Prisma™ Cloud 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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

September 17, 2019

Table of Contents

Get Started with Prisma Cloud....7

Prisma Cloud....9
Prisma Cloud License Types....11
Prisma Cloud—How it Works....13
Get Prisma Cloud From the Palo Alto Networks Marketplace....15
Get Prisma Cloud From the AWS Marketplace....17
Access Prisma Cloud....20
Prisma Cloud—First Look....22
Prisma Cloud—Next Steps....23
NAT Gateway IP Addresses for Prisma Cloud....24
Prisma Cloud FAQs....26
- Account Onboarding and SSO....26
- Password and Help....26
- Policy and Alerts....27

Connect Your Cloud Platform to Prisma Cloud....31

Cloud Account Onboarding....33
Add Cloud Account Using the Guided Tour....34
Onboard Your AWS Account....37
- Set Up Your AWS Account....37
- Add an AWS Cloud Account on Prisma Cloud....42
- Update Your RedLock CloudFormation Template....45

Onboard Your Azure Subscription....47
- Azure Cloud Account Onboarding Checklist....47
- Set Up Your Azure Subscription for Prisma Cloud....49
- Create a Custom Role on Azure to Enable Prisma Cloud to Access Flow Logs....56
- Use the Azure PowerShell Script to Add an Azure Account....57
- Add an Azure Subscription on Prisma Cloud....59
- Troubleshoot Azure Account Onboarding....61

Onboard Your Google Cloud Platform Account....65
- Set Up Your GCP Account for Prisma Cloud....65
- Add Your GCP Project to Prisma Cloud....72
- Enable Flow Logs for GCP Projects....75
- Add Your GCP Organization to Prisma Cloud....79
- Enable Flow Logs for GCP Organization....85

Manage Prisma Cloud Administrators....87

Prisma Cloud Administrator Roles....89
Create Account Groups....90
Manage Prisma Cloud Account Groups....91
Create Prisma Cloud Roles....92
Manage Roles in Prisma Cloud....93
Add Administrative Users On Prisma Cloud....94
Create and Manage Access Keys....96
Manage your Prisma Cloud Profile....98
Set up SSO Integration on Prisma Cloud....99
- Set up Just-in-Time Provisioning on Okta....107

View Audit Logs....109

Define Prisma Cloud Enterprise Settings.... 110

Manage Prisma Cloud Alerts.... 111

Prisma Cloud Alerts and Notifications.... 113
Whitelist IP Addresses on Prisma Cloud.... 114
Enable Prisma Cloud Alerts.... 115
Create an Alert Rule.... 116
Configure Prisma Cloud to Automatically Remediate Alerts.... 120
Send Prisma Cloud Alert Notifications to Third-Party Tools.... 123
- Send Alert Notifications to Amazon SQS.... 123
- Send Alert Notifications via Email.... 124
- Send Alert Notifications to a Slack Channel.... 126
- Send Alert Notifications to Splunk.... 128
- Send Alert Notifications to Jira.... 129
- Send Alert Notifications to Google CSCC.... 131
- Send Alert Notifications to ServiceNow.... 132
- Send Alert Notifications to Webhooks.... 133
- Send Alert Notifications to PagerDuty.... 135
- Send Alert Notifications to AWS SecurityHub.... 136
- Send Alert Notifications to Microsoft Teams.... 137

View and Respond to Prisma Cloud Alerts.... 140
Alert Payload.... 144
Prisma Cloud Risk Ratings.... 147

Prisma Cloud Dashboards.... 149

Prisma Cloud Asset Inventory.... 151
SecOps Dashboard.... 153
- Monitored Accounts.... 153
- Monitored Resources.... 153
- Open Alerts.... 153
- Risk Rating by Scanned Accounts.... 153
- Top Instances by Role.... 153
- Alerts by Severity.... 153
- Policy Violations by Type over Time.... 153
- Top Policy Violations.... 153
- Top Internet Connected Resources.... 154
- Connections from the Internet.... 154

Export Data and Customize the SecOps Dashboard.... 155

Prisma Cloud Policies.... 157

Create a Policy on Prisma Cloud.... 159
Manage Prisma Cloud Policies.... 162
Anomaly Policies.... 166

Investigate Incidents on Prisma Cloud.... 167

Investigate Config Incidents on Prisma Cloud.... 169
Investigate Audit Incidents on Prisma Cloud.... 171
Use Prisma Cloud to Investigate Network Incidents.... 173

Prisma Cloud Compliance.... 175

Compliance Dashboard.....177
Download Compliance Standards.....179
Create a Custom Compliance Standard.....180
Add a New Compliance Report.....182

Configure External Integrations on Prisma Cloud.....185
Prisma Cloud Integrations.....187
Integrate Prisma Cloud with Slack.....189
Integrate Prisma Cloud with Splunk.....192
Integrate Prisma Cloud with Amazon SQS.....194
Integrate Prisma Cloud with Amazon GuardDuty.....199
Integrate Prisma Cloud with AWS Inspector.....201
Integrate Prisma Cloud with AWS Security Hub.....204
Integrate Prisma Cloud with Jira.....209
Integrate Prisma Cloud with Qualys.....218
Integrate Prisma Cloud with Google Cloud Security Command Center.....224
Integrate Prisma Cloud with Tenable.....228
Integrate Prisma Cloud with QRadar.....231
Integrate Prisma Cloud with Webhooks.....235
Integrate Prisma Cloud with PagerDuty.....237
Integrate Prisma Cloud with Microsoft Teams.....240
Prisma Cloud Integrations—Supported Capabilities.....241

Get Started with Prisma Cloud

Prisma Cloud is an API-based cloud service that connects to your cloud environments in minutes and aggregates volumes of raw configuration data, user activity information, and network traffic to analyze and produce concise and actionable insights.

> Prisma Cloud
> Prisma Cloud—How it Works
> Prisma Cloud License Types
> Get Prisma Cloud From the Palo Alto Networks Marketplace
> Get Prisma Cloud From the AWS Marketplace
> Access Prisma Cloud
> Prisma Cloud—First Look
> Prisma Cloud—How it Works
> NAT Gateway IP Addresses for Prisma Cloud
> Prisma Cloud FAQs

© 2019 Palo Alto Networks, Inc.

Prisma Cloud

Prisma Cloud is a cloud infrastructure security solution that provides complete visibility and control over risks within your public cloud infrastructure. This API-based service enables granular visibility in to your resources deployed on public cloud platforms—Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure—and in to the network traffic flows to these resources from the internet and between instances. Prisma Cloud also provides threat detection and response for resource misconfigurations and workload vulnerabilities and provides visibility into user activity within each cloud environment. Tracking user activity helps you identify account compromises, escalation of privileges with privileged accounts and insider threats from a malicious user, unauthorized activity, and inadvertent errors. This service continuously monitors your cloud environments to help ensure that your cloud infrastructure is protected from these security threats.

In addition to providing visibility and reducing risks, Prisma Cloud facilitates Security Operations Center (SOC) enablement and adherence to compliance standards. As the service automatically discovers and monitors compliance for new resources that are deployed in your cloud environment, it enables you to implement policy *guardrails* to ensure that resource configurations adhere to industry standards and helps you to integrate configuration change alerts into DevSecOps workflows that automatically resolve issues as they are discovered. This capability streamlines the process of identifying issues and detecting and responding to a list of prioritized risks to maintain an agile development process and operational efficiency.

Here are some highlights of Prisma Cloud:

- **Comprehensive Visibility**—View your resources—deployed on multiple cloud infrastructure platforms—from a single console. In addition to providing a consolidated view of the resources across the cloud platforms, Prisma Cloud integrates with threat intelligence feeds, vulnerability scanners, and Security Information and Event Management (SIEM) solutions to help you build a contextual view of your cloud deployments.
- **Policy Monitoring**—Use Prisma Cloud, which includes Security policies based on industry standards, to continuously monitor for violations. Because cloud platforms enable agility and your users can create, modify, and destroy resources on-demand, these user actions often occur without any security oversight. Prisma Cloud provides hundreds of out-of-the-box policies for common security and compliance standards, such as GDPR, PCI, CIS, and HIPAA. You can also create custom policy rules to address specific needs or to customize the default policy rules.
- **Anomaly Detection**—Automatically detect suspicious user and network behavior using machine learning. Prisma Cloud consumes data about your AWS resources from AWS CloudTrail, AWS Inspector, and

© 2019 Palo Alto Networks, Inc.

Amazon GuardDuty to detect account compromises and insider threats. This service uses machine learning to score the risk level for each cloud resource based on the severity of business impact, policy violations, and anomalous behavior. Risk scores are then aggregated so that you can prioritize your alerts and benchmark risk postures across your entire environment.

- **Contextual Alerting**—Leverage highly contextual alerts for prioritization and rapid response. Because Prisma Cloud also integrates with external vulnerability services, such as AWS Inspector, Tenable.io, and Qualys, to continuously scan your environment, it has additional context to identify unexpected and potentially unauthorized and malicious activity. For example, the service scans for unpatched hosts, escalation of privileges and use of exposed credentials, and scans communication for malicious IP addresses, URLs, and domains.
- **Cloud Forensics**—Go back to any point in time and investigate an issue within seconds. To help you identify security blind spots and investigate issues, Prisma Cloud monitors network traffic from sources such as AWS VPC flow logs, Azure flow logs, GCP flow logs, Amazon GuardDuty, and user activity from AWS CloudTrail, and Azure. .
- **Compliance Reporting**—Reports your risk posture to your management team, to your board of directors, and to auditors.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud License Types

Prisma Cloud licenses are available in two options:

- **Prisma Cloud Business Edition**—License includes configuration security posture management, compliance reporting, automated remediation, custom policy creation, and a standard success plan. The Business edition is tailored for investigating resource misconfigurations and verifying adherence to compliance standards so that you can take steps to implement policies and regulations that enable you to secure your public cloud deployments and comply with security standards.
- **Prisma Cloud Enterprise Edition**—License includes all features included in the Business edition license plus network security monitoring, user entity behavior analysis (UEBA) and integration with host vulnerability management tools, unlimited access to Prisma Cloud APIs, and a standard success plan. The enterprise edition supports the full feature set on Prisma Cloud and includes the ability to ingest and monitor all network, configuration, and user activity data on your cloud resources across all supported cloud platforms, as well as access to all Prisma Cloud policies, compliance reports, and UEBA capabilities for detecting location- and activity-based anomalies.

