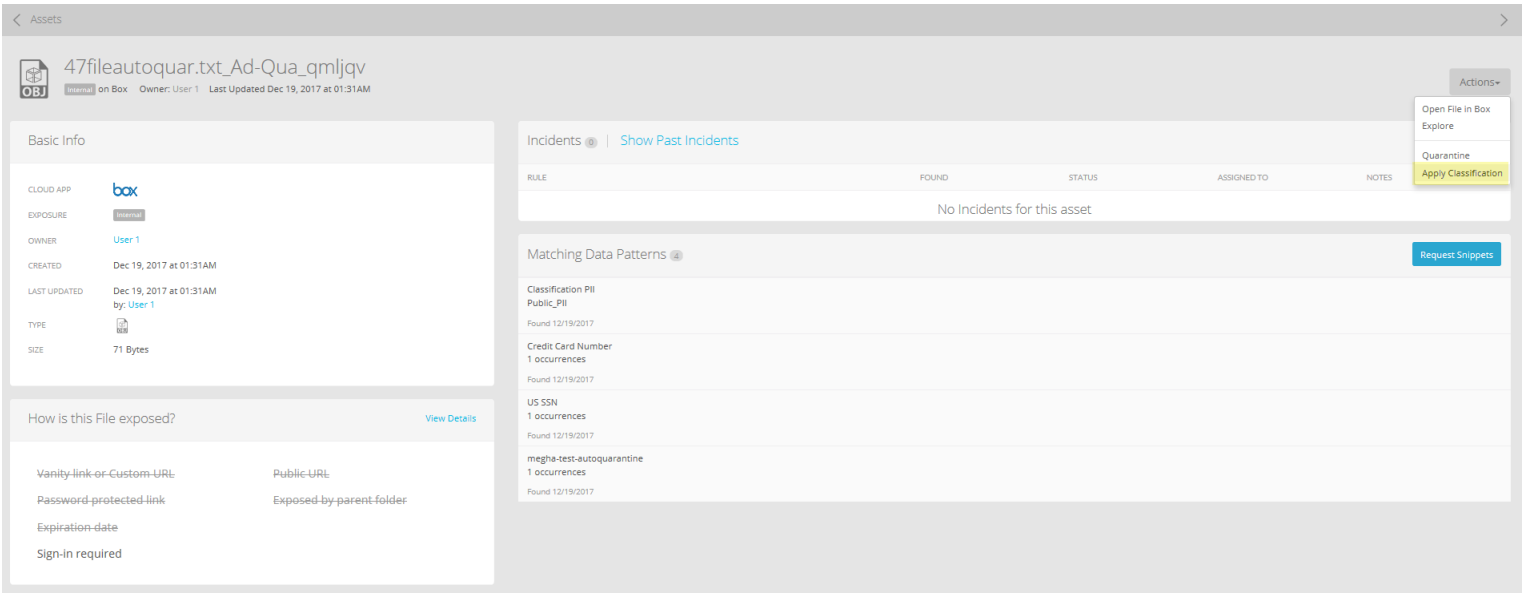
- Select **Display** to customize the columns displaying incident information.
- To filter Incidents and pinpoint risks, you can enter keywords to search for, such as a file name or part of a file name, sort each column by ascending or descending data, or you can use the built-in filters to see different views.
- Click **Export CSV** to download the current view of incidents in a comma-separated list.
- Use **Actions** to select and change the status of or assign up to 1000 incidents to another admin. You can view status changes in Remediation Activity Logs and incident assignment updates in the Admin Activity Logs.



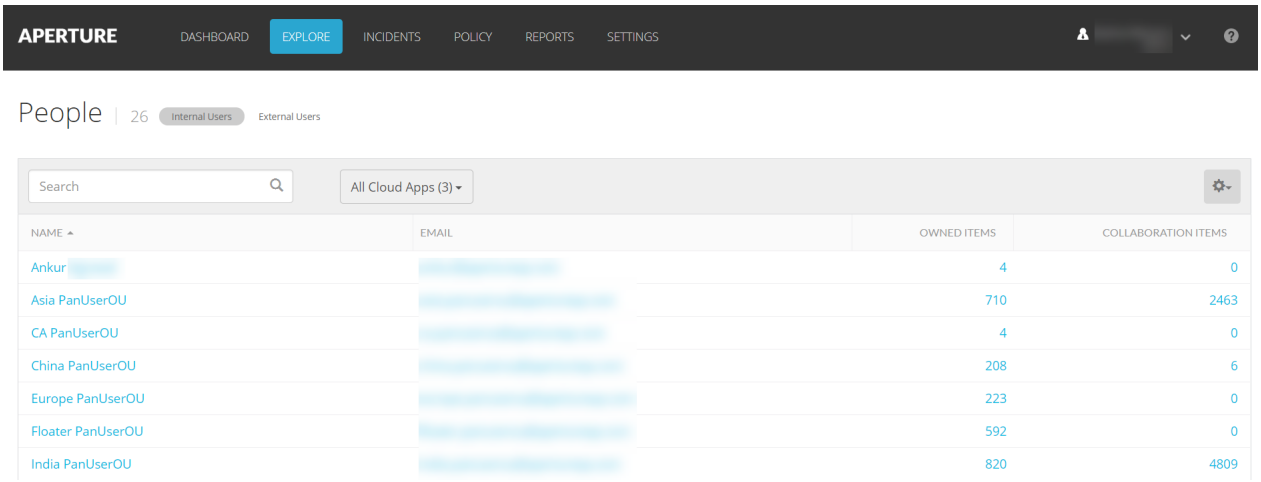
STEP 3 | Drill down into a particular asset by clicking on the **Item Name**. Asset Details displays basic info, the policy rule the asset violated, a snippet of the file with the risky content highlighted, if available, and a link to the asset in the associated cloud app so you can get more context into the incident.



STEP 4 | In **Actions**, depending on the asset type and cloud app, you can open the asset, quarantine, explore the hierarchy of the file, send an email to the owner, download the file, or apply classification labels to third-party apps.



STEP 5 | To filter incidents associated with users, click **Explore** > **People**, select **Internal Users** or **External Users**, and scan the columns for **Owned Items** and **Collaboration Items** to identify users with a pattern of risky behavior. Click the value in a column to view their email, any cloud applications used, role, and activity as well as **More Info** to see detailed information associated with the user.



STEP 6 | After you understand the incidents and the context around them, you can start to address incidents. If you have several incidents to resolve, you can configure Automatic Remediation for most of the cloud apps. There are several ways to remediate an incident:

- Use the WildFire Report to Track Down Threats
- Quarantine
- Change Sharing
- Assign Incidents to Another Administrator
- Modify Incident Status
- Close Incidents

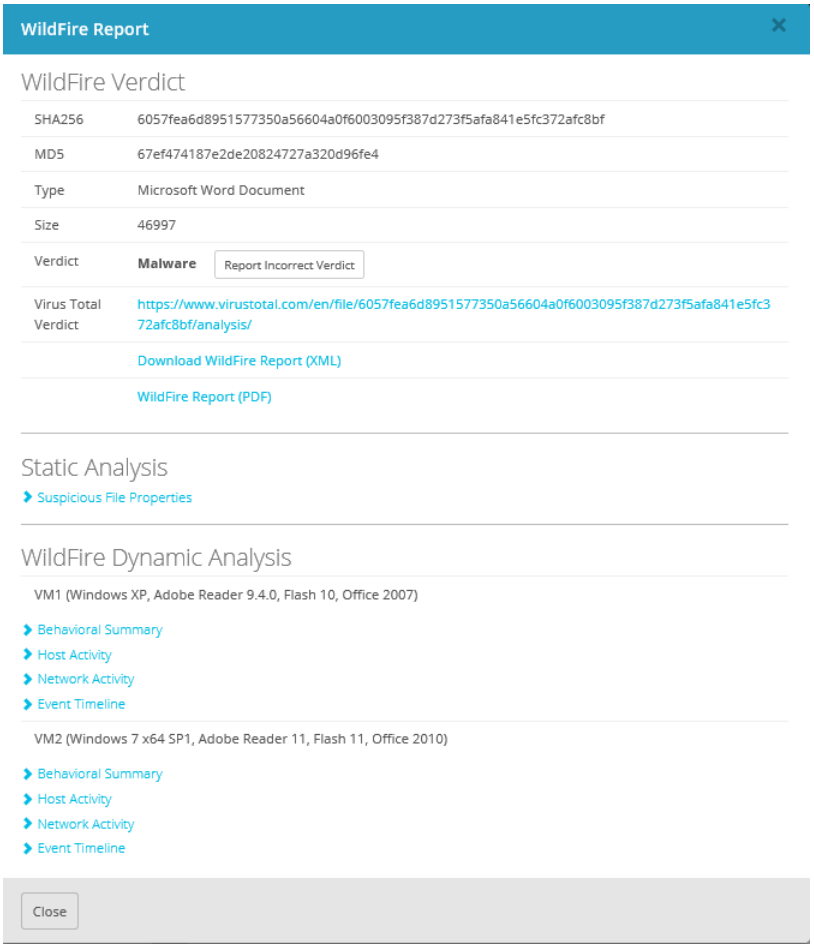
Security Controls Incident Details

Prisma SaaS scans and analyzes email assets, settings, and user behavior and applies Security Control policies to identify exposures, risky user behavior, and sensitive documents. The service also performs a deep content inspection for known and unknown malware, data exposure, and data exfiltration. When Prisma SaaS determines that the security control is an incident, it creates an incident detail view that you use to Assess Incidents in your managed SaaS applications. These details can include some or all of the following information:

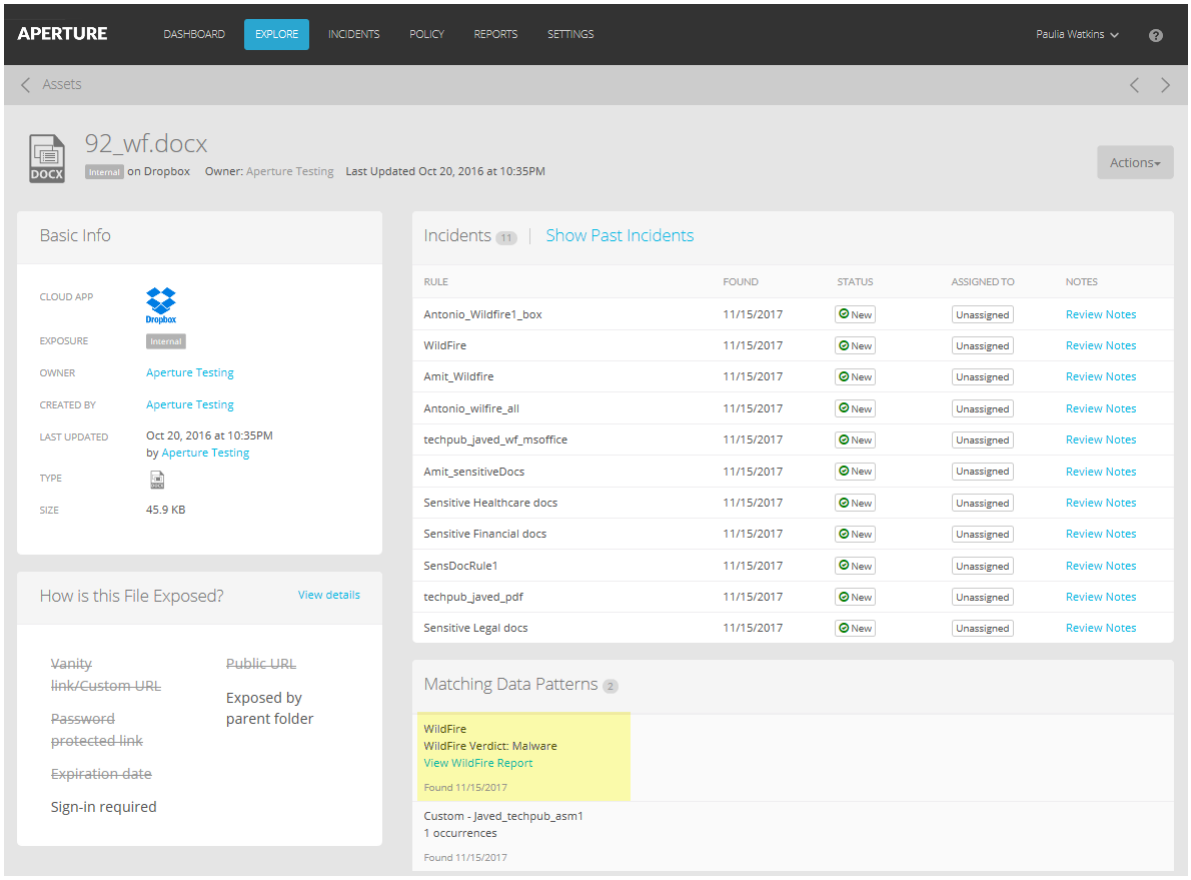
Incident Detail	Description
Setting Detail	Displays which security control rule was violated, the date Prisma SaaS discovered the incident, the scanned Cloud app, and identifies the email sender, principal owner, or folder owner. For assets that match the WildFire Analysis rule, you can Use the WildFire Report to Track Down Threats.
Setting Name	Links to the SaaS app and displays the settings available to configure, such as key rotation, password policy, and email auto-forward rules.
Options	Option to **Email** a message to the email sender, principal owner, or folder owner or **Dismiss** the incident.

Use the WildFire Report to Track Down Threats

If an asset in one of your monitored SaaS applications matches the WildFire Analysis rule, it means that WildFire has identified the asset as malicious. You can use the information in the corresponding WildFire Report to investigate the malware and the activities of the associated user on your network to determine whether the malware has taken hold within your network. Use the WildFire Report to track down potential threats on your network.

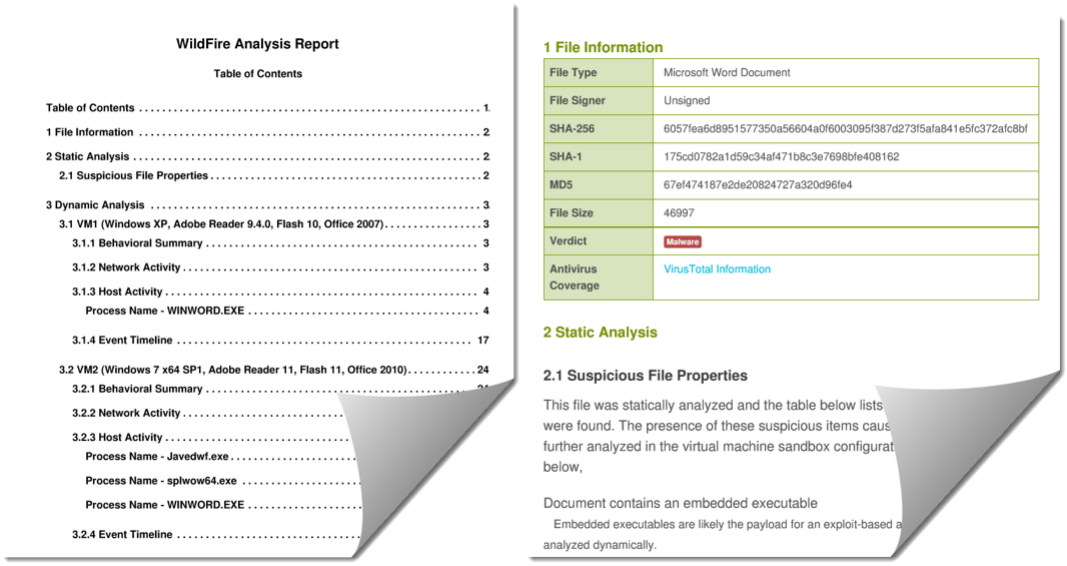


STEP 1 | In the matching data pattern section of the View Asset Details or Security Controls Incident Details, click **WildFire Report** (displays only for incidents that detail a WildFire Analysis rule violation).



STEP 2 | Review the WildFire Report to get context into the malware findings. You can download the report in XML or PDF format. This report contains the following sections:

- **WildFire Verdict**—Displays details about the file, including the hash (SHA256), file type, and size. Additionally, the report provides a link to the VirusTotal Verdict, if available (this link displays a **`file not found`** error if the malware has never been discovered before). If you disagree with a WildFire verdict, click **Report Incorrect Verdict**, and send Palo Alto Networks a request for further analysis.
- **Static Analysis**—Leverages the machine learning capabilities of WildFire to display samples that contain characteristics of known malware.
- **WildFire Dynamic Analysis**—Displays details about the malicious host and network activity the file exhibited in the different WildFire sandbox environments.



STEP 3 | If you have an AutoFocus subscription, you can use the hash (SHA256) in the WildFire report to search AutoFocus for any existing threat intelligence about the malware. This will give you context into whether firewalls within your organization have detected the file and whether the file is prevalent in your industry or globally. Additionally, AutoFocus highlights high-risk WildFire report artifacts (such as a URL or filename), which enables you to quickly find and investigate the artifacts that are frequently associated with malware. In AutoFocus, you can also:

- Search based on an artifact found in a WildFire report.
- Set up alerts based on a hash or an artifact and be notified whenever that hash or artifact is detected by WildFire (you can set the alert to trigger only for samples submitted from your network, only for global submissions, or for both).

STEP 4 | If you configured User-ID on your firewalls, you can generate a user activity report for the file owner or filter the logs by the file owner's user name to see if you can identify any suspicious Traffic logs or Threat logs that might indicate that the malware has propagated.

Customize the Incident Categories

Assigning an incident category to a policy violation allows you to filter and view incidents by category. By default, all incidents are new until categorized. You can assign incident categories when you Assess Incidents to provide a filtering mechanism or assign a category when you close incidents to provide an audit trail or when you Assign Incidents to Another Administrator to help provide context around the risk.

You cannot delete or rename default or custom categories.

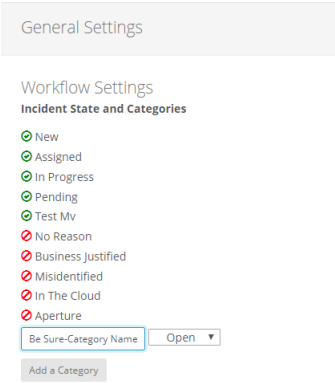
STEP 1 | Verify that you have the required permissions.

You must be an administrator with a Super Admin role or an Admin with access to all apps to create new categories.

STEP 2 | Select **Settings** > **General Settings** to create a custom category.

If the field is not accessible, you do not have the required permissions to create a custom incident category.

1. Enter a **`Category Name`** and select **Open** or **Closed** state.



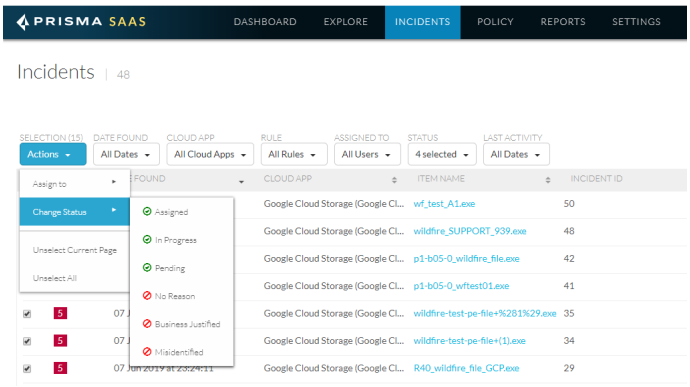
2. **Save** your changes.
3. Your custom category is an option when you Modify Incident Status or Close Incidents.