  You can optionally upgrade to a premium success plan that includes 24x7 access to customer success experts, custom workshops, implementation assistance, configuration and planning, online documentation, and best practices guides.

Prisma Cloud uses workload-based licensing. When you choose your license edition, you must estimate the number of workloads you want to monitor and protect. The following resource types are counted as licensable assets:

Workload Resource Type	AWS	Azure	GCP
Compute	EC2 Instance	Virtual Machine	Compute Engine
Managed Database	RDS, Redshift	SQL server, ManagedMySQL/ Postgres	Cloud SQL
Load Balancers	Elastic Load Balancer (ELB), Application Load Balancer (ALB)	Load Balancer	Load Balancer
Gateway	NAT Gateways	Gateways	Gateways
Containers	Number of nodes in EKS, ECS, and Fargate	Number of nodes in AKS	Number of nodes in GKE

After you Connect Your Cloud Platform to Prisma Cloud, you can review the actual number of licensable assets that you're securing with the service. The **Settings** > **Licensing** tab displays a resource count in a tabular format and a graphical view of the resource trend as a stacked bar chart. The default time range is three months, but you can select a time range of your choice. You can download and share the licensing information in a CSV file format.

© 2019 Palo Alto Networks, Inc.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud—How it Works

Prisma Cloud is a Security Operations Center (SOC) enablement tool that helps you to identify issues in your cloud deployments and to respond to a list of prioritized risks so that you can maintain an agile development process and operational efficiency.

When you add a cloud account to Prisma Cloud, the IaaS Integration Services module ingests flow logs, configuration logs, and audit logs data from your cloud environment over an encrypted connection and stores the encrypted metadata in RDS3 and RedShift instances within the Prisma Cloud AWS Services module. You then use the Prisma Cloud app or the APIs to interact with this data to configure policies, to investigate and resolve alerts, and to set up external integrations and forward alert notifications. The Enterprise integration Service module enables you to leverage Prisma Cloud as your cloud orchestration and monitoring tool and to feed relevant information to their existing SOC workflows. The integration service ingests information from your existing single sign-on(SSO) identity management system and allows you to feed information back in to your existing SIEM tools and collaboration and helpdesk workflows.

To ensure the security of your data and high availability of Prisma Cloud, Palo Alto Networks makes Security a priority at every step. The Prisma Cloud architecture uses Cloudflare for DNS resolution of web requests and for protection against DDoS. The following diagram represents the infrastructure within a region:

© 2019 Palo Alto Networks, Inc.

For data redundancy of stateful components, such as RDS and Redshift, and of stateless components such as the application stack and Redis (used primarily as a cache), the service uses native AWS capabilities for automated snapshots or has set up automation scripts using AWS Lambda and SNS for saving copies to S3 buckets.

Additionally, to ensure that these snapshots and other data at rest are safe, Prisma Cloud uses AWS Key Management Service (KMS) to encrypt and decrypt the data. To protect data in transit, the infrastructure terminates the TLS connection at the ELB and secures traffic between components within the data center using an internal certificate until it is terminated at the application node. This ensures that data in transit is encrypted using SSL. And, lastly, for workload isolation and micro segmentation, the built-in VPC security controls in AWS are in effect to securely connect and monitor traffic between application workloads on AWS.

© 2019 Palo Alto Networks, Inc.

Get Prisma Cloud From the Palo Alto Networks Marketplace

Purchase or try Prisma Cloud from the Palo Alto Networks Marketplace. Within 24 hours of purchase, you'll get access to the Prisma Cloud tenant that is provisioned for you.

STEP 1 | Go to the Palo Alto Networks Marketplace.

STEP 2 | Create an account.

Required, only if you do not have a Palo Alto Customer Support Portal (CSP) account.

1. Enter the personal and company information requested in the form. Required fields are indicated with red asterisks.
2. Accept the privacy agreement and click **Create an account**.
3. Look for the welcome email in your email inbox and click the link in that email to continue the activation process.
4. Click the **click here** link on the page that displays and enter your account credentials on the Palo Alto Networks single sign-on page.
5. Answer the security questions and **Save** your changes.

   You will be logged in to the Palo Alto Networks Marketplace.

STEP 3 | Scroll down to find the Prisma Cloud app on the Palo Alto Networks Marketplace and click **View app**.

STEP 4 | Select **Free Trial** or **Buy Now**.

The Enterprise edition is available in the Trial and Buy Now options; the Business edition is available as a Buy Now subscription only. See Prisma Cloud License Types for details.

- For **Buy Now**.

  1. Select the license edition – Business or Enterprise.
  2. Select the **Term** as 1 year.
  3. Select **Billing cycle**—yearly or monthly.
  4. Select the **Number of workloads** you need to secure.

     The range is 100-900 workloads. Contact sales if you need to secure more than 900 workloads.
  5. Opt in to purchase the **Premium Success Plan**.

     If you do not opt in you receive the standard success plan.
  6. Select the region in which you want to provision your Prisma Cloud instance.

     Currently, the available regions are Australia, Germany, GovCloud, and US.
  7. Click **Next**, and review the summary.
  8. Enter your Billing information.
  9. Review and **Accept** the terms and conditions of the EULA and click **Next**.

     You will see a success message on screen. Then, within the next 24 hours look for two emails. The first email is an order confirmation email and the second is a welcome email that includes a link to log in to your Prisma Cloud tenant. You can also access your Prisma Cloud tenant from the Palo Alto Networks hub, using the Prisma Cloud tile.
  10. Enable **Auto Renewal** to ensure that you have uninterrupted monitoring and protection for your public cloud deployments.

© 2019 Palo Alto Networks, Inc.

- For a Free trial.
  1. Select the region in which you want to provision your Prisma Cloud instance.

     Currently, the available regions are Australia, Germany, GovCloud, and US.
  2. **Accept** the EULA and click **Next**.

     A license confirmation displays.

LICENSE TYPE	Enterprise
SERIAL NUMBER	018810126730
SUPPORT	Standard
MARKETPLACE	Palo Alto Networks Marketplace
BILLING MODEL	Trial
WORKLOADS	100
START DATE	Apr 03, 2019 at 10:18 PDT
END DATE	May 01, 2019 at 17:00 PDT
Need Help? ppc-help@paloaltonetworks.com	Buy Now

Within the next 24 hours, you will receive a welcome email that includes a link to log in to the Prisma Cloud tenant that is provisioned for you. You can directly access the Prisma Cloud instance or log in to the hub and click the Prisma tile to log in to your Prisma Cloud tenant.

© 2019 Palo Alto Networks, Inc.

Get Prisma Cloud From the AWS Marketplace

Purchase Prisma Cloud directly from the AWS Marketplace. Within 24 hours of purchase, you'll get access to the Prisma Cloud tenant that is provisioned for you.

STEP 1 | Go to the AWS Marketplace.

STEP 2 | Select Prisma Cloud Threat Defense and Compliance Platform.

Search for Palo Alto Networks on the AWS Marketplace and click the link for the **Prisma Cloud Threat Defense and Compliance Platform**.

STEP 3 | Select **Continue to Subscribe**.

STEP 4 | Enter the details to get a Prisma Cloud subscription.

The subscription is for a 12-month period.

© 2019 Palo Alto Networks, Inc.

1. Select your auto-renewal preference.

   The default **Renewal Settings** is **Yes** so that your contract is automatically renewed before it expires. This ensures that you have uninterrupted coverage for securing your public cloud deployments.
2. Select the license edition and the number of units.

   The Prisma Cloud License Types are Business or Enterprise with the standard success plan. If you want to protect 1000 workloads, enter 10 units because 1 unit is equal to 100 workloads.
3. Select **Create contract**.
4. Confirm the contract and **Pay Now**.
5. Select **Set up your account** to continue with setting up Prisma Cloud.

This link has a temporary access token that expires in 24 hours. If you want to come back later and provide the details to provision your Prisma Cloud instance, you must log in to your AWS account. You can then use the View or Modify link for the active AWS Marketplace software subscription on Your Software page of the AWS Marketplace. You can then to get access to the link Click here to setup your account.

© 2019 Palo Alto Networks, Inc.

STEP 5 | Provide the details for provisioning your Prisma Cloud instance.

1. Enter the personal and company information requested in the form.
2. Select the region where you want your Prisma Cloud tenant provisioned.
3. Select **Register**.

   The message informs you whether the registration was successful. Look for the welcome email in your email inbox and click the link in that email to log in to the Palo Alto Networks hub.

4. Log in to the hub and click the Prisma Cloud tile to start using Prisma Cloud.

You are now ready for Prisma Cloud—First Look and Prisma Cloud—Next Steps.

© 2019 Palo Alto Networks, Inc.

Access Prisma Cloud

The welcome email you receive from Palo Alto Networks (ppc-help@paloaltonetworks.com) includes a link where you can access your instance of Prisma Cloud. If you are the first registered user, a Palo Alto Networks Customer Support Portal (CSP) account is created for you, and you can log in to Prisma Cloud to start securing your cloud deployments. For all other Prisma Cloud users, when your Prisma Cloud system administrator adds you to the tenant, you receive two emails. Use the *Welcome to Palo Alto Networks Support* email to activate the CSP account and set a password to access the Palo Alto Networks Support portal , before you click the Get Started button in the *Welcome to Prisma Cloud* email to log in to your Prisma Cloud instance.

The link in your welcome email varies depending on whether you are using Palo Alto Networks Customer Support (CSP) credentials to log in or if you are using a third-party IdP for Single Sign On (SSO):

If you have a Palo Alto Networks CSP account and are not using a third-party IdP, the link enables you to directly log in to Prisma Cloud using the email address and password registered with the CSP account.

If you are using a third-party IdP and the login URL is configured on Prisma Cloud, the link redirects you to your IdP's login page and you can log in using the credentials set up on your IdP.