Modify Incident Status

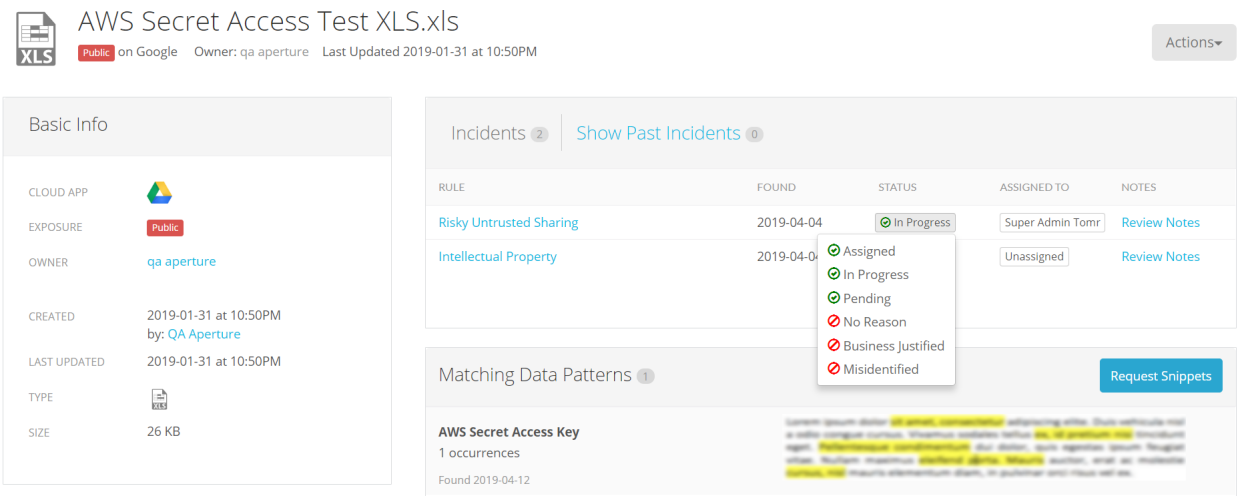
By default, Prisma SaaS identifies, performs appropriate actions, and updates the category and status for incidents matching a data pattern with automatic remediation. For other open incidents, Prisma SaaS identifies these incidents as **New** so you can Assess Incidents and modify the status for a single incident, or use **Actions** to update a group of incidents. You can select one of the default incident categories or Customize the Incident Categories.

Administration Activity Logs record any changes made to an incident and Remediation Activity Logs record an event for closed incidents.

- To modify a bulk of incidents, click **Incidents** > **Assets** and select up to 1000 incidents to modify. Click **Actions** > **Change Status** and select a category to move the group of events to.



- To modify a single incident, click the asset name to view the Asset Details or Security Controls Incident Details, and select a **Status** category.



Close Incidents

When you Assess Incidents, you might sometimes find the content of an asset or how the asset is shared does not pose a threat to your organization. In these cases, you can close the incident individually or use **Actions** to close a group of incidents. You can select a default close (denoted by a red icon) **Status** category:

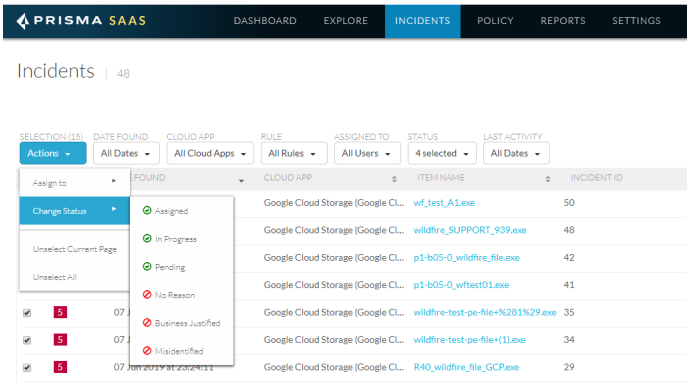
- **No Reason** found for the incident.
- **Business Justified** incidents such as testing, Prisma SaaS demonstrations, and training.
- **Misidentified** as a data pattern match or policy violation.

Additionally, you can Customize the Incident Categories to create close incident categories to suit your organization's needs.

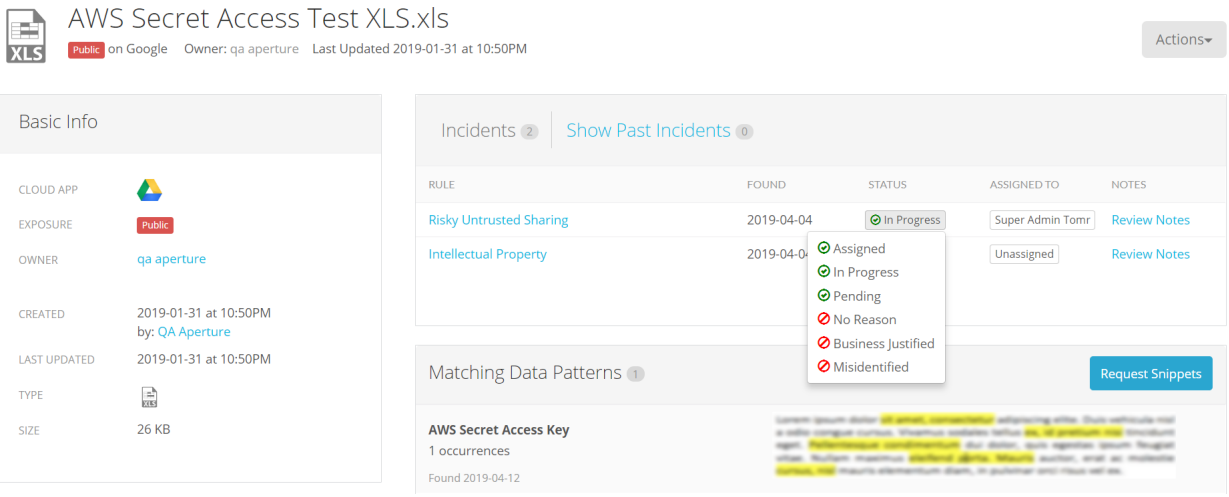
Keep in mind Prisma SaaS identified the asset as an incident because it matched one or more policy rules. Unless you change a setting (for example, changing a Collaborator or domain from Untrusted or Trusted), Prisma SaaS identifies the asset as an incident again the next time it scans that asset. You should Fine-Tune Policy rules to ensure assets that are real threats are the only assets identified as incidents.

If you want to review the events recorded when the status of an incident changes, review these changes in the Remediation Activity Logs.

- To close a group of incidents, click **Incidents** > **Assets**, and select up to 1000 incidents. Click **Actions** > **Change Status**, and select a close **Status**, denoted by a red icon.



- To close a single incident associated with an asset, click the asset name to view the Asset Details or Security Controls Incident Details, and select a close **Status**, denoted by a red icon.



Remediate Issues

Palo Alto Networks® Prisma SaaS provides detailed information about the issues it detects as it scans the assets in your managed SaaS applications. You can use these details to guide you when you decide whether the incidents or issues found pose real threats to your sensitive data and intellectual property, and to assess your app security controls and practices so that you can decide how to eliminate the issues you determine are risks.

- Automatic Remediation
- Supported Applications with Remediation
- Quarantine
- Change Sharing
- Remediation Digest Email
- Remediation Activity Logs
- Monitor User Activity
- Remediate Third-Party Apps
- Manually Remediate Incidents
- Create a Custom Email Template

Automatic Remediation

After you Assess Incidents you can determine the best approach for remediating each incident. Automatic remediation is a powerful tool you can use to address security incidents that Prisma SaaS discovers. When you add a new asset rule, select the remediation or action required to automatically address the incident. These capabilities depend on autoremediation support for your cloud app.

Setting Type	Action	Description
Autoremediate	Quarantine	If an incident poses an immediate threat to your intellectual property or proprietary data, you can automatically move the compromised asset to a quarantine folder. You can choose one: • **User Quarantine**—Send the asset to a special Admin quarantine folder which only Admin users can access. • **Admin Quarantine**—Send the asset to a quarantine folder in the owner's root directory for the associated cloud app. When an asset is automatically quarantined, you can send the asset owner a Remediation Email Digest that describes the changes that were made (**Actions Taken**).
	Change Sharing	If an incident includes a link that allows the asset to be publicly accessed (Public Link), you can automatically remove the links that allow the asset to be publicly accessed. You can remove the direct link on the asset only, or you can also remove links that expose the asset due to inheritance from parent folders. When an administrator automatically changes sharing on an asset, you can send the asset owner a Remediation Email Digest that describes the changes that were made (**Actions Taken**).
	Notify File Owner	Instead of automatically fixing the incident, send file owners a Remediation Email Digest that describes actions that they can take to remediate the policy violation (**Recommended Actions**).
	Notify via Bot	Instead of using the administrator account, use a machine account to send the file or message owner a message that describes the actions they can take to remediate the policy violation (**Recommended Actions**).

Setting Type	Action	Description
Other Actions	Create Incident	For most policy rules, verify that the **Actions** setting is **Create Incident**. This option allows you to identify potential risk for new cloud apps that you added. Then, after you uncover specific incidents that are determined to be high-compliance risks on your network, you can modify the rule or add a new rule that triggers one of the autoremediate actions to automatically remediate the policy violation.
	Send Admin Alert	If there are compliance issues that need immediate action, such as policy rules that are high-risk or sensitive, you can send one or more administrators an alert. Sends administrators a Remediation Email Digest that describes actions administrators can take to remediate policy violations (**Recommended Actions**).

Supported Applications with Remediation

Automatic remediation is supported on the following cloud apps. Alternatively, you can Manually Remediate Incidents for individual assets. The following table outlines support by remediation capability. If a capability is not listed, the option is supported by default. For example:

- When an *admin* quarantine is supported, all file actions within that quarantine are too, including **Delete** asset, **Restore** assets, and **Download** asset.
- All cloud apps support basic incident management actions, including **Send Admin Alert** and **Create Incident**.

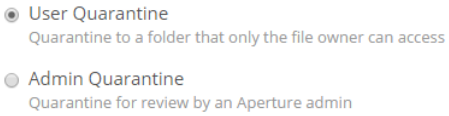
Cloud App	Quarantine		Change Sharing Remove Public Links (Files & Folders)		Notifications		Notes
	User	Admin	Direct link	Inherited link	Notify File Owner	Notify via Bot	
Amazon S3	Yes	Yes	Yes	Yes	No	No	—
Amazon Web Services Console	No	No	Yes	No	No	No	—
Box	Yes	Yes	Yes	Yes	Yes	No	—
Citrix ShareFile	Yes	Yes	Yes	Yes	Yes	No	—
Cisco Webex Teams	No	No	No	No	Yes	Yes	Supports deletion of messages and files. You can view all messages and files that have violated policy on **Explore** > **Assets**, and can delete the asset from the list. Select the asset, and then **Actions** > **Delete Content** to delete it.

Cloud App	Quarantine		Change Sharing Remove Public Links (Files & Folders)		Notifications		Notes
	User	Admin	Direct link	Inherited link	Notify File Owner	Notify via Bot	
							Make sure to review the snippet (if available) before deleting the asset because you cannot restore after deletion.
Confluence	Yes	Yes	Yes	Yes	Yes	No	—
Dropbox	Yes	Yes	Yes	Yes	Yes	No	Assets found in team folders are unsupported.
Github	No	No	No	No	No	No	No remediation support. Only scanning is supported.
Gmail	Yes	Yes	Yes	Yes	No	No	—
Google Cloud Platform	No	Yes	Yes	Yes	Yes	No	—
Google Drive	Yes	Yes	Yes	Yes	Yes	No	When a file is restored from Admin quarantine, collaborators are not restored.
G Suite	No	Yes	Yes	No	Yes	No	—
Jive	Yes	Yes	Yes	Yes	Yes	No	—

Cloud App	Quarantine		Change Sharing Remove Public Links (Files & Folders)		Notifications		Notes
	User	Admin	Direct link	Inherited link	Notify File Owner	Notify via Bot	
Microsoft Azure	No	Yes	Yes, Only Folders	Yes, Only Folders	No	No	—
Microsoft Exchange	No	No	No	No	No	No	—
Microsoft Office 365 - OneDrive	Yes	Yes	Yes	No	Yes	No	—
Microsoft Office 365 - SharePoint	No	Yes	Yes	No	Yes	No	—
Salesforce	No	No	No	No	No	No	—
ServiceNow	Yes	Yes	Yes	Yes	Yes	No	—
Slack for Enterprise	No	Yes	No	No	Yes	No	Only file quarantine is supported. Notifications sent via Slack to the quarantine administrator and the asset owner.
Workplace by Facebook	No	No	No	No	No	No	—
Yammer	No	No	No	No	No	No	—

Quarantine

If an asset poses an immediate threat to your intellectual property or proprietary data, you can automatically move the compromised asset to a quarantine folder. You can choose between sending the asset to User Quarantine folder, a quarantine folder in the owner's root directory in the associated cloud app, or sending the asset to a special Admin Quarantine folder that only Admin users can access. These capabilities depend on autoremediation support for your cloud app.



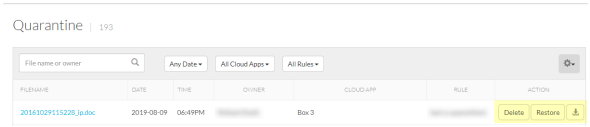
- **User Quarantine**—The asset is saved to a User Quarantine folder in the asset owner's root folder structure. Only the owner can access the asset. Any direct links and collaborators on the asset are removed. Owners can view and restore the quarantined asset.
- **Admin Quarantine**—The asset is saved to an Admin Quarantine folder in the root folder structure of the administrator who installed the associated cloud app. The folder name will include a date stamp. Only Prisma SaaS administrators can download, view, and restore these quarantined assets. This option is useful for assets that prevent serious threats to your network (for example, malware).

When you quarantine an asset, the original asset is replaced with a placeholder (tombstone) file, a plain-text file that contains a simple description to explain that the asset has been quarantined. Administrators can use **Settings** > **General Settings** > **Tombstoned Files** to customize this message.

You can quarantine assets automatically when you Add a New Asset Rule, or you can open View Asset Details or Security Controls Incident Details and select **Actions** > **Quarantine** to manually quarantine an asset.

View, Restore, or Delete Quarantined Files

You can use Prisma SaaS to view assets that have been automatically quarantined by a policy rule or manually quarantined by an administrator. You can restore the asset and return it back in the original location in the owner's directory, or permanently delete the asset.



STEP 1 | Select **Explore** > **Quarantine** to view a list of assets that have been quarantined.

STEP 2 | To filter the list and narrow the results to meet your needs, search or use the following settings:

- **Date**—Time frame when the quarantine occurred. For example: past week, past month, past year. You can also set a specific date or set a custom date range.
- **Cloud App**—List the applications for which the quarantine occurred. For example, Box.
- **Rule**—The policy rule that caused the asset to be quarantined.
- **Search**—Find an item using part of the filename, part of the asset owner's name or email address, or part of a report name.

STEP 3 | (Optional) You can **Restore** the asset to the owner's original location, permanently **Delete** the asset.

You cannot restore after deletion and you will not be prompted to confirm your choice.

STEP 4 | (Optional) Export this data to a CSV file to review the quarantined assets offline.

Change Sharing

SaaS applications make it easy for users to collaborate and share information in the cloud. However, tracking and controlling the different types of sharing in all cloud apps you sanction to ensure that your private data is not exposed can be challenging. This is why the View Asset Details and Security Controls Incident Details identify all the different ways that an asset is shared. In some cases, Prisma SaaS identifies an asset as a risk because it contains sensitive or private keywords or data and you can simply modify how the asset is shared to eliminate the risk.

Types of sharing that might pose a risk include the following:

- **Public share settings**—The asset is publicly indexed on Google or it is stored in a public repository.
- **Shared links**—The owner created a public link, vanity URL, or password-protected link for direct access to the asset.
- **External collaboration**—The owner shared the asset with users outside of your organization.
- **Company-wide collaboration**—The owner created a company-wide URL that gives anyone in the company direct access to the asset.
- **Internal collaboration**—The owner shared the asset with internal users.

When you Add a New Asset Rule, you can automatically change sharing to **Remove Public Links**. Choices include:

- **Only Remove Direct Links**—Remove any links on the asset that allow the asset to be publicly accessed. Only the link on the asset is removed. For some cloud apps, the asset may still be exposed due to inheritance from parent folders.
- **Remove Public Links on Parent Folders if Necessary**—For some applications, you can also remove public links from an asset if the risk is inherited (for example, if the folder where the asset resides has public links or Collaborators, but the file itself does not). This option removes any public links on the asset and removes any public links on parent folders that allow the asset to be publicly accessed.

When public links are automatically removed on an asset, you can send the asset owner a Remediation Email Digest that describes the changes that were made (**Actions Taken**).

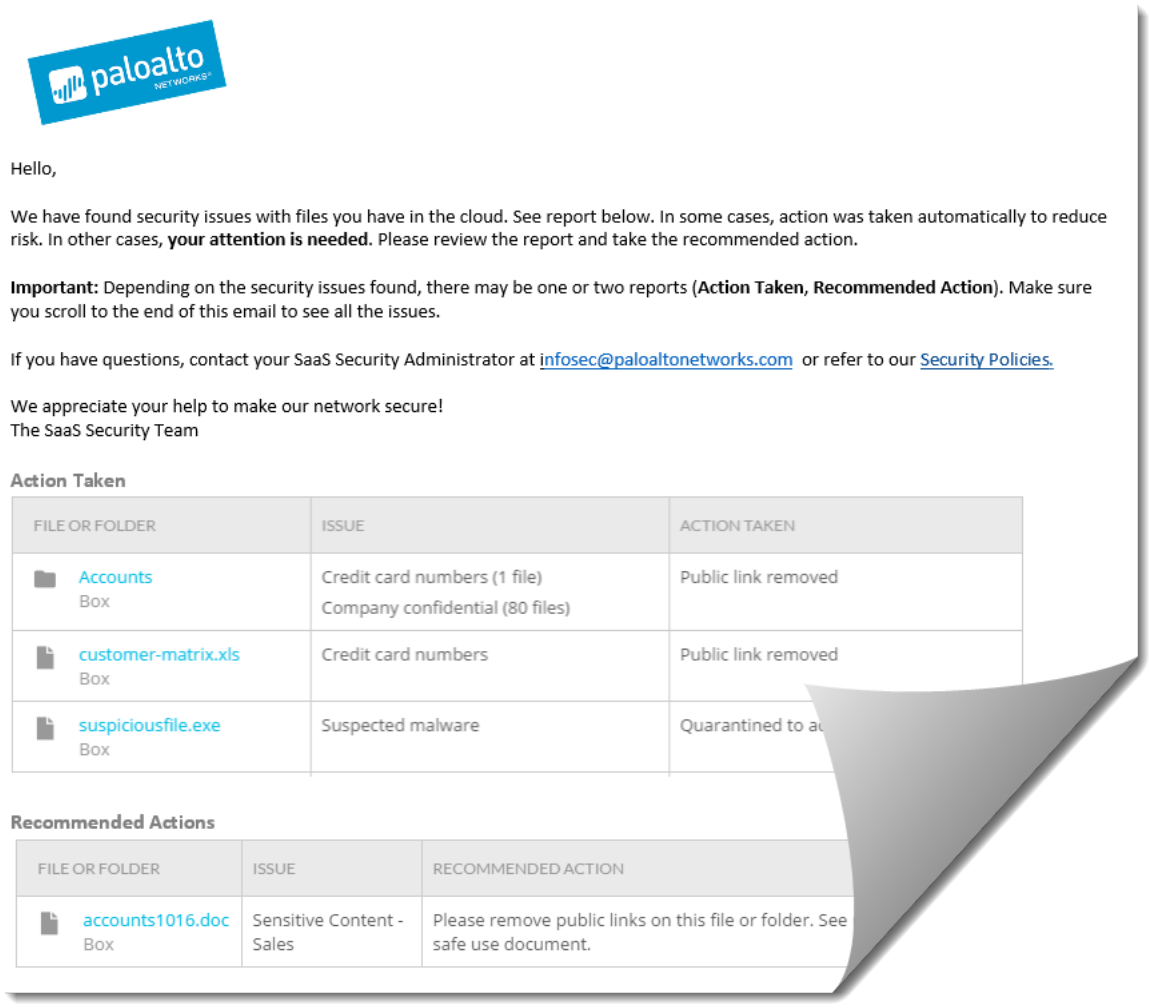
You can change sharing for assets automatically when you Add a New Asset Rule, or you can open View Asset Details or Security Controls Incident Details and select **Autoremediate** > **Change Sharing** to manually change sharing for an asset.