If you are using a third-party IdP but the login URL is not configured on Prisma Cloud, you must navigate to your IdP and click the Prisma Cloud tile there to log in using the credentials set up on your IdP.

Browser Support—To access the Prisma Cloud administrator console, Chrome version 72 or later is recommended for an optimal user experience. The Prisma Cloud console is not explicitly tested on other browsers and though we expect it to perform with graceful degradation, it is not guaranteed to work.

Status Updates—Use the Prisma Cloud status page to view operational status and subscribe to updates about the service.

STEP 1 | Launch a web browser and access the URL for Prisma Cloud or go to the Palo Alto Networks hub to access the app.

The URL for Prisma Cloud varies depending on the region and cluster on which your tenant is deployed. Your welcome email will include one of the following URLs that is specific to the tenant provisioned for you:

- https://app.prismacloud.io
- https://app2.prismacloud.io
- https://app3.prismacloud.io
- https://app.eu.prismacloud.io
- https://app.anz.prismacloud.io
- https://app.gov.prismacloud.io

© 2019 Palo Alto Networks, Inc.

On the hub, if you see the Prisma Cloud tile, but cannot login into the app because of a SAML error it probably means that you do not have an account on that Prisma cloud instance. Contact your system administrator for an account to access that instance.

STEP 2 | Accept the EULA.

After you accept the terms and conditions of use, use the get started guide to learn the basics.

STEP 3 | Select **Licensing** and verify that you have the correct Prisma Cloud License Types or get started with Prisma Cloud—First Look.

STEP 4 | Switch between Prisma Cloud instances.

If you are responsible for monitoring clouds belonging to different organizations (tenants), you can use your Palo Alto Networks login credentials to access all tenants from the hub.To enable multi-tenant login access, your system administrator must add your email address on each Prisma Cloud tenant (see Add Administrative Users On Prisma Cloud), and you then receive an email from Palo Alto Networks to get started. By default an administor on Prisma cloud is designated as an Instance Administrator for that tenant only on the hub. If you want to change a role or enable access to other apps, see roles.

With Palo Alto Networks CSP credentials, you can click the app switcher on the hub

and then select a different tenant to switch between instances.

If you see the serial number for your instance and want to change it to a descriptive label, navigate to the Settings page using the gear > Manage Apps in the upper right-hand corner of the hub menu. Click directly on the serial number and rename it. This new name displays on the hub only, and does not automatically apply to your Prisma Cloud instance.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud—First Look

When you Access Prisma Cloud, you see the Asset Inventory Dashboard first. You can then use the following tabs to interact with the data and visualize the traffic flow and connection details to and from the different resources in your cloud deployment, review the default policy rules and compliance standards, and explore how the web interface is organized to help you and DevSecOps teams to monitor cloud resources.

- **Dashboard**—Get a graphical view of the health cloud (security and compliance posture) of your assets deployed across multiple public cloud environments.
- **Investigate**—Identify security threats and vulnerabilities, create and save investigative queries, analyze impacted resources.
- **Policies**—Configure policies to maintain compliance and security.
- **Alerts**—View the list of violations and anomalies that have been discovered, drill in to the details and look up remediation options, create alert rules and notification templates.
- **Compliance**—Monitor your cloud accounts against compliance standards such as NIST, SOC 2, HIPAA, PCI, GDPR, ISO 27001:2013 and custom policies and generate reports for viewing offline.
- **Settings**—Add new cloud accounts and set up Prisma Cloud administrative users. You can also set up account groups, and create users, associate roles and permissions, add external integrations including SAML integration (SSO), view audit logs, manage IP whitelisting, and view licensing/usage reporting and modify browser session timeout.
- **Profile**—Maintain your profile and manage your credentials, and change the UI display language.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud—Next Steps

Now that you have familiarized yourself with Prisma Cloud, here are some things to consider next so that you can begin protecting your cloud resources:

- Whitelist the NAT Gateway IP Addresses for Prisma Cloud so that you can access Prisma Cloud from your network.
- Create Account Groups
- Connect Your Cloud Platform to Prisma Cloud
- Add Administrative Users On Prisma Cloud
- Create an Alert Rule
- Prisma Cloud Integrations
- Prisma Cloud Dashboards
- Investigate Incidents on Prisma Cloud
- Create a Policy on Prisma Cloud
- Add a New Compliance Report

© 2019 Palo Alto Networks, Inc.

NAT Gateway IP Addresses for Prisma Cloud

Prisma Cloud uses the following NAT gateway IP addresses. To ensure that you can access Prisma Cloud and the API for any integrations that you've enabled between Prisma Cloud and your incidence response workflows, review the list and update your IP address whitelists.

Prisma Cloud URL	NAT Gateway IP address
app.prismacloud.io	3.94.253.103 54.89.145.129 54.145.47.25 34.199.10.120 34.227.158.93 34.228.96.118
app2.prismacloud.io	3.16.7.30 13.59.164.228 18.191.115.70 18.218.243.39 18.221.72.80 18.223.141.221
app3.prismacloud.io	34.208.190.79 52.24.59.168 52.39.60.41 52.26.142.61 54.213.143.171 54.218.131.166
app4.prismacloud.io	52.52.110.223 13.52.175.228 52.52.50.152 13.52.27.189 13.52.105.217 13.52.157.154
app.anz.prismacloud.io	3.104.252.91 13.54.241.27 13.211.100.18 13.239.110.68

© 2019 Palo Alto Networks, Inc.

Prisma Cloud URL	NAT Gateway IP address
	52.62.194.176 52.62.231.151
app.eu.prismacloud.io	3.121.64.255 3.121.248.165 3.121.107.154 18.184.105.224 18.185.81.104 52.29.141.235
app2.eu.prismacloud.io	18.200.200.125 3.248.26.245 99.81.226.57 52.208.244.121 18.200.207.86 63.32.161.197
app.gov.prismacloud.io	96.127.115.247 96.127.90.208 52.61.113.234 52.61.112.59 52.61.164.254 160.1.65.168

© 2019 Palo Alto Networks, Inc.

Prisma Cloud FAQs

- Account Onboarding and SSO
- Password and Help
- Policy and Alerts

Account Onboarding and SSO

- **Explain VPC flow logs**

  VPC flow logs provide a unidirectional record of network traffic that inform you about how packets flowed from A to B, and from B to A (as in a separate record). They provide no direct insight into which endpoint is the server in any conversation or which endpoint initiated a conversation. You could look at which flow record has a lower timestamp and assume that the source in that record is the client but in the case of VPC flow logs, log collection is aggregated over several minute windows which removes the precision required to make this a reliable indicator. Additionally, long-lived connections and connections that appear on the boundaries of batches of logs will defeat this heuristic. There are other factors we can consider, such as source port vs the destination port. We can also compare the count of distinct peers for a given endpoint IP and port. Prisma Cloud evaluates all these conditions, plus others, with a weight given to each measure and a historical bias. These measures are heuristics and are therefore imperfect.
- **Why do we need list permissions for Key Vault in Azure?**

  To support Azure Key Vault based policies, Prisma Cloud needs to ingest Key Vault. We are NOT ingesting the keys or secrets, but only their ids and other metadata.
- **Which SAML binding should I use for SSO?**

  The Prisma Cloud SAML endpoint supports the HTTP POST binding.

Password and Help

- **What are the rules for password similarity and reuse in Prisma Cloud?**

  When you create a new password, we check for its similarity with the current password. The measure of similarity between the new and the current old password strings is determined by the minimum number of single-character edits like insertions, deletions, or substitutions that are required to change one word into the other.The new password string is not accepted if the similarity is upto 70% with the current old password.

  If for example, your current password is: MenloPark.123!

  You cannot use: M3nl0P@rk.123!

  You can use: ParkMenlo.123!
- **What are the complexity requirements for creating Prisma Cloud passwords?**

  Passwords should have, minimum 8 characters and maximum 30 characters, one upper-case letter, one lower-case letter, one digit between 0-9and one special character which could be any of ~`!@#$%^&*()-_+={}[]|\:;’,“.<>?/
- **Help icon on the bottom right hand corner is not visible. The application does not launch pages after clicking the Help Icon. What should I do?**

  Check your pop-up blocker and allow pop-ups. Check if your advertisement blocking software is blocking Prisma Cloud and whitelist the URL for your Prisma Cloud instance and app.pendo.io. Check and disable your local firewall rules or proxies that are blocking both these URLs.
- **Where do I submit documentation requests or report errors in the documentation?**

© 2019 Palo Alto Networks, Inc.

Please let us know how we are doing at documentation@paloaltonetworks.com. When writing to us about a documentation error, please include the URL for the page where you see the issue.

Policy and Alerts

- **What happens when I have two alert rules for the same conditions, one with and one without auto remediation?**

  The Alert Rule that has auto remediation enabled wins, and alerts will be auto resolved.
- **Which threat intelligence feeds does Prisma Cloud integrate with?**

  Prisma Cloud integrates with the threat intelligence feeds from Facebook ThreatExchange, AWS GuardDuty, and AWS Inspector to help you turn your threat data into actionable intelligence and focusing on what is relevant to your deployments.
- **How often does Prisma Cloud retrieve data from cloud services that provide automated security assessment or threat detection?**

  If you have set up an integration with Qualys, Tenable, Amazon GuardDuty, or AWS Inspector for additional context on risks in the cloud, Prisma Cloud retrieves data from these services periodically. The data from Qualys and Tenable is retrieved every hour, and with AWS Inspector and Amazon GuardDuty the data is retrieved at every ingestion cycle.
- **After I update a config policy query, how long does it take to auto resolve alerts that no longer match this policy.**

  When a Config based policy query is changed, all the alerts generated by this policy are re-evaluated at the next scan. Alerts that are no longer valid because of the policy change are auto resolved.
- **What is the list of web applications that Prisma Cloud auto classifies?**

Port Number	Application Classification
0	ICMP
21	FTP
22	SSH
23	TELNET
25	SMTP
53	DNS
80	Web (80)
88	Kerberos
111	RPC (111)
135	RPC (135)
143	IMAP
389	LDAP

© 2019 Palo Alto Networks, Inc.

Port Number	Application Classification
443	Web (443)
444	SNPP
445	Generic (445)
514	Syslog
587	SMTP
636	LDAP (TLS)
995	IMAP
1433	SQL Server
1515	OSSEC
1521	Oracle
2376	Docker TLS
3128	Web Proxy
3268	Active Directory (GC)
3306	My SQL
3389	RDP
5050	Mesos Server
5432	Postgress
5439	RedShift
5671	RabbitMQ
5672	RabbitMQ
5900	VNC
6168	Generic (6168)
6379	Redis
7200	Generic (7200)
7205	Generic (7205)
7210	MaxDB

© 2019 Palo Alto Networks, Inc.

Port Number	Application Classification
8000	HTTP (8000)
8080	HTTP (8080)
8140	Puppet
8332	Bitcoin
8333	Bitcoin
8443	HTTP (8443)
8545	Etherium (8545)
8888	HTTP (8888)
9000	Generic (9000)
9006	Web (9006)
9092	Kafka
9300	Elastic Search
9997	Splunk Logger
15671	RabbitMQ WebUI
15672	RabbitMQ WebUI
27017	MongoDB
29418	Git
30000	Generic (30000)
30303	Ethereum (30303)
52049	NFS
55514	Syslog
60000	Generic
61420	MinuteMan LB
61421	MinuteMan LB
61668	Generic (61668)

© 2019 Palo Alto Networks, Inc.

Connect Your Cloud Platform to Prisma Cloud

To begin monitoring the resources on your cloud infrastructure, you must first connect your public cloud accounts to Prisma Cloud. When you add your cloud account to Prisma Cloud, the API integration between your cloud infrastructure provider and Prisma Cloud is established and you can begin monitoring the resources and identify potential security risks in your infrastructure.

> Cloud Account Onboarding
> Add Cloud Account Using the Guided Tour
> Onboard Your AWS Account(self-guided)
> Onboard Your Azure Subscription(self-guided)
> Onboard Your Google Cloud Platform Account (self-guided)

© 2019 Palo Alto Networks, Inc.

Cloud Account Onboarding

To get the most out of your investment in Prisma Cloud, the first thing you need is to add your cloud accounts to Prisma Cloud. This process requires you to have the correct set of permissions to authenticate and authorize the connection and retrieval of data. For the onboarding of cloud accounts, Prisma Cloud administrators with the System Administrator and Cloud Provisioning Administrator roles have two options

- Use the instructions outlined in Connect Your Cloud Platform to Prisma Cloud. These workflows provide the context you need to add your cloud accounts to Prisma Cloud, while allowing you to make decisions and figure things out on your own.
- Use the cloud account onboarding guided tour, which makes the onboarding flow easy, for a good first-run experience. If you are logging in to Prisma Cloud for the first-time, the guided tour displays after the welcome tour and prompts you to pick a cloud platform to add on Prisma Cloud.

If you would like to access the guided tours subsequently, use the **Quick Start Checklist** on the top-left drop-down.

With the guided tour, you need to make a few choices and provide basic account details to retrieve configuration logs and get started with Prisma Cloud for monitoring and visibility. If you want to ingest data from event logs and flow logs, you need to perform some additional tasks. See Add Cloud Account Using the Guided Tour.

© 2019 Palo Alto Networks, Inc.

Add Cloud Account Using the Guided Tour

The guided tour for Cloud Account Onboarding uses automation scripts—Cloud Formation templates for AWS or Terraform templates for Azure and GCP—to create the custom roles and enable the permissions required to add the cloud account. To make sure that you have a good first-run experience, there are a few important things you need to know in order to be successful. Use the following checklist to avoid mistakes as you go through the onscreen instructions in the tour, and pay heed to the explanation on the left-pane of the tour:

- **AWS**
  - ❑ Choose a cloud account name to uniquely identify the AWS account on Prisma Cloud.

    If you want to onboard an AWS GovCloud account, use the workflow in Onboard Your AWS Account.
  - ❑ Decide whether you want to enable permissions to monitor (read-only access) your resources in your cloud account or to monitor and protect (read-write access) the resources in your cloud account.
  - ❑ Follow the on-screen instructions to add your cloud account. The AWS Cloud Formation Template (CFT) automates the process of creating the custom roles required to add your AWS account to Prisma Cloud.

    In the guided tour, VPC flow logs and AWS CloudTrail logs are retrieved only if you have already enabled them for the AWS account that you are onboarding. The CFT in the guided tour does not support the ability to enable Audit events and Flow logs for your AWS account or any other integrations such as Amazon GuardDuty or AWS Inspector.
  - ❑ Review the account onboarding status message to verify that you have provided the information required to successfully add your cloud account to Prisma Cloud and what data —Config logs, Audit logs and Flow logs — is being retrieved.
- **Azure**
  - ❑ Choose a cloud account name to uniquely identify the Azure account on Prisma Cloud.

    If you want to onboard a subscription on Azure Government, use the workflow in Onboard Your Azure Subscription.
  - ❑ Decide whether you want to enable permissions to monitor (read-only access) your resources in your cloud account or to monitor and protect (read-write access) the resources in your cloud account. If you want to review the permissions, see read-onlyand read-write templates.
  - ❑ From the Azure portal, collect your Azure Active Directory ID (Tenant ID), and Subscription ID.

    You must add one subscription at a time, if you have multiple subscriptions.
  - ❑ Enter a Service Principal password of your choice.

    Use a strong password that meets the Azure password complexity guidelines. If you later decide to change this password on the Azure portal, you must manually update on Prisma Cloud.
  - ❑ When you get to (step 3 of 5), where you receive instructions for adding the cloud account using the Terraform script. As a best practice create a directory to store the Terraform template that you download. This practice allows you to use the script the next time when you want to add a different Azure subcription to Prisma Cloud. Give the directory a name that allows you to uniquely identify the subscription for which you're using it, for example, onboard-<subscription-name>. Then, copy the Terraform template to that folder before you upload the script to Azure Cloud Shell and run the Terraform commands provided in the guided tour.

© 2019 Palo Alto Networks, Inc.

- If you want to **Ingest and Monitor Network Security Group Flow Logs** (step 4 of 5) you must first configure Network Security Groups and assign a storage account to enable Flow log ingestion on Prisma Cloud. If you enable this option without setting it up on the Azure portal, Prisma Cloud will not be able to retrieve any Flow logs.

- **GCP**
  - Choose a cloud account name to uniquely identify the GCP organization or project on Prisma Cloud.
  - Decide whether you want to enable permissions to monitor (read-only access) your resources in your cloud account or to monitor and protect (read-write access) the resources in your cloud account. Review the permissions associated with the project-level (read-only and read-write) and organization-level (read-only and read-write) templates.
  - Decide whether you plan to use a single service account to **`Automatically onboard projects that are accessible by this service account`**. A service account on GCP includes the permissions and roles that are granted to that Service Account to access your GCP resources.
  - From the Google Cloud Console, collect your project ID, or your GCP organization name and ID.
  - When you get to (step 2 of 3), where you receive instructions for adding the cloud account using the Terraform script. As a best practice create a directory to store the Terraform template that you download. This practice allows you to use the script the next time when you want to add a different GCP project to Prisma Cloud. Give the directory a name that allows you to uniquely identify the project for which you're using it, for example, onboard-<project-id>. Then, copy the Terraform template to that folder before you upload the script to Google Cloud Shell and run the Terraform commands provided in the guided tour.

  - Whether you are adding a single project or an organization, the service account that the Terraform template creates for you is hosted within the **Project ID** you provide. This service account has the appropriate permissions and roles required to enable the monitor (read only) or monitor and protect (read-write access) on your GCP resources. Because this service account is hosted within the Project ID you provided, if you delete the project, the service account is automatically deleted and Prisma Cloud can no longer monitor or protect your GCP resources.

© 2019 Palo Alto Networks, Inc.

If you want to use a single service account to **`Automatically onboard projects that are accessible by this service account`**, after you complete the guided tour, you must manually associate the service account with each project that you want to onboard to GCP. You have to manually associate the service account with every project on the GCP console to enable Prisma Cloud to start monitoring all the other projects at the next ingestion cycle. You can review and verify that all your projects have been added to Prisma Cloud on **Settings** > **Cloud Accounts**.

- Save the output from the Terraform script to a plain text file and save it with the **`.json`** file extension. This .json file is the key file for the service account.
- Review the account onboarding status message to verify that you have provided the information required to successfully add your cloud account to Prisma Cloud and what data is being retrieved.

GCP Flow logs are not retrieved with this guided tour workflow. Follow the instruction in Enable Flow Logs for GCP Organization *or* Enable Flow Logs for GCP Projects *to retrieve GCP Flow logs.*

© 2019 Palo Alto Networks, Inc.

Onboard Your AWS Account

To connect your public AWS or AWS GovCloud account to Prisma Cloud, you must complete some tasks on the AWS management console and some on Prisma Cloud.

The high-level workflow is as follows:

- Set Up Your AWS Account
- Add an AWS Cloud Account on Prisma Cloud

Set Up Your AWS Account

Before Prisma Cloud can monitor your AWS account, you must be grant Prisma Cloud access to your flow logs. Using a customized CloudFormation template, you can create a read-only role to retrieve and view the traffic log data or a limited read-write permission role to retrieve traffic log data and remediate incidents. The template specifies policies attached to the role and is deployed in the same region as your AWS account. Event logs associated with a monitored cloud account are automatically retrieved on Prisma Cloud.

After creating the role, you must enable VPC flow logs and create another new role with permissions to publish flow logs to CloudWatch, create a CloudWatch log group to publish the VPC flow log streams.

STEP 1 | Get the RedLock customized CloudFormation template.

The RedLock S3 bucket has read-only templates for the public AWS and AWS GovCloud environments, and read-and-write templates for the public AWS and AWS GovCloud environments.