Remediation Digest Email

The remediation digest email contains one or two reports:

- **Actions Taken**—When a risk is automatically remediated, this reports shows a description of the asset, the type of security risk, and the action taken.
- **Recommended Actions**—When a security issue is found, this reports shows a description of the asset, the type of security risk, and the action that the asset owner can take to remediate the risk.

Prisma SaaS sends the digest email once per day to asset owners who have security risks.



Hello,

We have found security issues with files you have in the cloud. See report below. In some cases, action was taken automatically to reduce risk. In other cases, **your attention is needed**. Please review the report and take the recommended action.

Important: Depending on the security issues found, there may be one or two reports (**Action Taken, Recommended Action**). Make sure you scroll to the end of this email to see all the issues.

If you have questions, contact your SaaS Security Administrator at infosec@paloaltonetworks.com or refer to our Security Policies.

We appreciate your help to make our network secure!
The SaaS Security Team

Action Taken

FILE OR FOLDER	ISSUE	ACTION TAKEN
Accounts Box	Credit card numbers (1 file) Company confidential (80 files)	Public link removed
customer-matrix.xls Box	Credit card numbers	Public link removed
suspiciousfile.exe Box	Suspected malware	Quarantined to a

Recommended Actions

FILE OR FOLDER	ISSUE	RECOMMENDED ACTION
accounts1016.doc Box	Sensitive Content - Sales	Please remove public links on this file or folder. See safe use document.

STEP 1 | Select **Settings** > **Remediation Email Digest**.

STEP 2 | Update the **Subject** and **Body** content as desired.

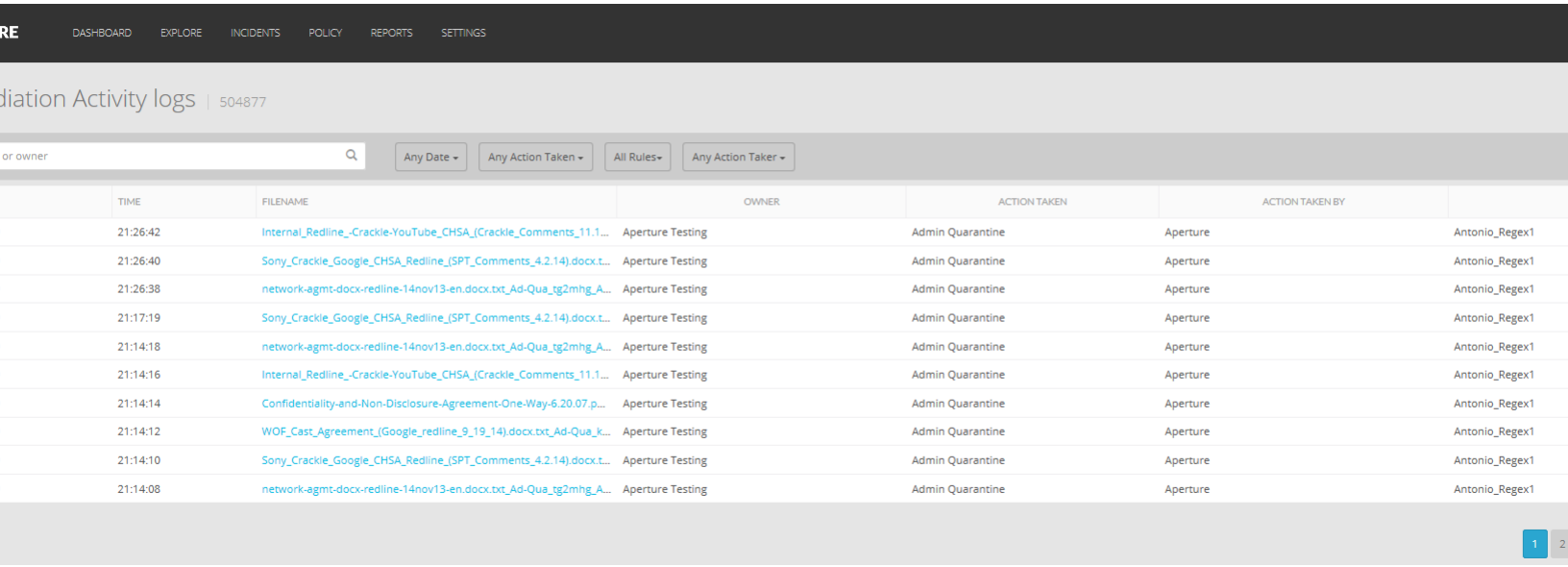
STEP 3 | (Optional) To include a logo as part of the email, select **Include logo in the email footer**. Refer to Configure the Email Alias and Logo for Sending Notifications for details.

STEP 4 | **Save** your changes.

Remediation Activity Logs

You can proactively monitor incident remediation logs to track activity. These logs are useful for auditing the progress of automatic remediation and tracking how incidents were addressed. The logs include actions taken automatically by Prisma SaaS and actions taken by users and administrators.

STEP 1 | Select **Reports** > **Remediation Activity**.



STEP 2 | To filter the list and narrow the results to meet your audit needs, search or use the following facets:

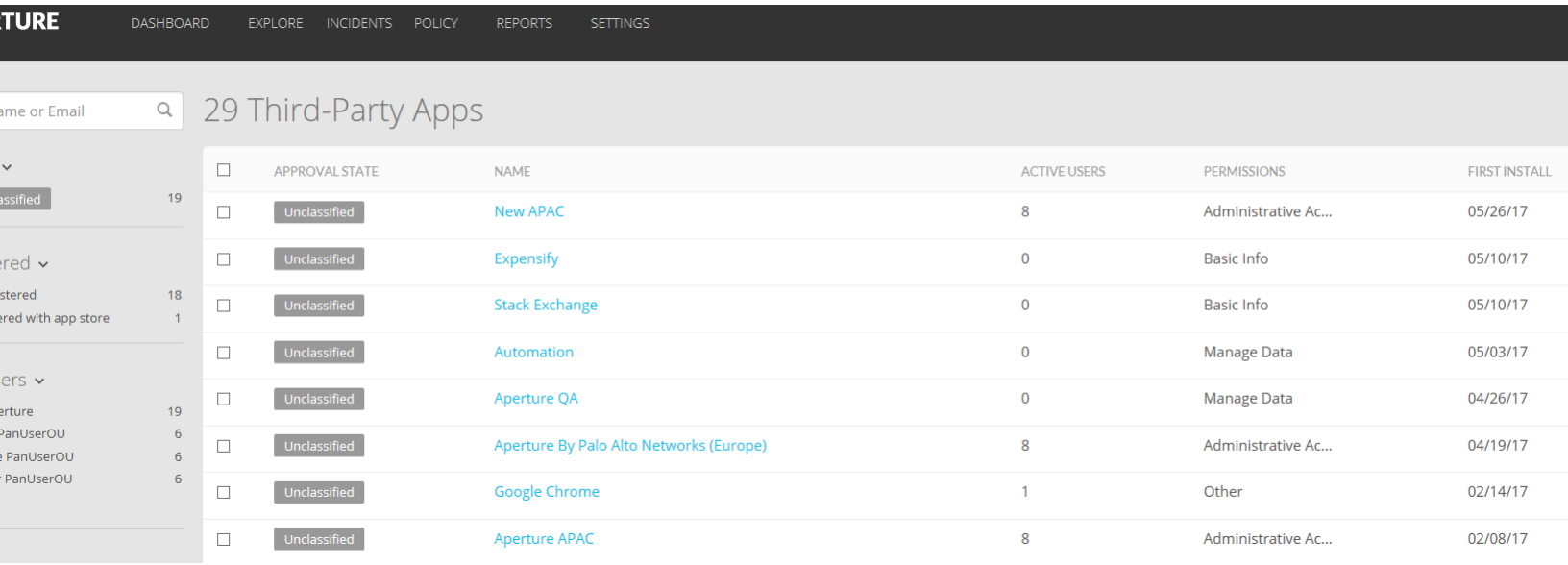
- **Date** —Time frame when the remediation activity occurred. For example: past day, past week, past month, or past year.
- **Any Action Taken**—Remediation action taken on the asset, including Direct Public Link Removed, Inherited Public Link Removed, User Quarantine, Admin Quarantine, Deleted, Restored, Email Sent, No Reason, Business Justified or Misidentified.
- **All Rules**—Policy rule used to discover the risk.
- **Any Action Taker**—The user (or service) that performed the action. Choose **Aperture** to view remediation activity that was done automatically as part of a policy rule.
- **Search**—Find an item using part of a filename or user name.

STEP 3 | Export this data to a CSV file to review the remediation logs offline.

Remediate Third-Party Apps

You can view and assess third-party apps to determine if the potential security threats are real and, if so, you can **Block** or **Restrict** them and send notifications to users. In some cases you may determine that an identified app does not pose a real threat and can **Approve** it. Use the following work flow to drill down into an app and assess whether it poses a security threat.

STEP 1 | Select **Explore > Third-Party apps**. By default, all discoveries are listed as **Unclassified** until they are assessed by the admin. You may **Approve** or **Block** any third-party app in the list view or click an app in the **Name** column to view the details and then **Approve**, **Block**, or **Restrict** the app.



STEP 2 | You can filter third-party apps associated with a particular end user by clicking (**Explore** > **People**).

STEP 3 | Drill down into the details by clicking **Name**. This detailed view displays the metadata of the third-party app and the associated links and cloud apps so that you can get more context around them.

STEP 4 | After you understand the details, you can apply remediation. There are several ways to remediate:

1. To remediate one or more results, select the log entry and click **Actions**, and then click either **Allow** or **Block**.
2. To filter the users accessing a specific third-party app and apply remediation, click **Name** on the log entry and then **Manage User Permissions**, select **All**, **Inactive**, or **Active**.
3. To filter the results by third-party app status, select **Approved**, **Restricted**, **Blocked**, or **Unclassified**.

When an app is either blocked or restricted, the user is sent an email to notify them of their access status.

- **Approved** the third-party app is accessible by all users.
- **Restricted** the third-party app is accessible for certain users you define, and blocked for all other users.

- **Blocked** all users are blocked access to the third-party app.
- **Unclassified** the admin has not assessed the third-party app.

(Optional) To download a spreadsheet of the third-party list for closer inspection, click CSV.

Manually Remediate Incidents

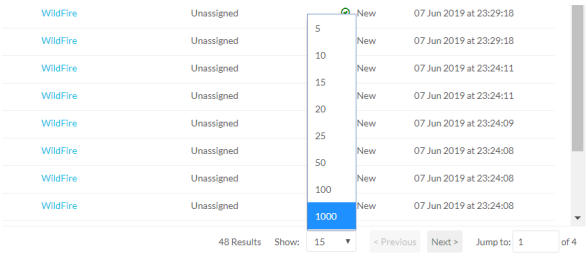
After you Assess Incidents you can determine the best approach for remediating each identified issue. For a large number of assets, you can set up a policy rule to perform Automatic Remediation. Alternatively, you can use the following methods for manually remediation of individual assets:

- Assign Incidents to Another Administrator
- Use the WildFire Report to Track Down Threats

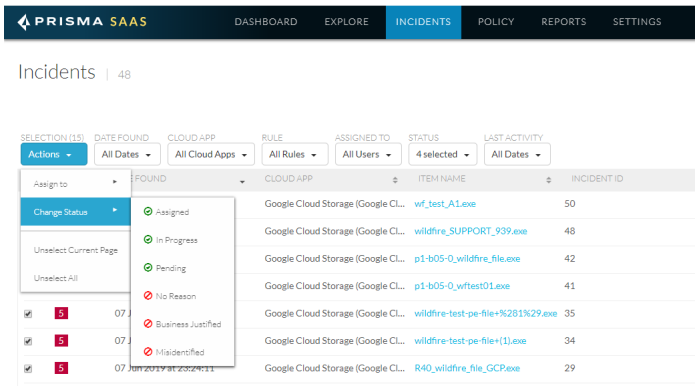
Assign Incidents to Another Administrator

Sometimes you don't have the proper context around the content or the Collaborators to properly Assess Incidents. In these cases, you can assign a single incident or group of incidents to another Prisma SaaS administrator who is more familiar with the content and its proper use. You must be an administrator with a Super Admin, Admin, or Limited Admin role to assign incidents to another admin.

- To assign a group of incidents, select **Incidents** > **Assets** and choose the incidents to assign to another administrator. If the list of incidents is too large, you can use the descending and ascending columns and predefined filters to narrow the list of results.
  1. You can select up to 1000 incidents individuals, in groups, or all at once to assign to another administrator.

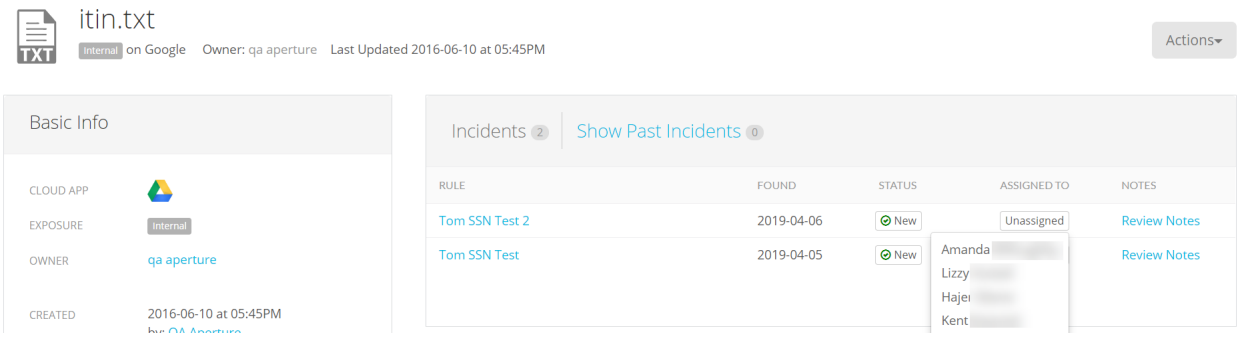


  2. Select **Actions** > **Assign to** and choose an administrator to assign the incidents to.
  3. You can verify the new assignments for each incident in View Administrator Activity Logs or select the administrator in the **Assigned To** search filter.



- To assign a single incident, go to **Incidents** > **Assets**, and click the **Item Name**.
  1. Click **Unassigned** and select an administrator.
  2. (Optional) Select an incident category to associate with the incident. By default, the category is **New**.
  3. (Optional) Click **Review Note** > **Add a Note** to add a provide additional details for the administrator you are assigning the incident to.

4. You can verify the new administrator assignment for the incident in View Administrator Activity Logs.



Create a Custom Email Template

Custom email templates save you time and enable you to define consistent messages:

- When you email your end users (asset owners), you can create email templates so that you don't need to compose each email separately for each notification you send.
- All administrators who assess and remediate risks can use the same templates and thereby reflect one voice.

By default, there is one predefined email template named **Sensitive file in public folder** that you can use as is or modify. You can also create additional templates as needed.

When you create a template, use the following variables in the **Subject** and **Body Text** fields of the template. Prisma SaaS automatically replaces the specific values from the risk details before sending the email to the asset owner.

Template Variable	Description
{AdminName}	The Name associated with your admin account.
{CloudAppName}	The cloud app in which Prisma SaaS identified the risk.
{FileOwnerName}	The cloud app user who owns the asset identified as at risk.

Use the following procedure to create an email template:

STEP 1 | Select **Settings** > **Email Templates**.

STEP 2 | **Add Template**.

STEP 3 | Enter a descriptive **Template Name** to help administrators understand when to use the template.

STEP 4 | (Optional) Enter the **Subject** and **Body Text** to include in every email notification that uses this template. You can use any of the template variables in either of these fields.

STEP 5 | (Optional) Select **Include logo in the email footer**.

Refer to Configure the Email Alias and Logo for Sending Notifications for details.

STEP 6 | Specify whether to **Include Fix and Close buttons** in emails generated using this template by selecting or clearing this option.

STEP 7 | **Save** the template.

You can now use the template to email the file owner.

Generate Reports on Prisma SaaS

You can generate reports on Prisma SaaS to proactively identify policy violations, exposed personal data, and determine your compliance standing. The SaaS Risk Assessment Report allows you to share the security posture of the cloud apps on your network while the GDPR Report gives you insight on potential compliance violations. If you want to review the Wildfire report to identify any assets that are identified as malicious, see Use the WildFire Report to Track Down Threats.

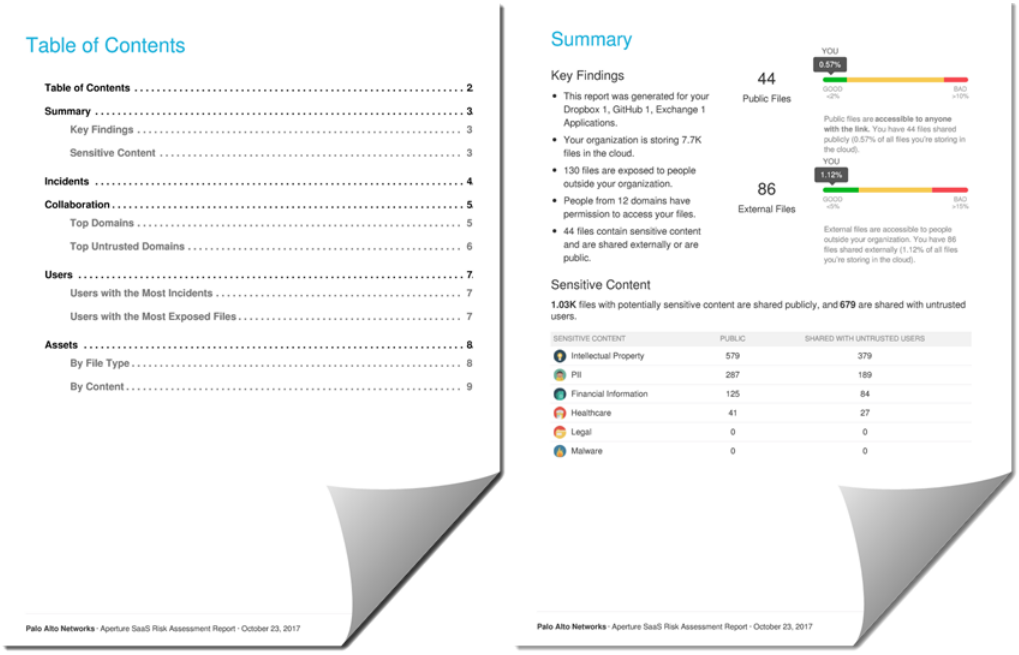
> Generate the SaaS Risk Assessment Report
> Generate the GDPR Report

Generate the SaaS Risk Assessment Report

Use the SaaS Risk Assessment Report to proactively identify problems with how assets are stored and shared across all applications secured by Prisma SaaS and take action to reduce exposure. You can share this on-demand PDF report with your information security team for a periodic check-in, or email it to your executives to highlight SaaS applications usage on your network and how your security posture for SaaS data and applications compares against competitors in your industry. In addition to a summary on key findings, the report summarizes information on policy violations, captures how sensitive content is exposed, lists the top domains with which your users are sharing files, identifies users with the most incidents, and enumerates the most popular file types and incidents per file type across managed cloud applications.

STEP 1 | Select **Reports** > **SaaS Risk Assessment Report**.

STEP 2 | **Generate Report Now** and the report will be emailed to you (the logged in administrator). You can then use your email application to forward this report to your C-level executives. In addition to sending an email to you, Prisma SaaS adds a link to the page so that you can regenerate the same report if required.



You can neither configure a time period nor schedule this on-demand report. The contents of the report use the data available at the time you generate it, and it is a snapshot of the findings up to the time you make the request.

Generate the GDPR Report

The GDPR Report summarizes evidence related to the data privacy regulations for your sanctioned SaaS applications. The report provides actionable intelligence around sensitive data exposure, user activities, your security posture, and the personal data that resides on your applications but does not provide a verdict for compliance. You can export the report to help your GDPR regulator review how you collect, use, and share PII data across your SaaS applications.

For example, you can generate a report to view the number of records transferred to a third country or to an international organization, to learn which sanctioned applications are sharing data externally.

STEP 1 | Select **Reports** > **GDPR Report**.

STEP 2 | Click **Generate Report Now** to view the report and review evidence identified and possible compliance issues. Each Regulation section can be expanded to review the description of the regulation and articles, your applications involved, and the validation used to determine compliance.

STEP 3 | Click **Export PDF** or **Export CSV** to download your report to forward on to your GDPR regulator.

Monitor Prisma SaaS Issues

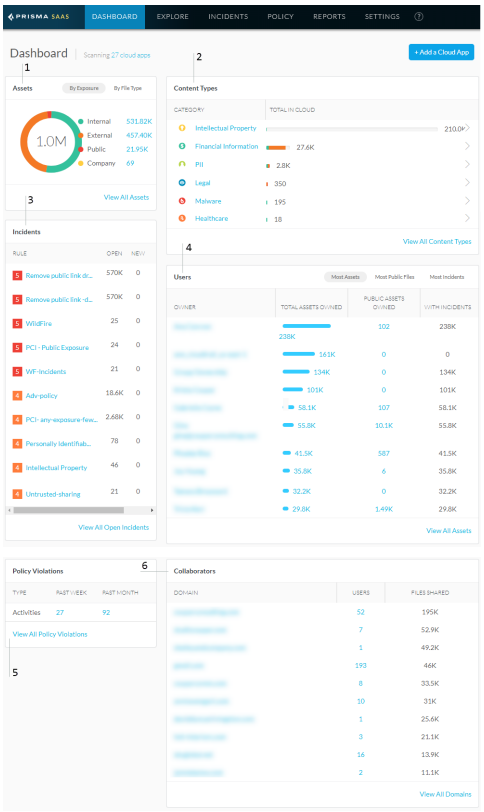
Prisma SaaS provides built-in tools—views and search methods—to help you investigate and monitor your sensitive data. These same tools help you fine-tune your policies over time.

Additionally, before you begin to monitor your sensitive data and if you have an external sys log server, configure sys log monitoring.

Monitor Scan Results on the Dashboard (Basic DLP)

As Prisma SaaS starts scanning the sanctioned SaaS applications, the **Dashboard** presents a summary of the scan in six panes.

The Prisma SaaS Dashboard



1	**Assets**	**Assets** displays the top violations by exposure, (public, external, company, and internal) and the file types associated with the exposure.
2	**Content Types**	**Content Types** displays six predefined data pattern groups and the total volume of content in the cloud for those data patterns. Click **>** to drill down into the details by content category.
3	**Incidents**	**Incidents** displays the number of the active incidents detected against data pattern and policy rule violations for each content type.
4	**Users**	**Users** displays a list of users who own assets, if the assets are public, and displays the number of incidents associated with an asset. You can filter the data to view the owner with the most assets, most public files, and most incidents.

The Prisma SaaS Dashboard		
5	**Policy Violations**	**Policy Violations** displays the type of policy violations and the number of new policies detected within the past week and passed week.
6	**Collaborators**	**Collaborators** displays the external collaborators with whom your internal users are sharing assets.

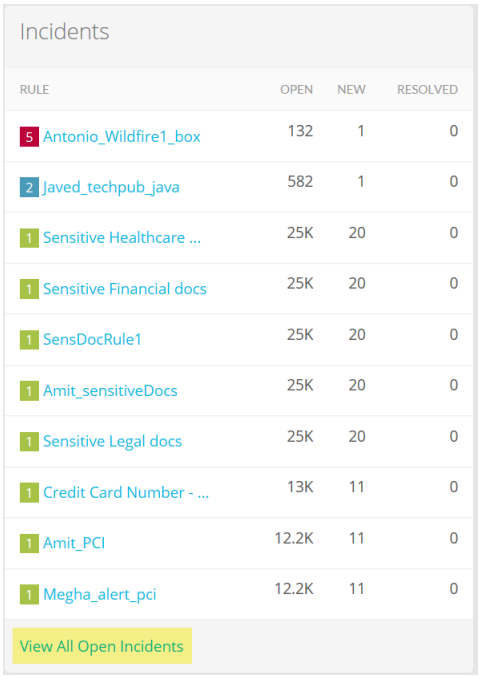
Use the Dashboard to explore the information on how and where assets are shared in your sanctioned SaaS applications, before you delve in to Assess Incidents or Fine-Tune Policy to rescan the assets and mitigate incidents. For example, you can use the Domains and Collaborators widgets on the Dashboard to see whether a collaborator or domain is properly identified as trusted or untrusted and make changes to the scan settings before the discovery phase is complete.

- View All Open Incidents
- View All Domains

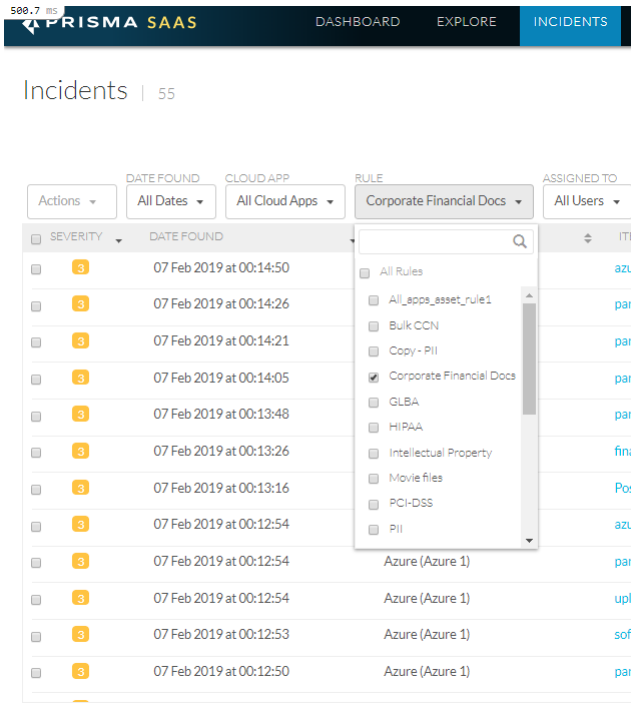
View All Open Incidents

The Incidents pane on the Dashboard summarizes the number of open incidents detected against each policy rule. When Prisma SaaS starts scanning files and matching them against enabled policy rules, the default action is to generate a log when a policy violation occurs. If you enabled email alerts for high-risk issues such as malware or PII compliance violations, you will also receive an automatic email notification in addition to the recording of an incident in the log. Using the Dashboard, you can quickly find and view all open incidents to investigate and remediate.

STEP 1 | On the Prisma SaaS dashboard, select **View All Open Incidents**.



STEP 2 | Select the **Rule** from the drop-down and further sort the open incidents using the columns.



STEP 3 | Continue to Assess Incidents and Manually Remediate Incidents, or review the asset rules that triggered the incident and configure Automatic Remediation.

View All Domains

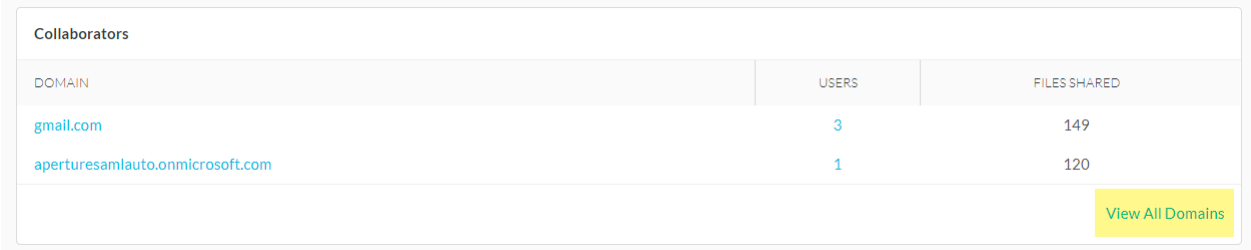
The Collaborators pane displays the email domain of the top ten external collaborators with whom your internal users are sharing assets with. It also lists the number of users for each domain and the number of files shared. Click on **View All Domains** to review the number of users and their trust settings. You can use this information to change the trust settings and/or remove collaborators at the asset level if you are an administrator with a Super Admin role or an Admin role with access to all apps.

STEP 1 | Select **Dashboard** and view the **Collaborators** pane to view a summary of the top ten domains of external collaborators. These are users that are not members of the internal domains you specified in Define Your Internal Domains and with whom internal users are explicitly sharing assets (files or folders).

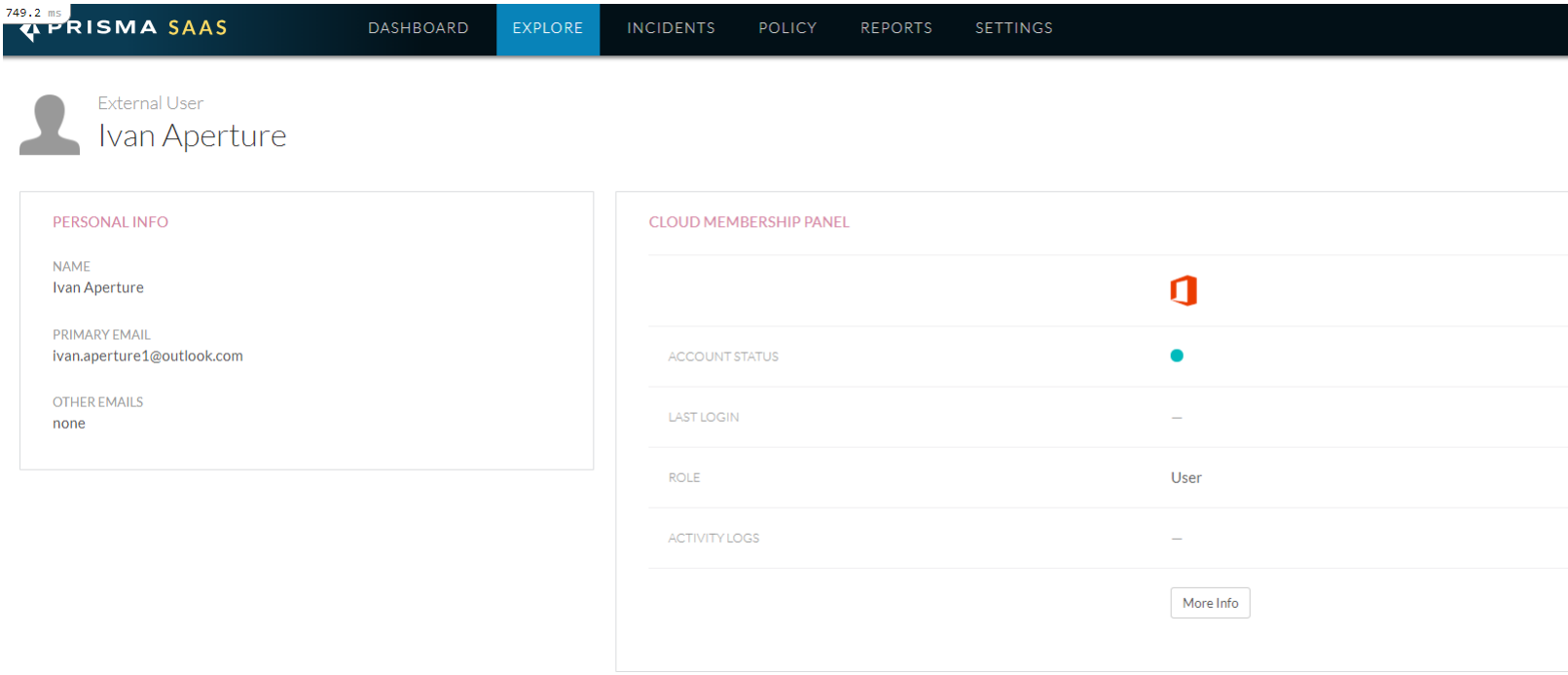
- To assign a domain as **Trusted** or **Untrusted**, select from the **Mark As** drop-down.

  When you mark a domain as **Untrusted**, the domain is added to the list of untrusted users. For details, see Define Trusted and Untrusted Users and Domains.

STEP 2 | Select **View All Domains** to investigate the domains of all external collaborators. This information is the same information found if you navigate using **Explore** > **Domains**.

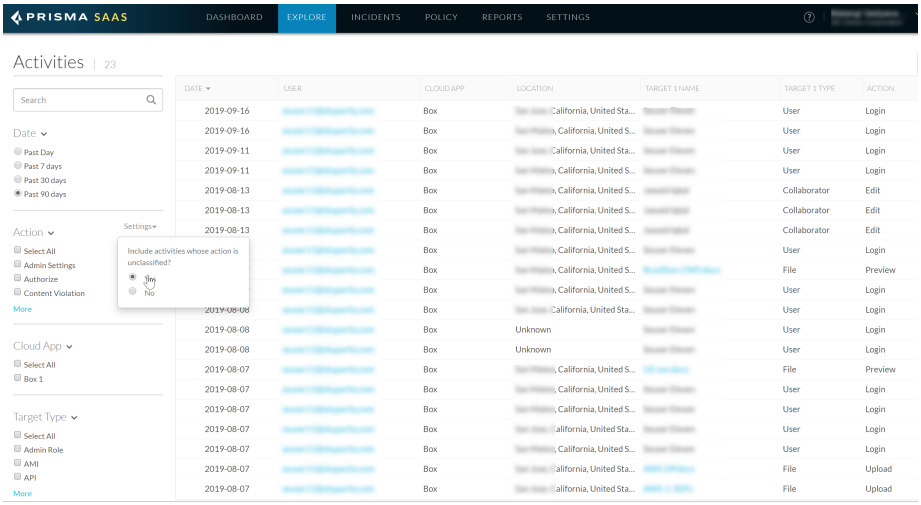


1. Select **External Users** or **Internal Users**.
2. Click the number of **Users** to view details on the names of the user, their email addresses, and number of items each user owns or collaborates on.
3. Click the **Name**, **Email**, **Owned Items**, or **Collaboration Items** link to review details about the user, including which Cloud Apps the user is an owner or collaborator.



Monitor User Activity

On Prisma SaaS, you can view user activity across all assets on Box, Microsoft Office 365 for OneDrive and SharePoint, Google Drive, and Salesforce, but it is more limited on Cisco Webex Teams. Because Prisma SaaS connects to each service using an API integration, it can retrieve the user activity logs and enable you to monitor and investigate the actions of your end users on your data and assets stored in these applications. You can track a variety of events such as file and folder downloads and uploads as well as failed login attempts, or you can learn how a user shared or collaborated on assets hosted in your SaaS applications.



STEP 1 | Select **Explore** > **Activities** to view a list of activity logs from application such as Box, Microsoft Office 365 for OneDrive and SharePoint, Google Drive, Salesforce, or Cisco Webex Teams.

Salesforce requires the User Event Monitoring license to enable the retrieval of all event logs. Without this additional license, only log in and log out events are available to Prisma SaaS.

Google Drive requires a Google Apps Unlimited or Google Apps for Education subscription to enable the retrieval of all event logs. Without this additional subscription, only login and logout events are available to Prisma SaaS.

STEP 2 | To filter the list and narrow the results to meet your audit needs, search or use the following facets:

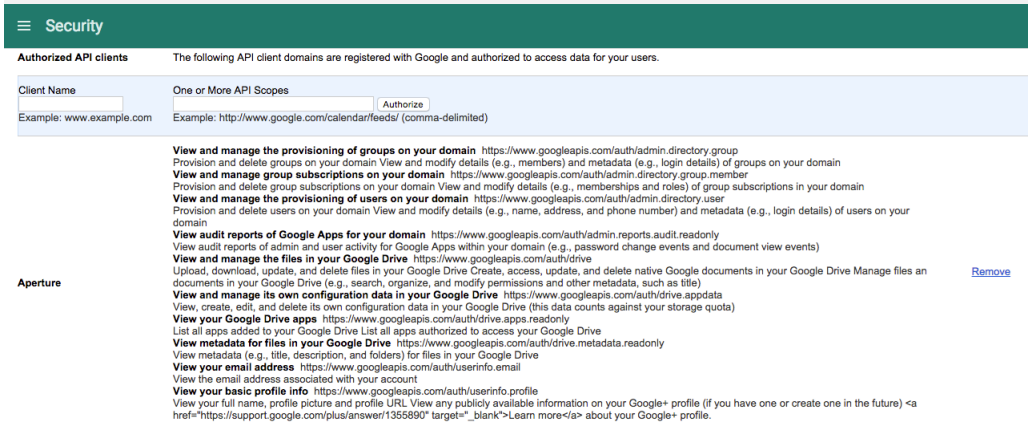
- **Date**—Time frame when the user activity occurred. For example: past day, past week, past month, or past year.
- **Action**—Activity the user initiated. For example, download, preview, sync, share, delete, or copy a file or folder.

  By default, any activity log with action Other is not displayed on Prisma SaaS. To include all activity logs, select Yes for Settings > Include activities whose action is unclassified?.
- **Cloud App**—Lists the application on which the user activity occurred. For example, Box.
- **Target Type**—Lists the location, user, or asset where an activity or change occurred. It allows you to learn about who did what, for example which user initiated an action on a file, space, or folder, or added a user, created a space, performed work on a report, or used the API.

- **Search**—Find an item using part of the filename or find a user by the full email address. Because the user activity logs include information on the email address of the user who logged in, the source IP address and location of the user who performed the action, and the name of the item being modified or created, you can match on a phrase or email address.

STEP 3 | If Prisma SaaS is not monitoring user activity on Google Drive, remove the API client access from Google, then authenticate the Google app again to re-enable access.

- Open a web browser and log in to **admin.google.com**.
- Navigate to **Manage API client access** (located in **Security** > **Advanced Settings**).
- Scroll to find the list of **Prisma SaaS** clients.
- Click **Remove**.



STEP 4 | Export this data to a CSV file to review the activity logs offline.

SaaS Application Visibility on Prisma SaaS

As your users adopt more SaaS applications, you need better visibility into usage, granular control over access, and compliance and security for your data in the cloud application. To help meet the challenge of understanding what is happening on your network (inline enforcement) and cloud applications (API-based protection), Prisma SaaS can access your next-generation firewall or Prisma Access (formerly known as GlobalProtect cloud service) logs stored in the Cortex Data Lake, and combine that data with Prisma SaaS data to present a consolidated view of sanctioned and unsanctioned application usage across your enterprise.

Application visibility on Prisma SaaS provides a list of all applications in use on your network, along with a description of each application, its characteristics, data on the number of users, bytes transferred, and number of sessions to learn about the application usage statistics. You can also learn about if an unsanctioned application is being used, if there are alternative sanctioned applications in use, and which groups of people are using the unsanctioned application.

This visibility will enable you to assess whether you need to secure and sanction other apps or talk with your network administrator to block access to these applications and minimize data security risk for the enterprise. You can continue to use the Prisma SaaS dashboard to deliver complete visibility and granular enforcement across all user, folder, and file activity within sanctioned SaaS applications.