- AWS public cloud

```
https://s3.amazonaws.com/redlock-public/cft/rl-read-only.template
```

```
https://s3.amazonaws.com/redlock-public/cft/rl-read-and-write.template
```

- AWS GovCloud

```
https://s3.amazonaws.com/redlock-public/cft/redlock-govcloud-read-and-write.template
```


© 2019 Palo Alto Networks, Inc.

```
https://s3.amazonaws.com/redlock-public/cft/redlock-govcloud-read-
only.template
```

STEP 2 | Create a Prisma Cloud role and attach policies using the CloudFormation template.

To monitor and analyze your AWS cloud without auto-remediation privileges, use the read-only CloudFormation template to create a read-only role. If you want to remediate any incidents discovered, use the read-write CloudFormation template to create a limited permission role.

1. Log in to AWS Console.
2. Select **Services** > **CloudFormation** > **Stacks** > **Create Stack**.
3. Select **Specify an Amazon S3 template URL**.
4. Paste the S3 URL and click **Next**.

   Use the read-only template to create a read-only role with **AWS SecurityAudit Policy** and **RedLock-IAM-ReadOnly-Policy**.

   Use the read-write template to create a limited permission role with **AWS SecurityAudit Policy** and **RedLock-IAM-Remediation-Policy**

5. Enter a Stack name, an External ID, and a Role ARN and click **Next**.

   The External ID and Role ARN will be needed when you Add an AWS Cloud Account on Prisma Cloud.

© 2019 Palo Alto Networks, Inc.

6. Optional Configure stack options.
7. Click **Next** and verify the settings.
8. Acknowledge the creation of the Prisma Cloud role and click **Create**.

When the stack creation completes, the Role ARN is available in the Outputs tab.

STEP 3 | Create a CloudWatch log group.

The CloudWatch log group defines where the log streams are recorded.

1. Select **Services** > **CloudWatch** > **Logs** > **Actions** > **Create log group**.
2. Enter a name for the log group and click **Create log group**.

STEP 4 | Enable flow logs.

You must enable flow logs and assign a IAM role with permissions to publish the flow logs to the CloudWatch log group. Make sure to create a new role or edit the role you created earlier to include the permissions below to publish flow log records to the CloudWatch log group, otherwise Prisma Cloud cannot ingest the data and an access error message displays on the Prisma Cloud administrative console.

1. Select **Services** > **VPC** > **Your VPCs**.
2. Select the VPC to enable flow logs for and select **Actions** > **Create flow log**.
3. Set the **Filter** to **Accept** or **All**.

© 2019 Palo Alto Networks, Inc.

Setting the filter to **All** will enable Prisma Cloud to retrieve accepted and rejected traffic from the flow logs. Setting the filter to **Accept** will only retrieve Accepted traffic. If you set the filter to **Reject**, Prisma Cloud will not retrieve any flow log data.

4. Verify **Destination** is set to **Send to CloudWatch Logs**.

   If you set the destination as Amazon S3 bucket, Prisma Cloud will be unable to retrieve the data.
5. Select the **Destination log group** from Step 3.
6. Create a new **IAM role** or edit the IAM role you created earlier to include the following permissions that enable you to publish flow logs to the CloudWatch log group and click **Create**.

   The permissions for this IAM role are:

```
{ "Version":"2012-10-17", "Statement":[ { "Sid":"", "Effect":"Allow",
 "Principal":{ "Service":"vpc-flow-logs.amazonaws.com" },
 "Action":"sts:AssumeRole" }, { "Action":[ "logs:CreateLogGroup",
 "logs:CreateLogStream", "logs:DescribeLogGroups",
 "logs:DescribeLogStreams", "logs:PutLogEvents" ], "Effect":"Allow",
 "Resource":"*" } ] }
```

STEP 5 | Configure a CloudTrail to deliver log files to the CloudWatch log group.

A CloudTrail is required to deliver the log streams to the CloudWtach log group. The CloudTrail configuration must be associated with a S3 bucket.

1. Select **Services** > **CloudTrail** > **View Trails** > **Create Trail**.
2. Enter a **Trail name**.
3. Verify **Apply trail to all regions** is set to **Yes**.
4. Select an option to apply the trail to your organization or not.
5. Configure your trail to log **All** Read/Write data events.

© 2019 Palo Alto Networks, Inc.

6. Select an existing S3 bucket or create a new one.
7. **Create** the CloudTrail.

8. Select the name of the CloudTrail created above.
9. **Configure** the CloudWatch log group.
10. Enter the name of the CloudWatch log group and click **Continue**.

11. Expand **Details**.
12. Select **Create a new IAM role** and enter a name.
13. Click **Allow** to grant the CloudTrail permissions to the displayed CloudWatch API calls.

© 2019 Palo Alto Networks, Inc.

STEP 6 | Add an AWS Cloud Account on Prisma Cloud

Add an AWS Cloud Account on Prisma Cloud

Use the following workflow to add your AWS account to Prisma Cloud. After adding your AWS cloud account, add your read-only or limited read-write permission role on Prisma Cloud to monitor and analyze AWS traffic flow logs.

STEP 1 | Gather your AWS account info.

Log in to your AWS account to retrieve your AWS Account ID, External ID, and Role ARN to enable authentication between Prisma Cloud and your AWS account.

1. Select **Services** > **IAM** > **Roles**.
2. Select the **Trust relationships** tab to find your External ID, and Role ARN.

STEP 2 | Access Prisma Cloud to add your AWS cloud account.

© 2019 Palo Alto Networks, Inc.

STEP 3 | Click Settings and select **Cloud Accounts**.

1. Click **+ Add New** and enter a **Cloud Account Name**.
2. Select **AWS** as the **Cloud Type**.

STEP 4 | Enter your AWS information on Prisma Cloud.

1. Enter your **AWS Account ID**.
2. Enter your **External ID**.
3. Enter the **Role ARN** and click **Next**.

STEP 5 | Select one or more account groups and click **Next**.

You must assign each cloud account to an account group, and Create an Alert Rule to associate the account group with it to generate alerts when a policy violation occurs.

© 2019 Palo Alto Networks, Inc.

STEP 6 | **Save** your changes.

STEP 7 | Click Settings and select **Cloud Accounts**, locate your AWS project and verify the onboarding status of your AWS project on Prisma Cloud.

© 2019 Palo Alto Networks, Inc.

ACCOUNT ID	CLOUD	NAME	TYPE	ACCOUNT GROUPS	STATUS	LAST MODIFIED BY
		Redlock Rocks		dummy	NA	
		gcp-redlock-qa-static		dummy, gcp-redlock-qa-static	NA	
		RedLock Sandbox		Temporary All Accounts Group	Error	
		ev-aws-5390		ev-account-group	Error	
		ev-aws-9491		ev-account-group	Error	
		ev-azure-d23			Error	
		Redlock GCP Dev Playgroundd		Temporary All Accounts Group	Success	
		Redlock QA Automation		dummy, Redlock QA Automation	Warning	
		Azure-Microsoft Azure Sponsorship		Temporary All Accounts Group	Warning	

Update Your RedLock CloudFormation Template

When Prisma Cloud releases a new policy that supports a new AWS service, you'll need to update the permissions associated with the AWS role for Prisma Cloud. You can update the CloudFormation template through the AWS console or using the AWS CLI.

- Use the AWS console to update the RedLock CloudFormation template.
  1. Log in to AWS console.
  2. Select **Services** > **CloudFormation** > **Stacks**.
  3. Select the Stack to update and click **Actions** > **Update Stack**.
  4. Select **Specify an Amazon S3 template URL**.

Role	S3 Template URL
Read-Only	https://s3.amazonaws.com/redlock-public/cft/rl-read-only.template
Read-Write (Limited)	https://s3.amazonaws.com/redlock-public/cft/rl-read-and-write.template

  5. Confirm Details and click **Next**.

     To create a new stack, enter a new ExternalID and RedlLockRoleARN or update the existing stack by clicking Next.
  6. Optional Configure stack options.
  7. Click **Next** and verify the settings.

     Preview your changes to the CloudFormation template for the role updated.
  8. **Update** your CFT,

- Use AWS Command Line Interface to deploy the updated RedLock CloudFormation Template.

© 2019 Palo Alto Networks, Inc.

1. Using the AWS CLI tool, enter the following command to retrieve the current CloudFormation template.

Role	CLI Comand
AWS Public cloud	
Read-Only	wget https://s3.amazonaws.com/redlock-public/cft/rl-read-only.template --quiet -O /tmp/rl-read-only.template
Read-Write (Limited)	wget https://s3.amazonaws.com/redlock-public/cft/rl-read-and-write.template --quiet -O /tmp/rl-read-and-write.template
AWS GovCloud	
Read-Only	wget https://s3.amazonaws.com/redlock-public/cft/redlock-govcloud-read-only.template --quiet -O /tmp/rl-read-only.template
Read-Write (Limited)	wget https://s3.amazonaws.com/redlock-public/cft/redlock-govcloud-read-and-write.template --quiet -O /tmp/rl-read-and-write.template

2. Enter the following command to deploy the updated CloudFormation template.

   Enter the correct name for the CloudFormation template, current stack name, role ARN and External ID to overwrite the current stack or enter new values to create a new stack.

Role	CLI Comand
Read-Only	aws cloudformation deploy --template-file /tmp/<RedLock-cloudformation-template-name> --stack-name <Stack Name> --parameter-overrides RedlockRoleARN=<Role ARN> ExternalID=<xxxxxxxxxx> --capabilities CAPABILITY_NAMED_IAM
Read-Write (Limited)	aws cloudformation deploy --template-file /tmp/<RedLock-cloudformation-template-name> --stack-name <Stack Name> --parameter-overrides RedlockRoleARN=<Role ARN> ExternalID=<xxxxxxxxxx> --capabilities CAPABILITY_NAMED_IAM

© 2019 Palo Alto Networks, Inc.

Onboard Your Azure Subscription

To begin monitoring and identifying compliance violations and vulnerabilities on your Azure commercial or Government environment, you must add your Azure subscriptions to Prisma Cloud. To successfully add your Azure subscriptions, you must enable authentication between Prisma Cloud and your Azure resources and configure the permissions required to read configuration data, flow logs, audit logs, and remediate issues that are identified on your Azure resources.