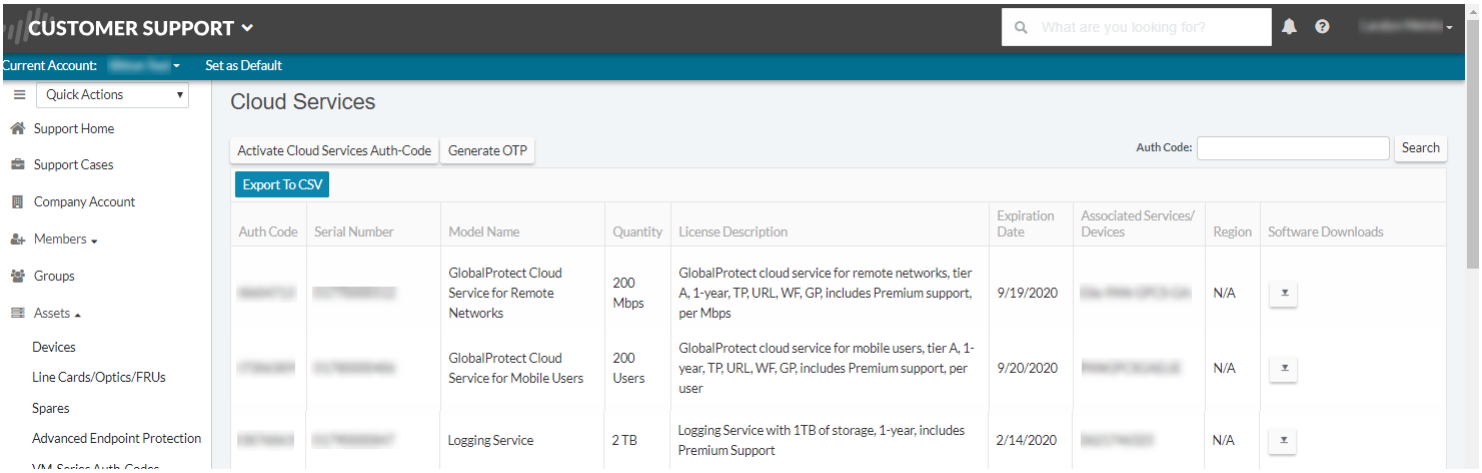
- Extend SaaS Visibility to Cortex Data Lake
- View SaaS Application Usage on Prisma SaaS

Extend SaaS Visibility to Cortex Data Lake

For an inventory of SaaS application usage and patterns on your network, and to identify shadow IT, you need to know about data residing within enterprise-enabled SaaS applications, and network traffic generated by users using managed and unmanaged devices within your organization.

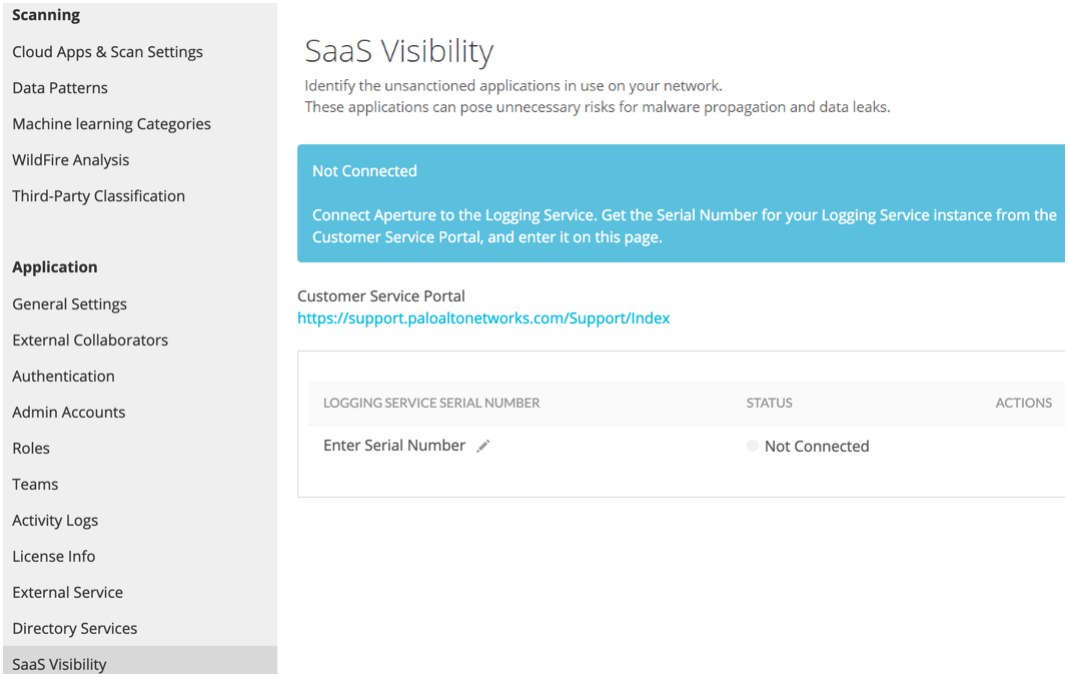
If you are using next-generation firewalls or GlobalProtect Cloud Service as an Internet gateway to secure on-premise or remote users and are storing traffic logs and other logs to the Cortex Data Lake, you need to connect Prisma SaaS to the Cortex Data Lake to extend application visibility. All you need is the serial number for your Cortex Data Lake instance.

STEP 1 | Log in to Customer Service Portal, select **Assets** > **Cloud Services** to locate your Cortex Data Lake (Logging Service) serial number.



STEP 2 | Log in to Prisma SaaS, select **Settings** > **SaaS Visibility**, and enter the serial number.

You must have Admin or Super Admin privileges to add SaaS Visibility on Prisma SaaS.

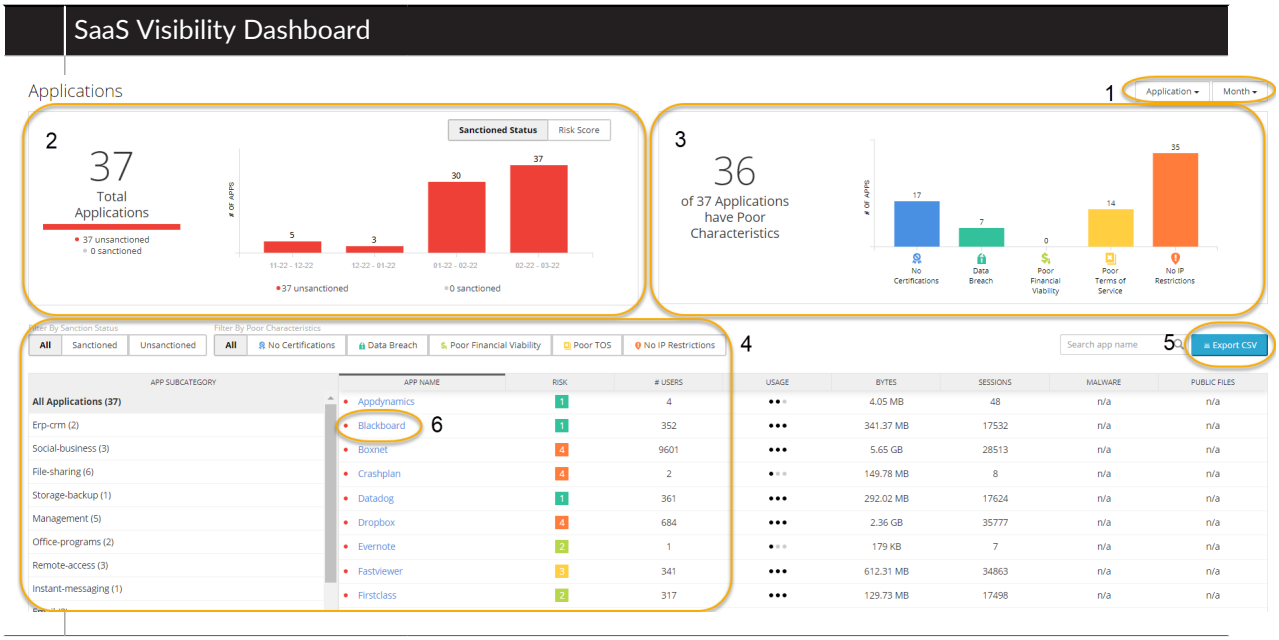


STEP 3 | Begin to View SaaS Application Usage on Prisma SaaS.

View SaaS Application Usage on Prisma SaaS

Wait for up to 24 hours after you connect Prisma SaaS to Cortex Data Lake to view details about data residing within enterprise-enabled SaaS applications and network traffic from firewall logs.

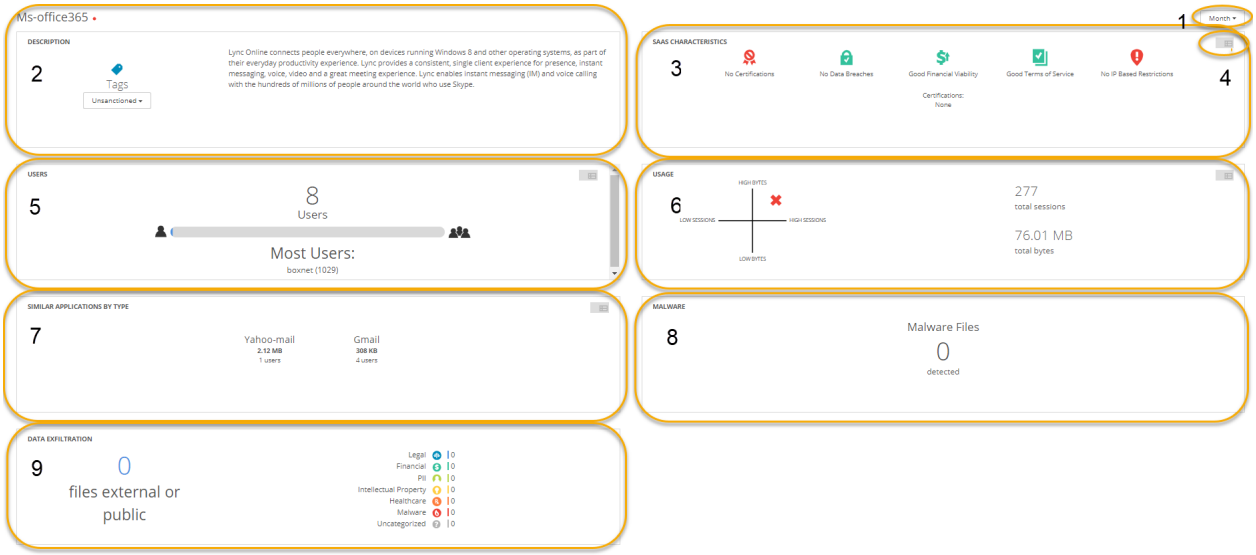
- Log in to Prisma SaaS, and click **Explore** > **SaaS Visibility**.



	SaaS Visibility Dashboard	
1	**Dashboard Filters**	The SaaS visibility dashboard allows you to filter applications by **Application** or **Bytes**, for the past **Month**, **Week**, or **Quarter**.
2	**Application**	Displays an interactive view of the total number of sanctioned and unsanctioned applications by **Sanctioned Status** or **Risk Score**.
3	**Characteristics**	Displays the number of applications or bytes with poor characteristics: • No Certifications • Data Breach history • Poor Financial Viability • Poor Terms of Service • No IP Restrictions
4	**All Applications**	Lists every sanctioned or unsanctioned application, by subcategory and App-ID, and can be filtered by Sanction Status or Poor Characteristics.
5	**Export CSV**	Export details for all applications into a CSV file.
6	**App Name**	Click the app name to view details (Description, SaaS Characteristics, Users, Usage, Similar Applications by Type, Malware, Data Exfiltration) by Week, Month or Quarter for the SaaS application.

- Click the **App Name** to view detailed application information populated from your Cortex Data Lake and Prisma SaaS.

App Detail View



1	**Dashboard Filter**	Filter the application details by Month, Week, or Quarter.

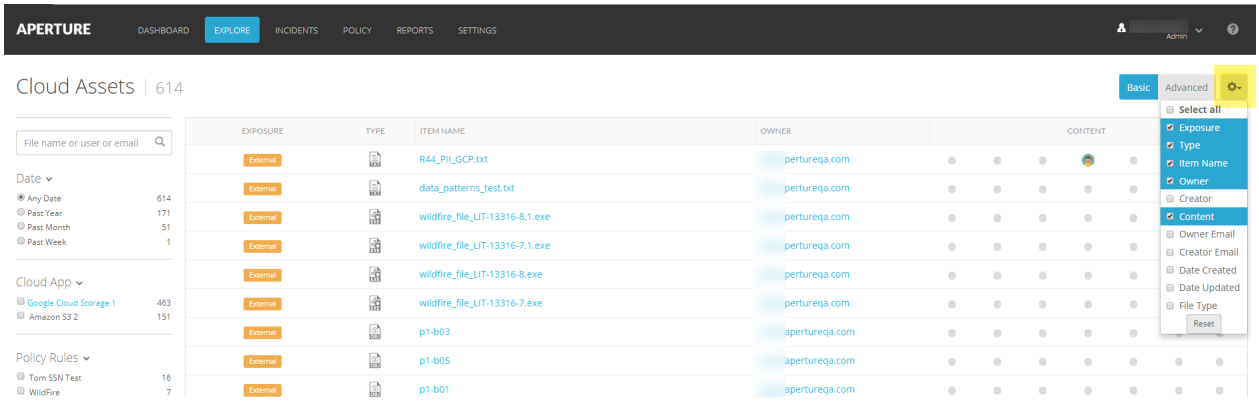
App Detail View		
2	**App Description**	Displays the application title, a sanctioned (grey) or unsanctioned (red) icon, app description populated from App-ID and the ability to tag the application **Sanctioned** or **Unsanctioned** on Prisma SaaS. This tag is local only to Prisma SaaS and will not be applied to the firewall.
3	**SaaS Characteristics**	View the Pass or Fail status for Certifications, Data Breaches, Financial Viability, Terms of Service, and IP Restrictions retrieved from the App-ID.
4	**View Icon**	Toggle between data visualization or table view to display the app details. The **Export CSV** link is available on the table view.
5	**Users**	Displays the number of users in comparison with the application with the most users. The table view displays a exportable list of usernames.
6	**Usage**	Displays the number of sessions and bytes transferred for the selected app in comparison to other sessions and bytes for other applications.
7	**Similar Applications by Type**	Displays the application, number of users and bytes of data transferred of similar applications.
8	**Malware**	Displays if any malware has been detected.
9	**Data Exfiltration**	Displays the total number of files exposed publicly or externally along with number of files in each classification. Click the total number of files to view the list of Assets.

Use Faceted Search to Filter Assets

In addition to the highlights from the Dashboard, Prisma SaaS provides visibility into all assets in your managed SaaS applications. Search provides you with different views to help you find the incidents that are most important to you. You can view incidents by user to see if any of your users (or external collaborators) have a history of misuse or you can view all incidents for a specific file type. You can also use search to simplify the remediation process and to determine if you should Fine-Tune Policy. For example, you can find PII violations with external exposure, assign issues to an administrator, and send an email to the owners—all in one streamlined workflow.

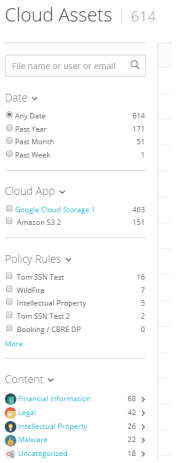
STEP 1 | Select **Explore** > **Assets** to view any scanned assets.

By default, Prisma SaaS displays the Exposure, Type, Item Name, Owner, and Content columns but you can add additional columns such as Creator, Owner Email, Creator Email, Date Created, Date Updated, and File Type.



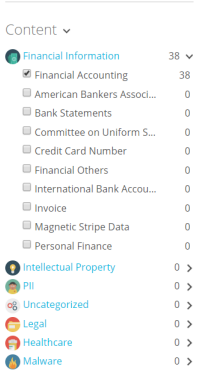
STEP 2 | Use the facets to narrow your search results.

Dropbox folders do not have metadata for the creation or updated date, preventing search filters other than Any Date to return these folders. However, you can still search for individual files within a folder by a creation or last modified date.



1. Select one or more of the following facets to create your search expression. With multiple filters, Prisma SaaS performs a logical AND search and rounds up the asset total in the search results.

- Enter the filename (or part of the filename), folder name, or email address in the **Search** box to find an item. To find specific users or Collaborators, enter their full email address.
- **Date**—The date range of the exposure. Choices include any date, past year, past month, and past week (default).
- **Cloud App** (instance name)—Assets associated with each instance of a cloud application.
- **Policy Rules**—Data pattern types available for scanning assets. Click to select the data patterns in which you are interested. For example, you can filter on assets that are sensitive documents with PII violations.
- **Content**—Lists the six predefined data pattern content categories, and **Uncategorized** for violations that are not associated with a specific data pattern.



- **Exposure Level**—Details about shared assets and who can access and view the asset.
- **Buckets**—Lists the number of assets associated to a bucket.
- **Shared With**—Select users or collaborators with access to shared assets. To see a list of shared assets, you can filter **Trusted Users** (those with internal domains), **Untrusted Users** (those with external domains), and **Anyone Except Trusted Users** (anyone other than a trusted user).
- **Top Owners**—Users who own the highest number of assets.
- **Top Creators**—Users who created the highest number of assets.
- **Shared with Domains**—Lists the domains with the highest number of sharing listed in order.
- **File Type**—File formats of the assets that reside in the cloud applications.

If you want investigate incidents associated with a specific cloud application, select Incidents > Assets, and select the cloud app from Cloud Apps to view a list incidents along with the policy rule violation.

STEP 3 | Download your current view into a **CSV** file.

When you download asset details to review offline, additional information such as external and internal collaborators, file size, and parent folder are included in the CSV file.

STEP 4 | Click **Advanced** to use RegEx to perform Advanced Searches.

Use Advanced Search

To perform an advanced search:

STEP 1 | Show the assets.

1. Select **Explore** > **Assets**.
2. Select **Advanced** to start an advanced search.

STEP 2 | Create your Use Advanced Search Expressions in the search box.

Your search expression is composed of a set of supported fields, operators, and values.

As you create your search expression, Prisma SaaS provides field name matching and syntax suggestions to help you complete the expression.

For **`policy.name`**, a list of existing policy names appears as you type so you can quickly pick the name from the list, instead of typing the full name.

If you want to view and sort search results in another application, such as Microsoft Excel, export that data to a CSV file.

STEP 3 | Take actions on the cloud assets that match your filtering criteria.

See Supported Applications with Remediation for a list of actions available.

1. Select the assets on which you want to take action.
   - Select specific assets in the display results.
   - To select all assets in the display results, select the Exposure column heading.
2. Select one or more of the following actions:
   - **Explore** to view details about the asset.
   - **Download File**.
   - **Delete Content**.
   - **Send Email** to the file owner. The email template automatically includes the email addresses of all selected assets.
   - **Notify via Webex Bot** to send a message using the Cisco Webex bot that you configured in Begin Scanning a Cisco Webex Teams App (Beta).
   - To Close Incidents, select a reason from the drop-down.
   - Assign an **Incident Category** to the asset. From the drop-down, select a category to apply; to create a new category see Customize the Incident Categories.
   - To Assign Incidents to Another Administrator, select an administrator from the drop-down.
   - **Add Note** to the asset. Adding a note allows you to provide context about your concern, give instructions, or supplement information about the asset before assigning to another administrator.

Use Advanced Search Expressions

In some cases, a faceted search will not provide you enough detail to find high priority incidents. To isolate important problems, it can help to match more than one rule or to ignore the incidents that match rules but that are not important to you. For these cases, you can perform an advanced search. Advanced search provides the same filters as a basic faceted search, but gives you more options to apply connectors and operators.

For example, if you have a company policy that considers social security numbers, tax information numbers, and credit card numbers to be sensitive data, you may need to search for all assets that contain any of these numbers and notify the owners.

An advanced search expression is composed of a set of supported fields, operators, and connectors. Fields and field values can include:

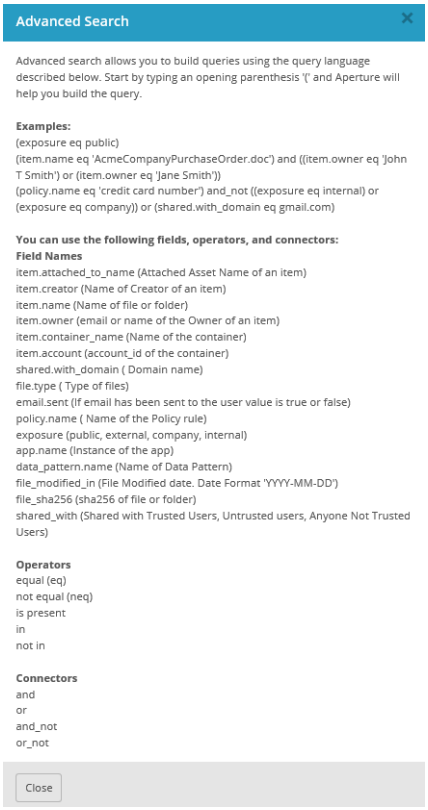
- **item.attached_to_name**—Attached asset name of an item.
- **item.creator**—Name of the creator of an item. The name can be partial.
- **item.creator_email**—Email of the creator of an item. The email address must be complete.
- **item.name**—Name of file or folder, such as techsupport.tgz.
- **item.owner**—Name of the owner of an item. The name can be partial.
- **item.owner_email**—Email of the owner of an item. The email address must be complete.
- **item.container_name**—Name of the container.
- **item.account**—Account ID of the container.
- **shared.with_domain**—Any domain name.
- **file.type**—File format supported by Prisma SaaS, such as TGZ. (See supported file types for details.)
- **email.sent**—If email has been sent to the user the value is true or false.
- **policy.name**—Name of a policy rule.
- **exposure**—**`Public`**, **`External`**, **`Internal`**, **`Company`**, or **`hasCustomURL`**.
- **app.name**—Name of any application instance, such as Google Drive Prod.
- **data_pattern.name**—Name of the data pattern.
- **file_modified_in**—File modification date with date format YYYY-MM-DD.
- **file_sha256**—sha256 of file or folder.
- **shared_with**—Shared with trusted users, untrusted users, or anyone not trusted users.

Operators define the relationship between a field and a value. Operators can include:

- **eq**—equals.
- **neq**—not equal.
- **is_present**—included (partial match).
- **in**—included.
- **not_in**—not included.

Connectors define the logic associated with groups of items. Connectors can include:

- **and**—logical AND operation.
- **or**—logical OR operation.
- **and_not**—AND is not.
- **or_not**—OR is not.



Combine fields, operators, and connectors based on the following syntax rules:

Syntax Rule	Example
Use parentheses to group items in an expression.	`(item.owner neq 'rjsmith@smith.com')`
Include field values in single quotes.	`(file.type eq 'PDF')`
Recognized keywords by Prisma SaaS and logical operators do not need quotes.	`(exposure eq public)`
Use comma-separated lists for multiple values.	`(file.type not_in 'PDF','PPT')`

The following are examples of advanced search expressions:

To Search for	Example
• Any asset owned by a user named msmith.	`(item.owner eq 'msmith')`
• Any asset with Public, External, or Company exposure that caused an email alert.	`(exposure neg internal) and (email.sent is true)`
• A file named “apple vs samsung.pdf” John T Smith or Jane Smith does not own.	`(item.name eq 'apple vs samsung.pdf') and ((owner neq 'John T Smith') or (owner neq 'Jane Smith'))`

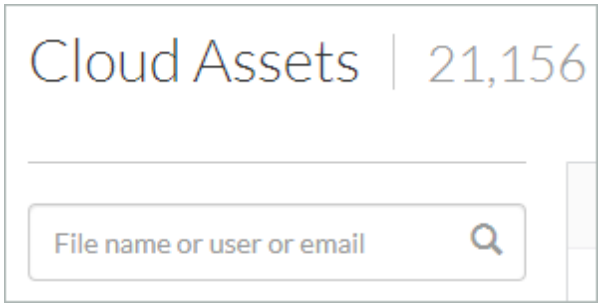
To Search for	Example
• Any asset that includes a credit card number and share on gmail.com or has Public or External exposure. Do not include assets with credit card numbers that have Internal or Company exposure.	`(policy.name eq 'credit card number') and not ((exposure eq internal) or (exposure eq company)) or (shared.with eq 'gmail.com')`

Export Search Results to CSV File

When you choose to download search results, such as incident and asset data, the service enables you to either download the data to a CSV file immediately or download the CSV file later after you receive an email notification with a download link.

Your ability to export data is directly tied to the number of records in your data set. Adhere to the following guidelines:

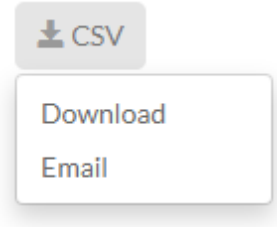
- Before you export data, apply filters to narrow your search and shrink your data set. Only include data that you need.
- Verify the number of records in your query by observing the record counter in the page header.



For a GDRP Report, there is no data set limit because the summary report is not based on records. The summary report includes as much data as the report needs to provide you actionable intelligence.

	Immediate Download Record Limit	Email Download Record Limit
Assets	100K	5M
Incidents	100K	5M
User Activity	100K	n/a
Quarantine	100K	n/a

STEP 1 | Click on the **Export CSV** link or **CSV** icon in the page.



STEP 2 | Select an export option.

- **Download** | **Download Now**—Immediately downloads the CSV file to your local drive if the file does not exceed the record limits outlined above.

- **Email**—Generates the CSV file that you request, then sends you a **Your file is ready email** notification with a link to download the CSV file (in `.zip`), if that file does not exceed the record limits outlined above.

  The download link is active for up to 30 days. For security reasons, you must log on as the user who initiated the request: if you forward the link to another user, the service denies that user file access.

Prisma SaaS Syslog and API Integration

You can now configure Prisma SaaS to interface with syslog servers and API clients. Prisma SaaS can push syslog information to external syslog servers and third-party API clients can pull log information from Prisma SaaS. Organizations that have standardized a specific Security Information and Event Management (SIEM) tool can leverage this feature for monitoring and data collection.

These topics describe how to configure Prisma SaaS for syslog and API client integration.

Prisma SaaS Syslog Integration

Syslog is a standard log transport mechanism that enables the aggregation of log data from different sources into a central repository for archiving. Prisma SaaS can forward every type of log it generates to an external syslog server. The Prisma SaaS Syslog feature requires TLS 1.0 (and above) communications protocol for connections between Prisma SaaS and the external syslog server. This topic describes how to configure syslog monitoring and includes a description of supported log types and log fields.

Configure Prisma SaaS Syslog Monitoring

Prisma SaaS supports the following log types:

- Incidents log
- Policy Violation log
- Remediation log
- Activity Monitoring log
- Admin Audit log

STEP 1 | Select **Settings** > **External Service**.

STEP 2 | Click **Add a Syslog Receiver** to create a Syslog server profile.

You can add only external service — forward logs to a syslog receiver or Add Your API Client App to Prisma SaaS.

STEP 3 | Enter a **Name** for the profile.

STEP 4 | **Add** the information Prisma SaaS requires to connect to it:

- **Name**—Unique name for the server profile.
- **Server IP**—IP address or fully qualified domain name (FQDN) of the syslog server.
- **Port**—The port number on which you send syslog messages. You must use the same port number for Prisma SaaS and the syslog server.
- **Facility**—Select a syslog standard value (for example, **LOG_USER**) to calculate the priority (PRI) field in your syslog server implementation. The PRI part of the syslog message represents the Facility and Severity of the message. Select the value that maps to how you use the PRI field to manage your syslog messages. Values can be **LOG_USER** or **LOG_LOCAL0** through **LOG_LOCAL7**. There is no default.
- **Message format**—Select the syslog message format to use: **BSD** (the default) or **IETF**. Traditionally, **IETF** format is used over TCP or SSL.

STEP 5 | Save your changes.

STEP 6 | On the Syslog server, make sure the TLS options in the syslog configuration file are set to:

```
peer-verify (optional-untrusted)
```

Syslog Field Descriptions

The following topics list the standard fields of each log type Prisma SaaS can forward to an external server, as well as the security levels, custom formats, and escape sequences. To help parsing, the delimiter is a comma and each field is a comma-separated value (CSV) string.

Incidents Log Fields

The incident log is generated when an incident is detected.

Field Name	Description
`detected_timestamp`	The time the incident was discovered in `YYYY-MM-DD HH:MM:SS` format with Augmented Backus-Naur Form (ABNF) to indicate the timezone.
`serial`	Serial number of the organization using the service (tenant).
`cloud_app_instance`	The instance name of the cloud application (not the type of cloud application).
`severity`	The severity of the incident valued between 0 and 5.
`incident_id`	Unique ID number for the incident.
`asset-id`	Unique ID number for the asset associated with the incident.
`item_name`	Name of the file, folder, email Subject, or user associated with the incident
`item_type`	`File`, `Folder`, or `User`
`item_owner`	The user who owns the asset identified in the incident.
`container_name`	The value is the `bucketname` for AWS S3, Google Cloud Platform, and Microsoft Azure assets. The value is `null` for the remaining apps.
`item_creator`	The user who created the asset identified in the incident.
`policy_rule_name`	The names of one or more policy rules (not policy type) that were matched.
`exposure`	The type of exposure associated with the incident. Values are `Public`, `External`, `Company`, or `Internal`.
`occurrences_by_rule`	Where applicable, the number of occurrences matched for the corresponding rule.
`state`	One of the following states:

Field Name	Description
	• Active • Remediated in cloud • Remediated by Prisma_SaaS • Remediated by <Admin_name> • Closed Business Justified • Closed Personal Content • Closed Risks mis-identified • Closed No reason given
collaborators	Any external or internal collaborators with access to view, edit, or download an asset.
datetime_edited	Last time the asset was updated.
incident_category	The category of the incident. For example, Personal or BusinessJustified.
incident_owner	The administrator assigned to the incident.
additional_notes	Any notes added by the administrator (first 20 bytes).
item_owner_email	Email address of the item owner or sender of email.
item_creator_email	Email address of the item creator.

Remediation Activity Log Fields

A remediation log is generated when an incident is manually remediated or if automatic remediation has been applied.

Field Name	Description
remediated_timestamp	Time the remediation action occurred. Values are in YYYY-MM-DD HH:MM:SS format.
serial	Serial number of the organization using the service (tenant).
cloud_app_instance	The instance name of the cloud application (not the type of cloud application) associated with the remediation of the incident.
severity	The policy violation or incident severity valued between 0 and 5.
incident_id	The unique ID number for the incident. Can be null (no value).
asset_id	The unique ID number for the asset associated with the remediation of the incident.
item_name	The name of the file, folder, or user associated with the remediation of the incident.

Field Name	Description
item_type	File, Folder, or User
item_owner	The user who owns the asset associated with the remediation.
container_name	The value is the bucketnamefor AWS S3, Google Cloud Platform, and Microsoft Azure assets. The value is null for the remaining applications.
item_creator	The user who created the asset associated with the remediation.
policy_rule_name	The names of one or more policy rules (not policy type) that were matched.
FUTURE_USE	Not currently implemented
action_taken	The remediation action taken on Prisma SaaS. (AdminQuarantine, User Quarantine, or Remove Public Links)
action_taken_by	The user who performed the remediation. For automated remediation, the value is Aperture.
item_owner_email	Email address of the item owner.
item_creator_email	Email address of the item creator.

Policy Violation Log Fields

The policy violation log is generated when an asset matches a policy rule.

Field Name	Description
violation_timestamp	Time the policy violation occurred. Values are in YYYY-MM-DD HH:MM:SS format.
serial	Serial number of the organization using the service (tenant).
cloud_app_instance	The instance name of the cloud application (not the type of cloud application) associated with the policy violation
severity	The policy violation severity valued between 0 and 5.
incident_id	The unique ID number for the incident. Can be null (no value).
asset_id	The unique ID number for the asset associated with the policy violation
item_name	The name of the file, folder, or user associated with the policy violation
item_type	File, Folder, or User

Field Name	Description
item_owner	The user who owns the asset associated with the policy violation.
item_creator	The user who created the asset identified in the policy violation.
policy_rule_name	The name of the policy rule that triggered the violation.
FUTURE_USE	Not currently implemented
action_taken	Action taken to remedy the policy violation. For example, Log only, or Send Administrator Alert
action_taken_by	The cloud app user who took action to remediate the policy violation. For automated remediation, the value is Aperture.

Activity Monitoring Log Fields

The activity monitoring log is generated when a user activity rule is matched.

Field Name	Description
timestamp	The time the activity occurred. Values are in YYYY-MM-DD HH:MM:SS format.
serial	Serial number of the organization using the service (tenant).
cloud_app_instance	The instance name of the cloud application (not the type of cloud application) associated with the activity.
target2_name	The name of the file, folder, or user associated with the activity.
target2_type	File, Folder, or User
user	The cloud app user who performed the activity.
source_ip	The source IP address where the activity was performed.
location	The location where the activity was performed.
action	The activity that occurred. For example, Login or Upload.
target_name	The field name updated or target of the activity.
target_type	The target type. For example, FieldName, Report, or File.

Admin Audit Log Fields

The admin audit log is generated when a Prisma SaaS administrator performs an action such as the remediation of an incident, creating a new policy rule, or adding internal or external collaborators.

Field Name	Description
`event_date`	The time the configuration change occurred. Values are in `YYYY-MM-DD HH:MM:SS` format.
`serial`	Serial number of the organization using the service (tenant).
`log_type`	The event type recorded. (`Admin Audit`)
`admin_id`	The email account associated with the Prisma SaaS administrator.
`admin_role`	Role assigned to the administrator: `super_admin`, `admin`, `limited_admin`, or `read_only`
`ip`	The IP address of the administrator who performed the action.
`event_type`	Type of configuration change:`settings`, `policy`, `remediation`, `login`
`item_type`	The type of item in the configuration that changed: `user`, `apps`, `settings`, `content_policy`, `file`, `risk`, `general_settings`
`item_name`	The name of the item that changed in the configuration.
`field`	The name of the field associated with the configuration change.
`action`	The configuration change activity that occurred: `create`, `edit`, `delete`, `login`, `logout`
`resource_value_old`	The value before the configuration change occurred.
`resource_value_new`	The value after the configuration change occurred.
`FUTURE_USE`	Not currently implemented
`FUTURE_USE`	Not currently implemented

Prisma SaaS API Integration

Prisma SaaS includes a Public REST API to give you the ability to write API clients to integrate with Prisma SaaS and collect log events.

Prisma SaaS (formerly known as Aperture) is hosted in the United States (aperture.paloaltonetworks.com), EMEA (aperture-eu.paloaltonetworks.com) and APAC (aperture-apac.paloaltonetworks.com).

Topics include:

- Add Your API Client App to Prisma SaaS
- API Client Authentication
- Public API References

Add Your API Client App to Prisma SaaS

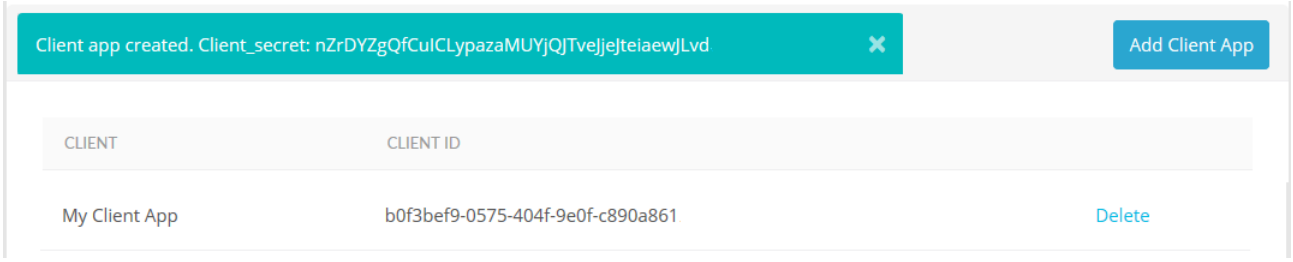
You can write a third-party API client and the API client will use OAuth to authenticate a connection to Prisma SaaS.

STEP 1 | Select **Settings** > **External Service**.

STEP 2 | Click **Add Client App** to register an API client.

STEP 3 | Enter a unique **Name** for the API client.

STEP 4 | **Save** your changes to grant Prisma SaaS the ability to generate and display a Client ID and a Client Secret. The Client Secret displays in a pop up and after dismissal, you cannot access the Client Secret again. Use the Client ID and Client Secret to authenticate your API client to Prisma SaaS.



STEP 5 | (Optional) To delete a client, click **Delete**.

API Client Authentication

For the API client to authenticate to Prisma SaaS, you must provide the Client ID and Client Secret generated when you registered the API client to Prisma SaaS and configure the client to retrieve an OAuth token. All requests must use the host **`api.aperture.paloaltonetworks.com`** with **`https`** (for example, **`https://api.aperture.paloaltonetworks.com`**).

- Retrieve a Token
- Authentication Errors

Retrieve a Token

The API client can a retrieve a token for Prisma SaaS using **POST** request to the **/oauth/token** endpoint. To request a token, Prisma SaaS submits the request with the OAuth2 client credentials.

Request Headers

Name	Description
Authorization	Basic auth header containing the Client ID and Client Secret delimited with a colon (:) Base 64 encoded. Example: **Base64(acme:acmesecret)**

Request Parameters

Parameter	Description
grant_type	OAuth2 grant type. Only client credentials are supported.
scope	Scopes the app is requesting

Example Request

```
POST /oauth/token HTTP/1.1
Authorization: Basic YWNtZTphY21lc2VjcmV0
Accept: application/json
Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1
Host: api.aperture.paloaltonetworks.com

grant_type=client_credentials&scope=api_access
```

Example Response

```
HTTP/1.1 200 OK

{
"access_token" :
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZSI6WyJhcGlfYWNjZXNzIl0sImV4cCI6MTQ5MTUy
MzA4OCwianRpIjoiZDY2YWJmYWQtOGMzYy00MGQxLThjMWYtOTFjYzBlMTkzMWYxIiwidGVuYW50IjoidGVzdC
B0ZW5hbnQiLCJjbGllbnRfaWQiOiJhY21lIn0.vxao73NJcehYkngrI9WvHIxugbhDzOEWDBbR4TS99Eg",
"token_type" : "bearer",
"expires_in" : 7199,
"scope" : "api_access",
"tenant" : "test tenant",
"jti" : "d66abfad-8c3c-40d1-8c1f-91cc0e1931f1"
}
```

Response Fields

The following table displays the response fields used when you attempt to get a token.

Path	Type	Description
access_token	String	Access token for requests
token_type	String	Type of token
expires_in	Number	Number of seconds until the token expires. No value means it does not expire.
scope	String	Scopes granted
jti	String	Token ID
tenant	String	Tenant name

Authentication Errors

No Basic Auth Header

Not including the basic auth header when retrieving a token results in a 401 response. To try again, see Retrieve a Token.