If you are have chosen to skip the guided tour, the high-level workflow is as follows:

- Azure Cloud Account Onboarding Checklist
- Set Up Your Azure Cloud Account Manually or Use the Azure PowerShell Script
- Add an Azure Subscription on Prisma Cloud
- Troubleshoot Azure Account Onboarding

Azure Cloud Account Onboarding Checklist

Prisma Cloud supports both Azure commercial and Azure Government. To successfully onboard and monitor the resources within your Azure subscription, use this checklist to authorize the correct set of access rights to Prisma Cloud:

- ❑ Collect your Azure Subscription ID from the Azure portal.

  Get your Azure Subscription ID. Make sure that you have Account Owner or Contributor privileges so that you can add Prisma Cloud as an application on your Azure Active Directory. To onboard your Azure subscription on Prisma Cloud, you'll need to set up an Active Directory application object (Application ID) and a Service Principal object (Object ID) that together enable API access. The process of setting up Prisma Cloud on Azure Active Directory will provide you with the keys and IDs that are required to establish an identity for sign-in and access to resources in your Azure subscription. The Service Principal ID defines the permissions and scope that is assumed by Prisma Cloud.
- ❑ Review the roles and associated permissions required:

Role	Description
Reader	The Reader role at the subscription level is required for Prisma Cloud to monitor the configuration of existing Azure resources within your Azure subscription. Prisma Cloud requires this role to ingest config and activity logs.

© 2019 Palo Alto Networks, Inc.

Role	Description
Reader and Data Access	The Reader and Data Access role at the subscription level is required for Prisma Cloud to fetch flow logs and storage account attributes so that you can use Prisma Cloud policies that assess risks in your storage account.This role includes the permissions to access the storage account keys and authenticate to the storage account in order to access the data. • *For Prisma Cloud to access flow logs stored in storage accounts that belong to subscriptions that are not monitored by Prisma Cloud, you must provide **Reader and Data Access** role on the storage accounts.* • *Reader and Data Access role is not a superset of the Reader role. Although this role has read-write access, Prisma Cloud only uses these permissions to access and read the flow log from the storage account.*
Network Contributor or a **custom role** to query flow log status	The built-in Network Contributor role can manage network data necessary to access and read flow logs settings for all Network Security Groups along with the details on the storage account to which the flow logs are written. It also enables auto-remediation of network related incidents. You can use the built-in role or create a custom role to allow Prisma Cloud to fetch flow log status. As a best practice Create a Custom Role on Azure to Enable Prisma Cloud to Access Flow Logs and use the least privilege principal to enable access only to the required permissions. The network contributor built-in role provides a much broader set of permissions than required by Prisma Cloud. *To create a custom role, you must have the **`Microsoft.Authorization/roleDefinitions/write`** permission on all AssignableScopes, such as Owner or User Access Administrator.* *You can then use the Azure CLI to create a custom role with the **`Microsoft.Network/networkWatchers/queryFlowLogStatus/action`***

© 2019 Palo Alto Networks, Inc.

Role	Description
	permission to query the status of flow logs.
Storage Account Contributor	(Optional, only required if you want to enable auto-remediation) The Storage Account Contributor role is required on all storage accounts to allow auto-remediation of policy violations.
Custom role with permissions	Optional, only required if you want to enable ingestion of the listed services. Create a custom role with the following permissions: • **`Microsoft.ContainerRegistry/registries/webhooks/getCallbackConfig/action`**—To ingest data from Azure Container Registry webhooks that are triggered when a container image or Helm chart is pushed to a registry, or deleted from it. • **`Microsoft.Web/sites/config/list/action`**—To ingest Authentication/Authorization data from Azure App Service that hosts websites and web applications. The Reader Role listed earlier is adequate to ingest configuration data from the Azure App Service.

Prisma Cloud provides a JSON file that makes it easier for you to create a custom role with the read-only permissions required to monitor your Azure resources.

- Enable Prisma Cloud to obtain network traffic data from Network security group (NSG) flow logs: NSG flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through an NSG.
  - Create one or more Network Security Groups, if you have none.
  - Create Azure Network Watcher instances for the virtual networks in every region where you collect NSG flow logs.

    Network Watcher enables you to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.
  - Create storage accounts. You must have a storage account in each region where you have NSGs. This is because flow logs are written to the same region as the NSGs. As a best practice, configure a single storage account to collect flow logs from all NSGs in a region.
  - Enable Network Watcher and register Microsoft.Insights provider.

    Microsoft.Insights is the resource provider namespace for Azure Monitor which provides features such as metrics, diagnostic logs, and activity logs.
  - Enable NSG flow logs version 1 or 2. Azure does not support NSG flow logs version 2 in all regions.
  - Verify that you can view the flow logs.

Continue to Set Up Your Azure Subscription for Prisma Cloud.

Set Up Your Azure Subscription for Prisma Cloud

Connect Prisma Cloud to your Azure cloud environment to monitor for threats and compliance violations, auto-remediate incidents, and identify hosts or containers with vulnerabilities. Before Prisma Cloud can

© 2019 Palo Alto Networks, Inc.

monitor the resources within your Azure subscription, you must add Prisma Cloud as an application to your Azure Active Directory and configure your Azure subscription to allow Prisma Cloud to analyze flow log data.

Prisma Cloud requires your Azure **Subscription ID** to identify your Azure cloud account and retrieve the storage account and key vault information. It also needs the **Directory ID**, **Application ID**, **Application Key**, and **Service Principal ID** to establish the connection between Prisma Cloud and Azure Active Directory and access the resources in your subscription.

STEP 1 | Locate and copy your Azure subscription ID.

Prisma Cloud requires the **Subscription ID** to identify your Azure cloud account and retrieve the storage account and key vault information.

1. Log in to Microsoft Azure, select **All services** > **Subscriptions**, select your subscription and copy the **Subscription ID**.

STEP 2 | Add Prisma Cloud as a new application on Azure Active Directory.

Registering Prisma Cloud as an application on Azure AD generates an Application ID. You need this ID and an Application key to authenticate Prisma Cloud on Azure and maintain a secure connection.

1. Log in to Microsoft Azure, select **Azure Active Directory** > **App registrations** > **New application registration**.

© 2019 Palo Alto Networks, Inc.

2. Enter a **Name** to identify the Prisma Cloud application, select the **Supported account types** that can use the application as **Accounts in this organizational directory only**, enter your log in URL for Prisma Cloud in **Redirect URI**, and click **Register**.

   The log in URL for Prisma Cloud is the URL you received in your order confirmation email, and it is the URL you use to log in to Prisma Cloud. This URL varies depending on your region.

3. Generate a client secret for the Prisma Cloud application.

   The client secret is the application password for Prisma Cloud.

   1. Select **Azure Active Directory** > **App Registrations** > **All Applications** and select the Prisma Cloud application.
   2. Select **Certificates & Secrets** > **New client secret**, to add a client secret (or the application password)
   3. Enter a **Description**, select a **Duration** which is the term of which the key is valid.
   4. Click **Add** and copy the value of the client secret.

      Make sure to copy this key value because you cannot view this key again. You need this application key when you Add an Azure Subscription on Prisma Cloud.

STEP 3 | Copy the information on the Prisma Cloud application from Azure Active Directory.

For Prisma Cloud to interact with the Azure APIs and collect information on your Azure resources, you require all the details listed in this step.

© 2019 Palo Alto Networks, Inc.

1. Select **Azure Active Directory** > **App Registrations** > **All Applications**, find the Prisma Cloud application you created and copy the **Directory ID**.

2. Select **Azure Active Directory** > **Enterprise Applications**.
3. Select your Prisma Cloud application **Properties**, and copy the **Application ID** and the **Object ID**.

   You must enter the Object ID as the Service Principal ID in the next step.

   Make sure to get the Object ID for the Prisma Cloud application from Enterprise Applications > All applications on the Azure portal, and not from App Registrations.

STEP 4 | Grant permissions for the Prisma Cloud application to access information at the Azure Subscription level.

To assign roles, you must have Owner or User Access Administrator privileges on your Azure Subscription.

1. Select **All Services** > **Subscriptions**.
2. Select your subscription and click **Access Control (IAM)** > **Add role assignment**.

© 2019 Palo Alto Networks, Inc.

3. Select the **Role**, verify Azure AD user, group, or service principal is selected in **Assign access to**, and select the administrative user to whom you want to assign the roles.

   Review the Azure Cloud Account Onboarding Checklist for a description of the roles and permissions that are required at the subscription level. Then decide which ones you must add for your security and monitoring needs—**Reader Role**, **Reader and Data Access Role**, Create a Custom Role on Azure to Enable Prisma Cloud to Access Flow Logs or **Network Contributor Role**, **Storage Account Contributor Role**.

STEP 5 | (Optional) Grant permissions for the Prisma Cloud application to access the Azure Key Vault service.

If you use Azure Key Vault to safeguard and manage cryptographic keys and secrets used by your cloud applications and services, Prisma Cloud needs permission to ingest key vault data.

1. From Azure, select **All Services** > **Key Vaults**.
2. Select your Key vault name and click **Access Policies**.

© 2019 Palo Alto Networks, Inc.

3. Click **Add new** > **Select Principal**, select your Prisma Cloud application and click **Select**.

4. Select List for **Key permissions**, List for **Secret permissions** and both List, and List Certificate Authorities for **Certification permissions** and click **OK**.

STEP 6 | On the Azure portal, Enable Network Watcher and register Insights provider.

STEP 7 | On the Azure portal,Create a storage account on Azure for NSG flow logs.

© 2019 Palo Alto Networks, Inc.

Your Azure storage account stores flow logs necessary for Prisma Cloud to monitor and analyze network traffic. When Prisma Cloud ingests the data in these logs, you can interact with the information in Prisma Cloud. You can for example, run queries against it, visualize network topology, and investigate traffic flows between two instances. You can also apply network policies on this traffic.

Set the log retention period to at least 15 days, if you do not have regulatory guidelines to which you must adhere.

STEP 8 | On the Azure portal,Enable NSG flow logs.

STEP 9 | Configure Prisma Cloud Reader and Data Access role for your Azure storage account.