- **Example Request**

```
$ curl 'https://api.aperture.paloaltonetworks.com/oauth/token' -i -X POST -H
 'Accept:
application/json' -H 'Content-Type: application/x-www-form-urlencoded;
 charset=ISO-
8859-1' -d 'grant_type=client_credentials&scope=api_access'
```

- **Example Request Body**

```
POST /oauth/token HTTP/1.1
Accept: application/json
Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1
Host: api.aperture.paloaltonetworks.com

grant_type=client_credentials&scope=api_access
```

- **Example Response**

```
HTTP/1.1 401 Unauthorized

{
"error" : "unauthorized",
"resolution" : "Please submit valid credentials.",
"error_description" : "Invalid credentials"
}
```

Invalid Credentials

Providing invalid credentials will result in a 401 response. To try again, see Retrieve a Token

- **Example Request**

```
$ curl 'https://api.aperture.paloaltonetworks.com/oauth/token' -i -X POST -H
 'Accept:
application/json' -H 'Content-Type: application/x-www-form-urlencoded;
 charset=ISO-
8859-1' -d 'grant_type=client_credentials&scope=api_access'
```

- **Example Request Body**

```
POST /oauth/token HTTP/1.1
Accept: application/json
Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1
Host: api.aperture.paloaltonetworks.com

grant_type=client_credentials&scope=api_access
```

- **Example Response**

```
HTTP/1.1 401 Unauthorized

{
"error" : "unauthorized",
"resolution" : "Please submit valid credentials.",
"error_description" : "Invalid credentials"
}
```

Token Expiration

Performing a request with an expired token results in a `401` response. To try again, see Retrieve a Token.

- **Example Request Body**

```
POST /oauth/token HTTP/1.1
Accept: application/json
Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1
Host: api.aperture.paloaltonetworks.com

grant_type=client_credentials&scope=api_access
```

- **Example Response**

```
HTTP/1.1 401 Unauthorized

{
"error": "invalid_token",
"resolution": "Please retrieve a new token.",
"error_description": "Authentication token was invalid."
}
```

Public API References

Use these HTTP Request Methods and Log Events API to retrieve events.

- HTTP Request Methods and Status Codes
- Log Events API

HTTP Request Methods and Status Codes

HTTP Request Methods

These set of request methods can be used to retrieve or modify resources on Prisma SaaS.

Verb	Usage
GET	Retrieves a resource
POST	Creates a new resource
PUT	Replaces an existing resource
DELETE	Deletes an existing resource

HTTP Status Codes

The following is a list of the HTTP Status Codes Prisma SaaS will return in response to the requests listed above.

Status Code	Usage
`200 OK`	The server successfully processed the request.
`201 Created`	The server successfully processed the request and created a new resource.
`204 No Content`	The server successfully processed the request, but did not return any content.
`400 Bad Request`	The server cannot process the request due to a client error (for example, validation).
`401 Unauthorized`	The server cannot process the request because it lacks valid authentication credentials for the target resource.
`403 Forbidden`	The server refused to authorize the request.
`404 Not Found`	The requested resource could not be found.

Log Events API

A registered API client on Prisma SaaS can long poll the log events endpoint to retrieve events as they occur. There are five types of log events available:

- Activity Monitoring
- Incidents
- Remediation
- Policy Violation

- Admin Audit

Get Events

A **GET** request to the **/api/v1/log_events** endpoint with **api_access** scope is used to access the client's event stream. One event will be returned for each call or nothing when there is a Request Timeout.

Example Request

```
$ curl 'https://api.aperture.paloaltonetworks.com/api/v1/log_events' -i -H
'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZSI6WyJhcGlfYWNjZXNzIl0sImp0aSI6IjA5ZjljN
DVkLTA1NTYtNDY4MS05YWFhLWM4MGNiNWQ5ZjRiYSIsInRlbmFudCI6InRlc3QgdGVuYW50IiwiY2xpZW50X2l
kIjoiYWNtZSJ9.lQpl3taZros7xzQNVMRaOy7KIrKGkwNKmTPq667kJUQ' -H 'Accept:
application/json'
```

Example Request Body

```
GET /api/v1/log_events HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZSI6WyJhcGlfYWNjZXNzIl0sImp0aSI6IjA5ZjljN
DVkLTA1NTYtNDY4MS05YWFhLWM4MGNiNWQ5ZjRiYSIsInRlbmFudCI6InRlc3QgdGVuYW50IiwiY2xpZW50X2l
kIjoiYWNtZSJ9.lQpl3taZros7xzQNVMRaOy7KIrKGkwNKmTPq667kJUQ
Accept: application/json
Host: api.aperture.paloaltonetworks.com
```

Activity Monitoring

Example Response

```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Application-Context: public_api:test:0
Content-Type: application/json;charset=UTF-8
```

```
Transfer-Encoding: chunked
Date: Fri, 17 Feb 2017 00:18:59 GMT
Content-Length: 361
{
"log_type" : "activity_monitoring",
"item_type" : "File",
"item_name" : "My File",
"user" : "John Smith",
"source_ip" : "10.10.10.10",
"location" : "Somewhere, USA",
"action" : "delete",
"target_name" : null,
"target_type" : null,
"serial" : "mySerial",
"cloud_app_instance" : "My Cloud App",
"timestamp" : "2017-02-17T00:18:58.961Z"
}
```

Response Fields

Path	Type	Description
`log_type`	String	Event type
`item_type`	String	Item type (`File`, `Folder`, or `User`)
`item_name`	String	Name of the file, folder, or user associated with the event.
`user`	String	The cloud app user that performed the action
`source_ip`	String	Original session source IP address
`location`	String	Location of the cloud app user that performed the event.
`action`	String	Action performed
`target_name`	Null	Target name

Path	Type	Description
target_type	Null	Target type
serial	String	Serial number of the organization using the service (tenant).
cloud_app_instance	String	Cloud app name (not cloud app type).
timestamp	String	ISO8601 timestamp to show when the event occurred.

Incidents

Example Response

```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Application-Context: public_api:test:0
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 17 Feb 2017 00:18:58 GMT
Content-Length: 520
{
"log_type" : "incident",
"item_type" : "File",
"item_name" : "My File",
"asset_id" : "ce7c9ed11e6f4891ae73c1601af7f741",
"item_owner" : "John Smith",
"container_name": "test-container",
"item_creator" : "John Smith",
"exposure" : "public",
"occurrences_by_rule" : 5,
```

```
"serial" : "mySerial",
"cloud_app_instance" : "My Cloud App",
"timestamp" : "2017-02-17T00:18:58.347Z",
"incident_id" : "9610efdcd8a74a259bf031843eac0309",
"policy_rule_name" : "PCI Policy",
"incident_category" : "Testing",
"incident_owner" : "John Smith"
"item_owner_email": "owner@email-domain.com",
"item_creator_email": "owner@email-domain.com",
}
```

Response Fields

Path	Type	Description
`asset_id`	String	Unique ID number for the asset identified as a risk.
`cloud_app_instance`	String	Cloud app name (not cloud app type)
`collaborators`	String	List of collaborators for file, or recipients of email
`container_name`	String	The value is the `bucket name` for AWS S3, Google Cloud Platform, and Microsoft Azure assets. The value is `null` for the remaining apps.
`datetime_edited`	String	Last time file was edited
`exposure`	String	Exposure level (`Public`, `External`, `Company`, or `Internal`)
`incident_category`	String	The category of the incident. For example, `Personal` or `Business Justified`.
`incident_id`	String	Unique ID number for the incident
`item_owner`	String	The user who owns the asset identified as a risk
`item_creator`	String	The user who created the asset identified as a risk.
`item_creator_email`	String	Email address of the item creator.
`item_name`	String	Name of the file, folder, email subject, or user associated with the event.

Path	Type	Description
`incident_owner`	String	The administrator assigned to the incident.
`item_owner_email`	String	Email address of the item owner.
`item_type`	String	Item type (`File`, `Folder`, or `User`)
`log_type`	String	Event type
`occurrences_by_rule`	Number	Number of times the asset violated the policy.
`policy_rule_name`	String	The names of one or more policy rules (not policy types) that were matched.
`serial`	String	Serial number of the organization using the service (tenant)
`severity`	Number	The incident severity. Values are 0 to 5.
`timestamp`	String	ISO8601 timestamp to show when the event occurred

Remediation

Example Response

```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
X-Application-Context: public_api:test:0
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 17 Feb 2017 00:18:56 GMT
Content-Length: 468
{
"log_type" : "remediation",
```

```
"item_type" : "File",
"item_name" : "My File",
"asset_id" : "ce7c9ed11e6f4891ae73c1601af7f741",
"item_owner" : "John Smith",
"item_creator" : "John Smith"
"container_name": "test-container",
"action_taken" : "quarantine",
"action_taken_by" : "John Smith",
"serial" : "mySerial",
"cloud_app_instance" : "My Cloud App",
"timestamp" : "2017-02-17T00:18:55.581Z",
"incident_id" : "9610efdcd8a74a259bf031843eac0309",
"policy_rule_name" : "PCI Policy"
"item_owner_email": "owner@email-domain.com",
"item_creator_email": "owner@email-domain.com",
}
```


Response Fields

Path	Type	Description
`log_type`	String	Event type
`item_type`	String	Item type (`File`, `Folder`, or `User`)
`item_name`	String	Name of the file, folder, or user associated with the event.
`serial`	String	Serial number of the organization using the service (tenant)
`cloud_app_instance`	String	Cloud app name (not cloud app type)
`timestamp`	String	ISO8601 timestamp to show when the remediation occurred
`incident_id`	String	Unique ID number for the remediated incident (risk)
`asset_id`	String	Unique ID number for the remediated asset

Path	Type	Description
item_owner	String	The user who owns the remediated asset
container_name	String	The value is the bucket name for AWS S3, Google Cloud Platform, and Microsoft Azure assets. The value is null for the remaining apps.
item_creator	String	The user who created the remediated asset
policy_rule_name	String	The names of one or more policy rules (not policy types) that were matched
action_taken	String	The action taken to remediate (Admin Quarantine, UserQuarantine, or Remove Public Links)
action_taken_by	String	The cloud app user who took the remediation action. For automated remediation, the value is Aperture.
item_owner_email	String	Email address of the item owner.
item_creator_email	String	Email address of the item creator.

Policy Violation

Example Resposne

```
HTTP/1.1 200 OK
{
"log_type" : "policy_violation",
"severity" : 3.0,
"item_type" : "File",
"item_name" : "My File",
"item_owner" : "John Smith",
"item_creator" : "John Smith",
"action_taken" : "download",
"action_taken_by" : "John Smith",
"asset_id" : "ce7c9ed11e6f4891ae73c1601af7f741",
"serial" : "serial",
"cloud_app_instance" : "My Cloud App",
```

```
"timestamp" : "2017-01-06T19:04:06Z",
"policy_rule_name" : "Policy Rule",
"incident_id" : "9610efdcd8a74a259bf031843eac0309"
"item_owner_email": "owner@email-domain.com",
"item_creator_email": "owner@email-domain.com",
```

Response Fields

Path	Type	Description
`log_type`	String	Event type
`item_type`	String	Item type (`File`, `Folder`, or `User`)
`item_name`	String	Name of the file, folder, or user associated with the event.
`serial`	String	Serial number of the organization using the service (tenant)
`cloud_app_instance`	String	Cloud app name (not cloud app type)
`timestamp`	String	ISO8601 timestamp to show when the policy violation occurred
`incident_id`	String	Unique ID number for the policy violation incident (risk)
`asset_id`	String	Unique ID number for the asset which violated the policy
`item_owner`	String	The user who owns the asset which violated the policy
`item_creator`	String	The user who created the asset which violated the policy
`policy_rule_name`	String	The names of one or more policy rules (not policy types) that were matched
`action_taken`	String	Action taken to fix the policy violation. For example, `Alerted Admin`, `Removed PublicLinks`, `Quarantine`, or `EmailOwner`
`action_taken_by`	String	The cloud app user who took the action. For automated remediation, the value is Aperture.
`severity`	Number	The incident severity. Values are 0 to 5.

Path	Type	Description
item_owner_email	String	Email address of the item owner. This value is null for now.
item_creator_email	String	Email address of the item creator. This value is null for now.

Admin Audit

Example Response

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 380
x-response-time: 297ms
{
"log_type" : "admin_audit",
"admin_id" : "admin id",
"admin_role" : "admin role",
"ip" : "ip address",
"event_type" : "event type",
"item_type" : "File",
"item_name" : "My File",
"field" : "field",
"action" : "action",
"resource_value_old" : "old val",
"resource_value_new" : "new val",
"timestamp" : "2017-04-06T21:35:10.025Z",
"serial" : "mySerial"
}
```

Response Fields

Path	Type	Description
log_type	String	Event type

Path	Type	Description
`timestamp`	String	ISO8601 timestamp to show when the event occurred
`serial`	String	Serial number of the organization using the service (tenant)
`admin_id`	String	Email account associated with the administrative user
`admin_role`	String	Role assigned to the administrative user: `super_admin`, `admin`, `limited_admin`, or `read_only`
`ip`	String	IP address of the administrative user who performed the action.
`event_type`	String	Type of configuration change event: `settings`, `policy`, `remediation`, `login`
`item_type`	String	The type of item in the configuration that changed: `user`, `apps`, `settings`, `content_policy`, `file`, `risk`, `general_settings`
`item_name`	String	Name of the item that changed in the configuration.
`field`	String	Name of the field associated with the configuration change.
`action`	String	The configuration change activity that occurred: `create`, `edit`, `delete`, `login`, `logout`
`resource_value_old`	String	Value before the configuration change occurred.
`resource_value_new`	String	Value after the configuration change occurred.

Request Timeout

Requests time out after 20 seconds and an http response with code `204` is returned. After receiving the response, you can initiate a new request.

Example Request

```
$ curl 'https://api.aperture.paloaltonetworks.com/api/v1/log_events' -i -H
'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZSI6WyJhcGlfYWNjZXNzIl0sImp0aSI6IjA5ZjljN
```

```
DVkLTA1NTYtNDY4MS05YWFhLWM4MGNiNWQ5ZjRiYSIsInRlbmFudCI6InRlc3QgdGVuYW50IiwiY2xpZW50X2l
kIjoiYWNtZSJ9.lQpl3taZros7xzQNVMRaOy7KIrKGkwNKmTPq667kJUQ' -H 'Accept:
application/json'
```

Example Request Body

```
GET /api/v1/log_events HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZSI6WyJhcGlfYWNjZXNzIl0sImp0aSI6IjA5ZjljN
DVkLTA1NTYtNDY4MS05YWFhLWM4MGNiNWQ5ZjRiYSIsInRlbmFudCI6InRlc3QgdGVuYW50IiwiY2xpZW50X2l
kIjoiYWNtZSJ9.lQpl3taZros7xzQNVMRaOy7KIrKGkwNKmTPq667kJUQ
Accept: application/json
Host: api.aperture.paloaltonetworks.com
```

Example Response