To ingest Azure flow logs you have to grant access to the storage account in which the logs are stored. The Reader and Data Access role provides the ability to view everything and also allows read/write access to all data contained in a storage account using the associated storage account keys If your flow logs are stored in storage accounts that belong to one or more subscriptions which are not monitored by Prisma Cloud, you must provide the Prisma Cloud application with Reader and Data Access role to each storage account.

1. After creating your storage account, select **Access control (IAM)** > **Add role assignment**.

2. Select **Reader and Data Access** in Role, select the administrative user to whom you want to assign the role to and click **Save**.

STEP 10 | Add an Azure Subscription on Prisma Cloud.

© 2019 Palo Alto Networks, Inc.

Create a Custom Role on Azure to Enable Prisma Cloud to Access Flow Logs

To enable Prisma Cloud to access Azure flow logs and monitor flow-related data, such as volume of traffic generated by a host, top sources of traffic to the host, or identify which ports are in use, you need to provide the required permissions. While you can use the built-in Network Contributor role that enables a much broader set of permissions, as a best practice create a custom role so that you follow the principle of least privilege and limit access rights to the bare minimum. Use the Azure Cloud Account Onboarding Checklist to verify what services you want to ingest data on and manually assign the permissions for this custom role or use the JSON file (link below) with the permissions required. To create a custom role, install Azure CLI and create a limited role named **Prisma Cloud - Flow Logs Setting Reader** and then enable the role to access flow logs.

STEP 1 | Create a custom role using Azure CLI.

If you have already assigned a Network Contributor Role to an Azure user, you can skip this step and go to Step 2. You have two options for defining custom roles, create a custom role JSON file manually or use the JSON file that Prisma Cloud provides for you.

- Use the JSON file that Prisma Cloud provides with the permissions required.
  1. Download and save the JSON file from here.
  2. Install the Azure CLI and log in to Azure.
  3. Log in to the Azure portal from the same Windows system and complete the following steps.
     1. Open a PowerShell window (or a DOS Command Prompt Window)
     2. Go to the directory where you stored the JSON file.
     3. Enter the following Azure CLI command; if you renamed the file, you will need to replace the JSON filename to match that in the command below.

```
az role definition create --role-definition
"azure_prisma_cloud_lp_read_only.json"
```

- Create a custom role JSON file manually.
  1. Install the Azure CLI and log in to Azure.
  2. Open a text editor (such as notepad) and enter the following command in the JSON format to create a custom role.You can create custom roles using Azure PowerShell, Azure CLI, or the REST API. The steps here use the Azure CLI command (run on Powershell or on the DOS command prompt) to create the custom role with queryFlowLogStatus permission. Replace xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx in the last line with your Azure Subscription ID.
  3. Save the JSON file on your local Windows system and give it a descriptive name, such as ad-role-cli.json.
  4. Log in to the Azure portal from the same Windows system and complete the following steps.
     1. Open a PowerShell window (or a DOS Command Prompt Window)
     2. Go to the directory where you stored the JSON file.
     3. Enter the following Azure CLI command; you will need to replace the JSON filename to match what you named it.

```
az role definition create --role-definition "ad-role-
cli.json"
```


© 2019 Palo Alto Networks, Inc.

The output is as follows:

```
          {"assignableScopes": [    "/subscriptions/
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"  ],    "description": "Allows
 Reading Flow Logs Settings",    "id": "/subscriptions/16dfdbcc-
e407-4fbe-9096-e7a97ee23fb5/providers/Microsoft.Authorization/
roleDefinitions/088c8f48-201c-4f8d-893f-7716a8d58fa1",    "name":
 "088c8f48-201c-4f8d-893f-7716a8d58fa1",    "permissions":    [{
          "actions": [        "Microsoft.Network/networkWatchers/
queryFlowLogStatus/action"],          "dataActions": [],
       "notActions": [],          "notDataActions": []
  }],    "roleName": "RedLock Flow Log Settings Reader",
 "roleType": "CustomRole",    "type": "Microsoft.Authorization/
roleDefinitions"}
```

STEP 2 | Configure the custom role to access flow logs.

1. Log in to the Microsoft Azure Portal.
2. Select **All services** > **Subscriptions** and select your subscription.
3. Select **Access control (IAM)** > **Add role assignment**

   In the Role drop-down, verify that you can see the new custom role that you created.
4. Assign the **Role** to Prisma Cloud and enable the permission to query flow log status and **Save** your changes.

Use the Azure PowerShell Script to Add an Azure Account

To save time and reduce the likelihood of human error, you can use the Azure PowerShell Az module to automate the process of setting up the Prisma Cloud application on your Microsoft Azure cloud environment. Because this script adds the Prisma Cloud application on your Azure Active Directory, you must be an administrator with authorization to create roles, and add an application to manage your Azure subscription.

STEP 1 | Download the RedLock Azure Onboarding script.

STEP 2 | Launch Azure Cloud Shell.

Verify that you are in Power

STEP 3 | Upload the RedLock Azure Onboarding script.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Verify the script is in the local directory and then enter **./RedLock-Azure-Onboarding-Beta-V5.ps1**

By default, the file is uploaded to your home directory and you might need to use **`cd ~`** and then enter **./RedLock-Azure-Onboarding-Beta-V5.ps1**

STEP 5 | When prompted, enter your Azure **SubscriptionID**, a name to identify the RedLock application for example, **`APPNAME-RedLock-V2`**, and the URL that you use to access Prisma Cloud, for example **`https://app.redlock.io`**.

```
PS /home/[redacted]> ls
clouddrive  Redlock-Azure-Onboarding-Beta-V2.ps1
PS /home/[redacted]> ./Redlock-Azure-Onboarding-Beta-V2.ps1

cmdlet Redlock-Azure-Onboarding-Beta-V2.ps1 at command pipeline position 1
Supply values for the following parameters:
azSubId: 67d[redacted]
applicationName: APPNAME-Redlock-V2
applicationURI: https://[redacted].redlock.io
```

STEP 6 | When prompted, open the link on your browser.

```
You should be prompted with a browser window, Login to Azure with user who has permissions to create Application,Roles,ServicePrincipal and change Application permissions.
WARNING: To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code AX[redacted] to authenticate.
```

STEP 7 | Log in to Windows Azure PowerShell.

Log in to Azure using an account with Owner or Admin access.

STEP 8 | Enter the authentication code and click **Continue** to log in to Windows Azure PowerShell.

© 2019 Palo Alto Networks, Inc.

STEP 9 | Verify the details on successful completion of the process.

The Azure PowerShell window displays the results of the script. It is also saved to a file named Subscription-ApplicationName.txt

1. The **Application ID**.

```
Secret                : System.Security.SecureString
ServicePrincipalNames : {f36b0f[illegible], https://app.redlock.io}
ApplicationId         : f36b0[illegible]
ObjectType            : ServicePrincipal
DisplayName           : APPNAME-Redlock-V2
Id                    : a4821c[illegible]
Type                  :
```

2. The **Reader** role.

```
RoleAssignmentId   : /subscriptions/67d7e[illegible] provi
Scope              : /subscriptions/67d7e[illegible]
DisplayName        : APPNAME-Redlock-V2
SignInName         :
RoleDefinitionName : Reader
RoleDefinitionId   : acdd72[illegible]
ObjectId           : a4821d[illegible]
ObjectType         : ServicePrincipal
CanDelegate        : False
```

STEP 10 | Generate the Application Key (client secret) for the Prisma Cloud application.

The script does not create the application key. To generate an application key (Step 2-3), you must log in to the Azure portal.

STEP 11 | Copy the Prisma Cloud application details from Azure Active Directory.

Prisma Cloud requires the Directory ID, Application ID, Application Key, and Service Principal ID to establish the connection between Prisma Cloud and Azure Active Directory and access the resources in your subscription.

STEP 12 | Continue to Add an Azure Subscription on Prisma Cloud.

Add an Azure Subscription on Prisma Cloud

Connecting Prisma Cloud to your Azure cloud account enables you to analyze and monitor traffic logs, and detect potential malicious network activity or compliance issues. To enable API access between Prisma Cloud and your Microsoft Azure Subscription, you need to gather account information about your

© 2019 Palo Alto Networks, Inc.

subscription and Prisma Cloud that you registered on Azure Active Directory so that Prisma Cloud can monitor the resources in your cloud account. See Set Up Your Azure Subscription for Prisma Cloud for help.

STEP 1 | Add your Azure subscription on Prisma Cloud.

1. Log in to Prisma Cloud.
2. Select **Settings** > **Cloud Accounts** > **Add New**
3. Enter a **Cloud Account Name**.
4. Select **Cloud Type** Azure and the environment where your resources are deployed—**Government** or **Commercial**, click **Next**.

5. Enter your Azure **Subscription ID**, **Active Directory ID**, **Application ID**, **Application Key** and **Service Principal Id**.

6. Select **Ingest & Monitor Network Security Group flow logs** and click **Next**.

   Network security group (NSG) flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through an NSG. Make sure that Azure Flow logs are stored within a storage account in the same region as the NSG. See Azure Cloud Account Onboarding Checklist for the set up details to ensure that Prisma Cloud can successfully ingest NSG flow logs.
7. Select the **Account Groups** you want to add and click **Next**.

   You must assign each cloud account to an account group, and Create an Alert Rule to associate the account group with it to generate alerts when a policy violation occurs.

8. Verify the **Status** and **Save** your changes.

© 2019 Palo Alto Networks, Inc.

If Prisma Cloud was able to successfully make an API request to retrieve the Azure flow logs, the status is displayed with a green check mark. If Prisma Cloud is unable to retrieve the logs, the error message indicates what failed. See Troubleshoot Azure Account Onboarding for help.

STEP 2 | Verify that you can view the information on your Azure resources on Prisma Cloud.

Wait for approximately 10-24 hours after you onboard the Azure subscription to Prisma Cloud, to review the data that was collected about your Azure resources. After Prisma Cloud ingests data, the information is available for compliance checks, configuration review, audit history, and network visualization.

It takes about four to six hours before you can view flow logs in Prisma Cloud. Prisma Cloud ingests flow logs from the previous seven days from when you onboard the account.