```
HTTP/1.1 204 No Content
Content-Type: application/json; charset=utf-8
x-response-time: 1019ms
```

There is no response body in the response of a request timeout.

Connect Prisma SaaS to Directory Services (Beta)

Connecting your enterprise directory service to Prisma SaaS allows you to retrieve information on user groups and group membership from your centralized repository of users and groups in your organization. With the combination of Prisma SaaS and your directory service, you can choose to selectively include or exclude user groups when scanning assets in the supported application. If you need to exclude a user group due to differences in data privacy rules or have private assets to exclude from scanning, connecting a directory service and enabling selective scanning will address this need.

Begin Selective Scanning Using Azure Active Directory Groups

Prisma SaaS allows you to integrate with an Azure Active Directory to manage cloud-based identity, and access management service. Once Microsoft AD connects, Prisma SaaS retrieves your Azure AD group information, enabling you to select which groups to include or exclude from global scan settings, policy rules, and monitor for risks.

Before you can begin scanning your cloud app, you need to collect information from your Azure AD and select which groups to include or exclude. An example of how to use selective scanning with an application would be in the case of needing to exclude a group with different privacy rules than another group. Another example would be in a case where you need to exclude users within a group due to owning confidential assets.

To begin scanning your Azure AD groups, you need to register an application one of two ways —

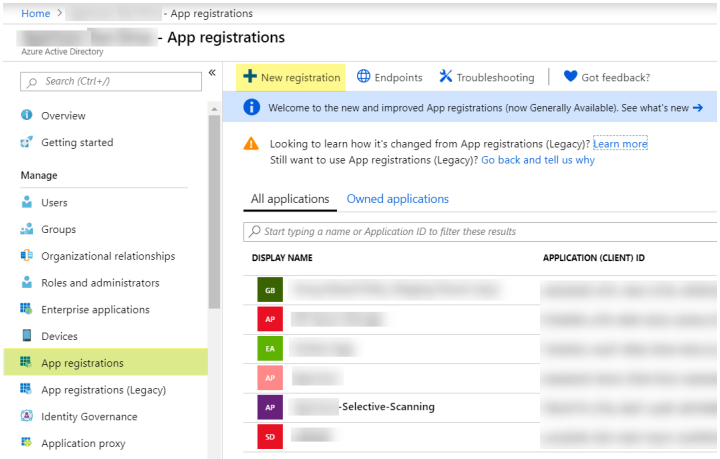
- App registration on Azure Active Directory
- App registration (Legacy) on Azure Active Directory

Register an application on Azure Active Directory

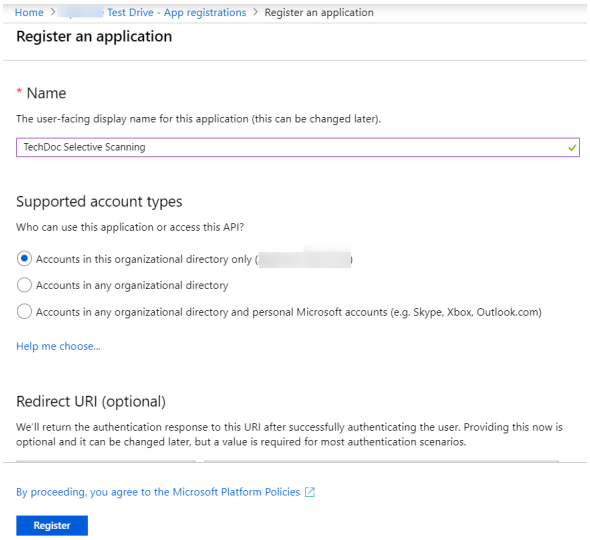
- Gather information needed to connect Azure AD to Prisma SaaS.

  You need the **Directory ID**, **Application ID**, and **Application Key** to establish a connection between Prisma SaaS and Azure Active Directory, to retrieve user group and membership information.

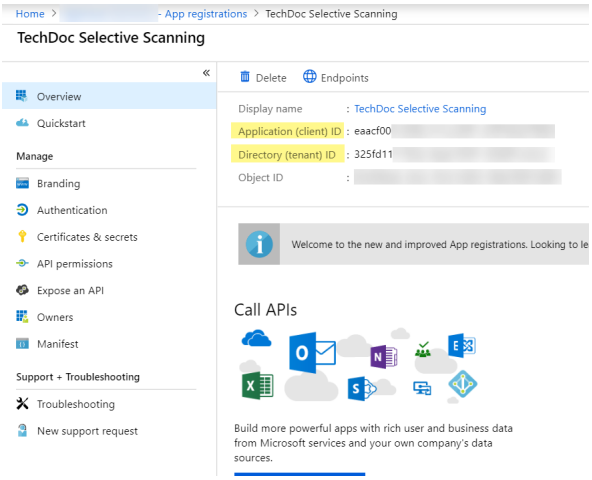
  1. Log in to Microsoft Azure and select **Azure Active Directory** > **App registrations** > **New registration**.



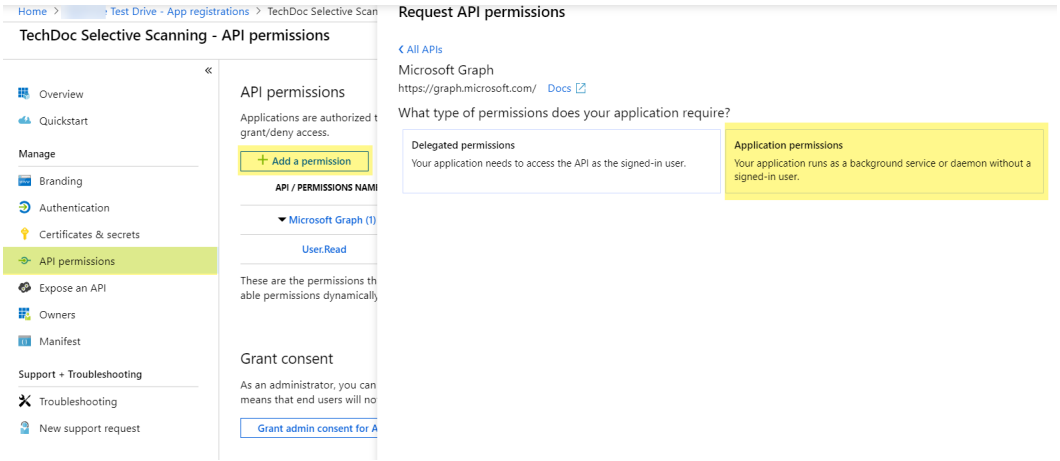
  2. Enter a **Name**, select **Accounts in this organizational directory only**, and click **Register**.



3. Copy the **Application (client) ID**.
4. Copy the **Directory (tenant) ID**.



5. Click **API permissions** > **Add a permission** > **Microsoft Graph** > **Application permissions**

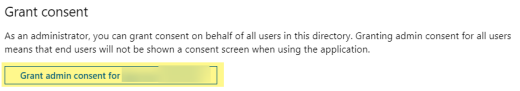


6. Select **Directory** > **Directory.Read.All**.

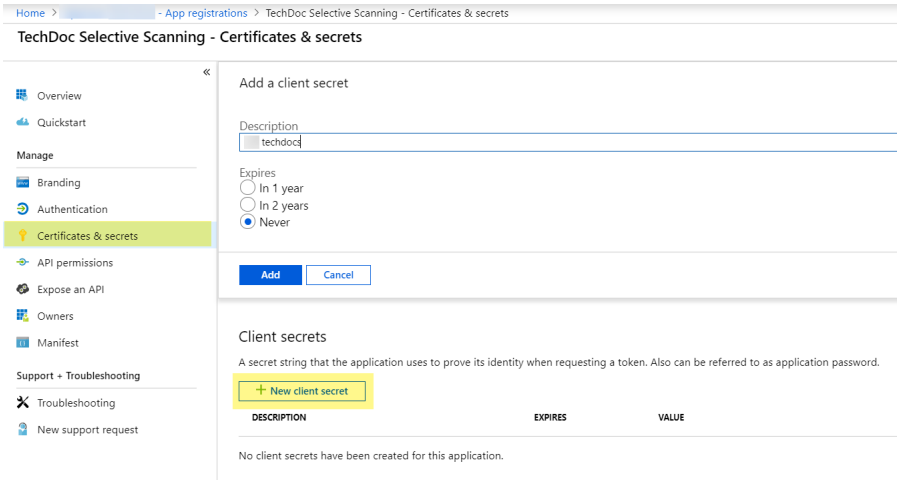
   Enable permissions to read directory data to allow Prisma SaaS to connect to the Azure AD application to read users, groups, and apps in the organization's directory.

7. Select **Group** > **Group.Read.All** and **Add permissions**.

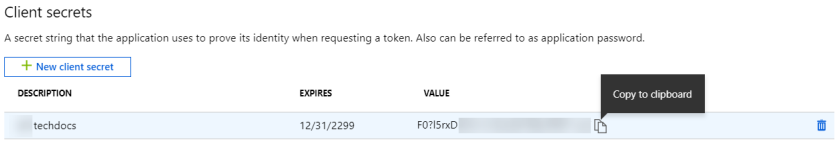
   Enable permissions to read all groups to allow Azure Active Directory to list groups, read their properties and membership, and enable Prisma SaaS to populate a list of groups to scan.
8. Click **Grant consent** and click **Yes** to confirm permission change.



9. Select **Certificates & secrets** > **New client secret**, enter a **Description**, select an expiration, and click **Add**.



10. Copy the unique **Client secret** (Prisma SaaS Application Key).



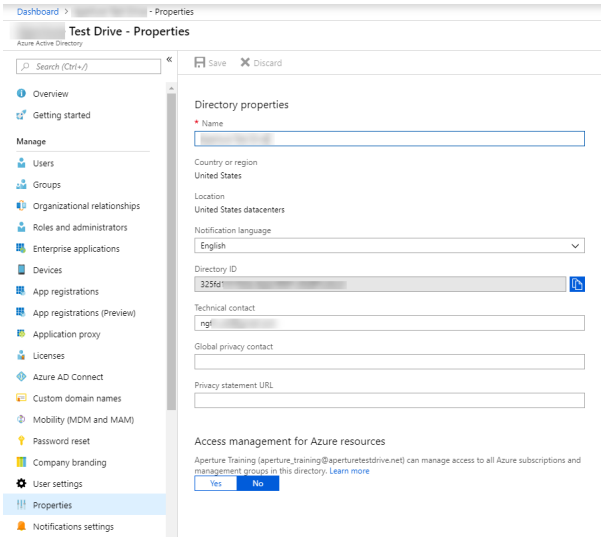
- Connect Azure Active Directory to Prisma SaaS.

Register an application (Legacy) on Azure Active Directory

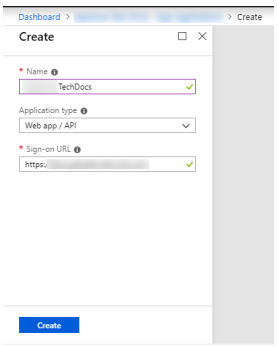
- Complete new and improved app registration on Azure Active Directory.

  You need the **Directory ID**, **Application ID**, and **Application Key** to establish the connection between Prisma SaaS and Azure Active Directory, to retrieve user group and membership information.

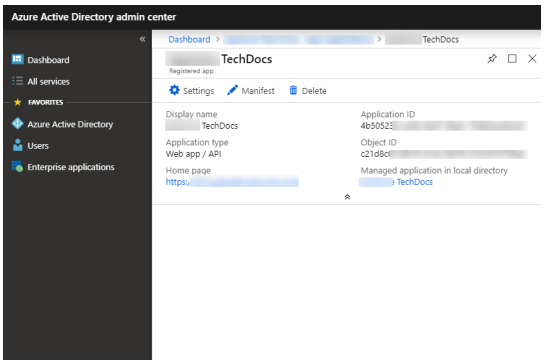
  1. Log in to Microsoft Azure, select **Azure Active Directory** > **Properties** and copy the **Directory ID**.



2. Select **App registrations** > **New application registration** and enter in **Name** and **Sign-on URL**.

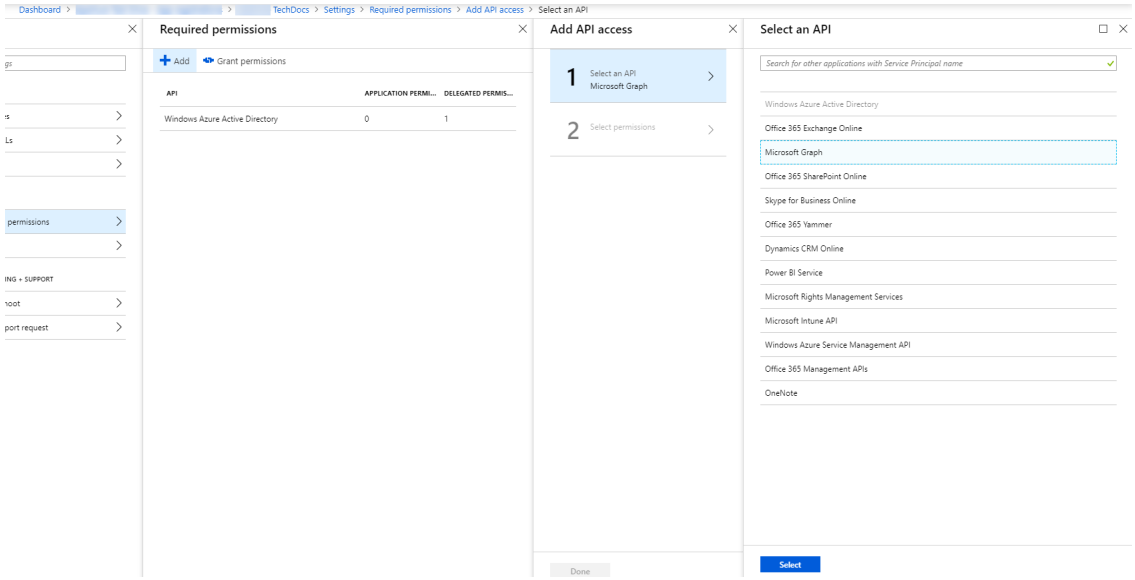


3. Click **Create**.
4. Copy the **Application ID**.

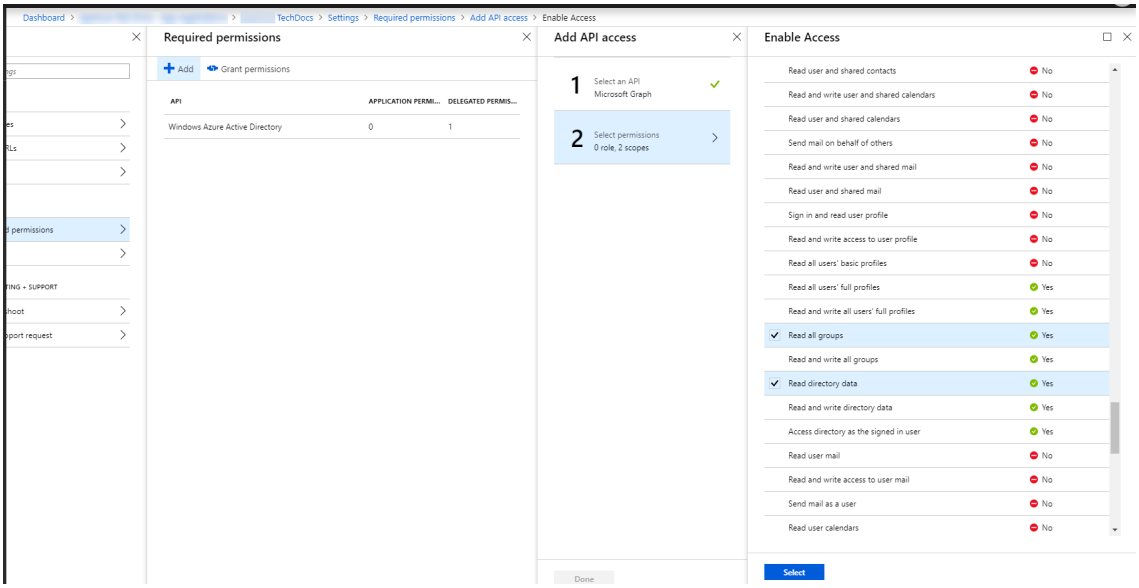


5. Select **Settings** > **Required Permissions** > **Add** > **Select an API** > **Microsoft Graph**.

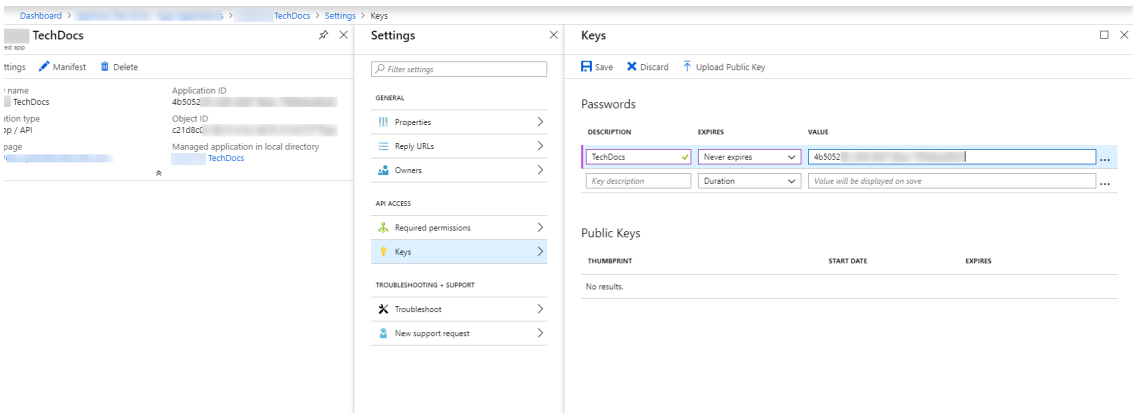
   To scan groups, permissions to Read all groups, and Read directory data need to be added. Read all groups allows Azure Active Directory to list groups, read their properties, and group memberships. Read directory data enables Azure Active Directory to read users, groups, and apps in the organization's directory.



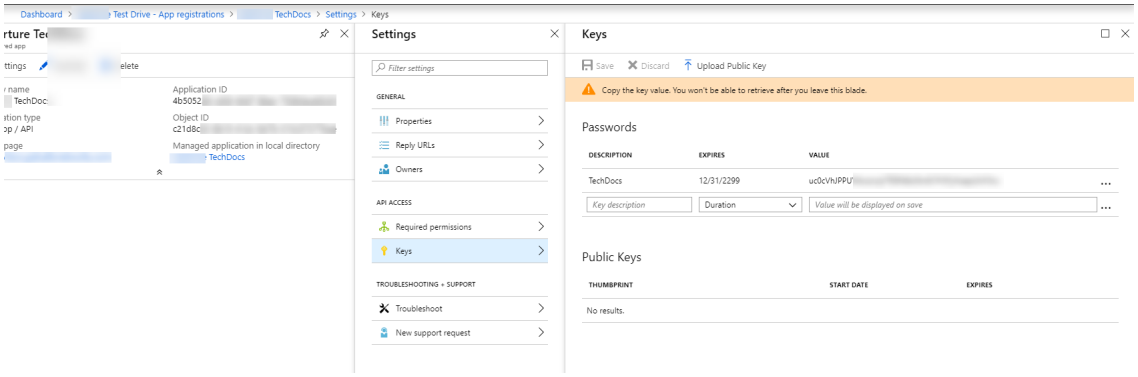
6. Click **Select** to open the **Enable Access** list, and choose **Read all groups** and **Read directory data**.



7. Click **Select** to enable access and **Done** to add permissions.
8. Select **Keys**, enter a **Description**, select a **Duration**, and paste the **Application ID**.



9. Click **Save** and copy the Application Key.

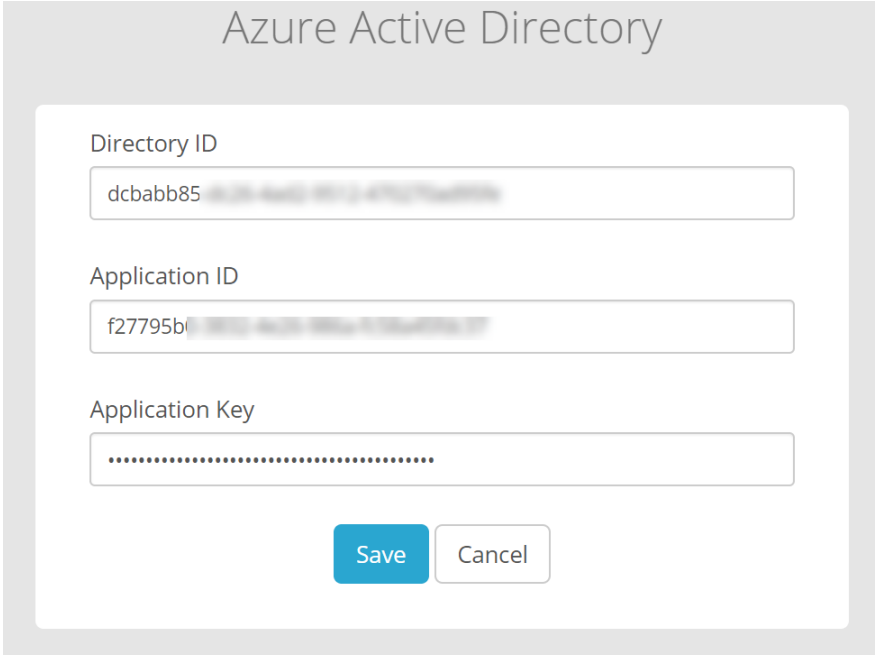


Connect Azure Active Directory to Prisma SaaS

STEP 1 | Connect Azure AD on Prisma SaaS to populate groups to scan.

Ensure the Azure AD role you are connecting to Prisma SaaS has administrator privileges.

1. Log in to Prisma SaaS.
2. Select **Settings** > **Directory Services** > **Connect New** .
3. Select Azure Active Directory and enter the **Directory ID**, **Application ID**, and **Authentication Key**.



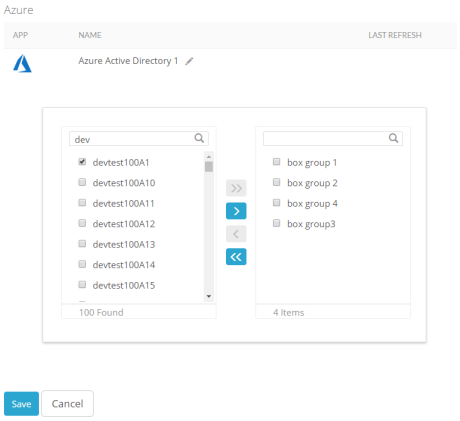
4. Click **Save** to authenticate Azure Active Directory and retrieve the group lists and membership information.

   You can give your Azure AD instance a descriptive name other than the default name which is Azure Active Directory *n* to differentiate it from other instances.

STEP 2 | Add a subset of groups to scan or exclude from scanning.

1. From **Settings** > **Directory Services**, select the Azure AD instance.
2. Enter the first few letters or name of the group you want to scan for.

You can add all groups using >> or a single group using > but can only add 100 groups in total. If a group is edited or removed from selective scanning, it can take up to 7 days to remove assets or activities, and close any related incidents. Adding a group back to selective scanning will record new user activities but not older, previously removed user activities.



3. Select **Save**.

STEP 3 | Connect your Box app to Prisma SaaS.

Begin Scanning a Box App and enable selective scanning to choose a subset of Azure Active Directory groups to scan.

Manage Your Directory Service on Prisma SaaS

When you connect your directory service to Prisma SaaS, you provide the identifiers and keys authorizing the service to establish a secure connection to the directory to populate your user group information. Prisma SaaS refreshes every 24 hours, but if there are changes to user group membership you'd like to retrieve before the automatic refresh, you can manually update your user and group information.

The directory service and Prisma SaaS maintain a secure connection, but sometimes you need to re-authenticate if there is a network connectivity issue or if the login credentials have changed.

To stop scanning a directory service, you can remove the connection on Prisma SaaS by deleting the directory service instance. Any cloud apps utilizing the subset of groups in scanning will need to be re-authenticated.

- Refresh a Directory Service.
  1. Select **Settings** > **Directory Services**.
  2. In the row of the directory service instance, select **Actions** > **Refresh**.
  3. To begin a rescan after you successfully Refresh, Rescan a Managed Cloud App.

- Re-authenticate a Directory Service.
  1. Select **Settings** > **Directory Services**.
  2. In the row of the directory service instance, select **Actions** > **Re-authenticate**.
  3. Follow the same process to connect the directory service you did when you first added it. See Reauthenticate to a Cloud App for details on the required information and privileges needed to authenticate the directory service.
  4. To refresh the directory service after you successfully re-authenticate, select **Actions** > **Refresh**.

- Delete a Directory Service.
  1. Select **Settings** > **Directory Services**.
  2. Select **Actions** > **Delete** in the row that corresponds to the directory service instance you want to delete.