1. Log in to Prisma Cloud.
2. Select **Investigate** and enter the following RQL query.

   This query allows you to list all network traffic from the Internet or from Suspicious IP addresses with over 0 bytes of data transferred to a network interface on any resource on any cloud environment.

```
        network where cloud.account = '{{cloud account name}}' AND
source.publicnetwork IN ('Internet IPs', 'Suspicious IPs') AND bytes >
0
```

Troubleshoot Azure Account Onboarding

After you have completed onboarding your Azure subscription to Prisma Cloud, use these checks to resolve issues if Prisma Cloud cannot retrieve logs and metadata including resource configurations, user activities, network traffic, host vulnerabilities/activities on your Azure resources. Without enabling the correct permissions and configuration on the Azure portal and on Prisma Cloud, you'll be unable to identify, detect, and remediate issues to manage the risks in your environment.

- Verify that the cloud account permissions are accurate on **Settings** > **Cloud Accounts** > **Cloud_Account_Name** > **Status**.

  At every ingestion cycle when Prisma Cloud connects to the Azure subscription to retrieve and process the data, the service validates that you continue to have the permissions required to continue

© 2019 Palo Alto Networks, Inc.

monitoring the resources within your Azure subscription. Periodically, review the status of these checks to learn of any changes or modifications that limit your ability to maintain visibility and security governance over the resources within your Azure subscription.

- Reader role, and Reader and Data Access role at the subscription level.

  If you see the error Subscription does not have Reader role(s) assigned, verify that you have entered the correct Service Principal ID. On the Azure portal, the Object ID for the Prisma Cloud application is what you must provide as the Service Principal ID on Prisma Cloud. Make sure to get the Object ID for the Prisma Cloud application from Enterprise Applications > All applications on the Azure portal.

- Checks for the Network Contributor role or Custom role that is required to query flow log status.
- Checks for the Reader and Data Access role on the storage accounts to access the flow logs stored in storage buckets in subscriptions that are not monitored by Prisma Cloud.
- Checks for the Storage Account Contributor role (optional and required only for remediation) that is required for auto remediation of policy violations related to storage accounts.
- Checks whether flow logs are published to the storage account.

- Check that Azure flow logs are being generated and written to the storage account.
  1. Log in to the Azure portal.
  2. Select **Storage Accounts** and select the storage account that you want to check.
  3. Select **Blobs** > **Blob Service** and navigate through the folders to find the *.json files.

     These are the flow logs that Prisma Cloud ingests.

- On the Azure portal, check that you have created storage accounts in the same regions as the Network Security Groups.

  Network security group (NSG) flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through an NSG. Azure flow logs must be stored within a storage account in the same region as the NSG.

© 2019 Palo Alto Networks, Inc.

1. Log in to Prisma Cloud.
2. Select **Investigate** and enter the following RQL query **`network where source.publicnetwork IN ('Internet IPs', 'Suspicious IPs') AND bytes > 0`**

   This query allows you to list all network traffic from the Internet or from Suspicious IP addresses with over 0 bytes of data transferred to a network interface on any resource on any cloud environment.

- On the Azure portal, verify that you have enabled Network Watcher instance.

  The Network Watcher is required to generate flow logs on Azure.

  1. Log in to the Azure portal and select **Network Watcher** > **Overview** and verify that the status is **Enabled**.

  2. Log in to Prisma Cloud.
  3. Select **Investigate** and enter the following RQL query **`config where cloud type ='azure' AND api.name ='azure-network-nsg-list' addcolumn provisioningState`**.

- On the Azure portal, check that you have enabled flow logs on the NSGs.

  1. Log in to the Azure portal, and select **Network Watcher** > **NSG Flow Logs** and verify that the status is **Enabled**.

  2. Log in to Prisma Cloud.

© 2019 Palo Alto Networks, Inc.

3. Select **Investigate** and enter the following RQL query **`network where source.publicnetwork IN ('Internet IPs', 'Suspicious IPs') AND bytes > 0`**

   This query allows you to list all network traffic from the Internet or from Suspicious IP addresses with over 0 bytes of data transferred to a network interface on any resource on any cloud environment.

© 2019 Palo Alto Networks, Inc.

Onboard Your Google Cloud Platform Account

To enable Prisma Cloud to retrieve data on your Google Cloud Platform (GCP) resources and identify potential security risks and compliance issues, you must connect your GCP accounts to Prisma Cloud. In keeping with the GCP resource hierarchy, you can choose whether you want Prisma Cloud to monitor one or more GCP Projects or all projects that are under your GCP Organization. Regardless of what you choose, the process of onboarding requires you to create a service account, create and associate roles with the service account, and enable specific APIs.

The high-level workflow to start monitoring your GCP resources is as follows:

- Set Up Your GCP Account for Prisma Cloud
- Add Your GCP Project to Prisma Cloud
- Add Your GCP Organization to Prisma Cloud

Set Up Your GCP Account for Prisma Cloud

Before Prisma Cloud can analyze and monitor your Google Cloud Platform account, you must create a service account, create and associate roles to the service account and enable specific APIs. These accounts, roles and APIs enable Prisma Cloud to retrieve data about your GCP resources and identify potential security risks and compliance issues. You must configure your GCP account whether you elect to add a GCP project or organization to Prisma Cloud.

STEP 1 | Create a Prisma Cloud Viewer custom role on the GCP console.

Prisma Cloud needs this custom role to grant cloud storage bucket permission to read storage bucket metadata and update bucket IAM policies.

1. Log in to the GCP console, select your organization, and select **IAM & Admin** > **Roles** > **Create Role**.
2. Enter a **Title** and **Description**.
3. Verify that **ID** is set to CustomRole and select **General Availability** in the **Role launch stage** drop-down.

© 2019 Palo Alto Networks, Inc.

4. Click **+ ADD PERMISSIONS**, select **storage.buckets.get** to retrieve your list of storage buckets, and **storage.buckets.getIampolicy** to retrieve the IAM policy for the specified bucket.
5. Click **Add**.

6. Click **Create**.

STEP 2 | Create a GCP service account.

You need a service account, which is an authorized identity, to enable authentication between Prisma Cloud and GCP. Because you can create a service account under a GCP project only and not directly under the GCP Organization, you must select a project when you create the service account.

1. Select your project and select **Service accounts** > **+ CREATE SERVICE ACCOUNT**.

2. Enter **Service account name**, **Service account ID**, **Service account description** and click **Create**.

© 2019 Palo Alto Networks, Inc.

STEP 3 | Grant the service account permissions to access your GCP project.

The service account must have three roles to analyze and monitor your resources and data on GCP:

- Viewer—Primitive role on GCP.
- Prisma Cloud Viewer— Custom role that you created in Step 1.
- Compute Security Admin—Predefined role on GCP. An optional privilege that is required for auto-remediation.

1. Select **Project** > **Viewer** and click **+ ADD ANOTHER ROLE**.

   The Project Viewer role is a primitive role allowing Prisma Cloud read-only access to the resources or data in your selected project or projects.
2. Select **Custom** > **Prisma Cloud Viewer** (or another custom name) and click **+ ADD ANOTHER ROLE**.

   This custom role allows Prisma Cloud to read storage bucket metadata and IAM policies associated with the selected project.
3. Select **Compute Engine** > **Compute Security Admin** and click **Continue**.

   (Optional role, only required for enabling auto-remediation) The Compute Security Admin is a predefined role that allows full control to remediate any incidents or policy violations on compute engine resources.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Create a security key for the service account.

The service account security key is used for service-to-service authentication within GCP. The private key file is required to authenticate API calls between your GCP projects and Prisma Cloud.

1. Click **+ CREATE KEY**.

   See Create a key, if you are modifying an existing service account.
2. Select **Key type** as **JSON**.
3. **Create** the key and download the JSON private key file for the service account.

STEP 5 | Enable GCP APIs for your GCP project.

Prisma Cloud can ingest data from several GCP APIs. While you must enable Stackdriver Logging API (logging.googleapis.com) to monitor audit logs, for all the other APIs, you can opt to enable only the ones you are using and want Prisma cloud to monitor across your cloud accounts.

1. Go to the GCP Console API Library and select your GCP project.
2. Select **Enable APIs and Services**.

© 2019 Palo Alto Networks, Inc.

3. Enable the APIs.

   You can either enable all the necessary APIs using the Google Command Line Interface as follows:

```
gcloud services enable compute.googleapis.com sql-
component.googleapis.com storage-component.googleapis.com
 iam.googleapis.com container.googleapis.com logging.googleapis.com
 monitoring.googleapis.com cloudresourcemanager.googleapis.com
 cloudkms.googleapis.com bigquery-json.googleapis.com dns.googleapis.com
```

   or search for each API is in the list and enable them from the Google cloud console.

API	Description	Service Name
BigQuery API	Allows you to create, manage, share, and query data.	`bigquery-json.googleapis.com`
Cloud Resource Manager API	Creates, reads, and updates metadata for Google Cloud Platform resource containers.	`cloudresourcemanager.googleapis.c`

© 2019 Palo Alto Networks, Inc.

API	Description	Service Name
Cloud Key Management Service (KMS) API	Google Cloud KMS allows customers to manage encryption keys and perform cryptographic operations with those keys.	`cloudkms.googleapis.com`
Cloud SQL Admin API	API for Cloud SQL database instance management.	`sqladmin.googleapis.com`
Compute Engine API	Creates and runs virtual machines on the Google Cloud Platform.	`compute.googleapis.com`
Google Cloud DNS API	Google Cloud DNS translates requests for domain names into IP addresses and manages and publishes DNS zones and records.	`dns.googleapis.com`
Google Cloud Storage	Google Cloud Storage is a RESTful service for storing and accessing your data on Google's infrastructure.	`storage-component.googleapis.com`
Identity and Access Management (IAM) API	Manages identity and access control for GCP resources, including the creation of service accounts, which you can use to authenticate to Google and make API calls.	`iam.googleapis.com`
Kubernetes Engine API	Builds and manages container-based applications, powered by the open source Kubernetes technology.	`container.googleapis.com`
Stackdriver Monitoring API	Manages your Stackdriver Monitoring data and configurations.	`monitoring.googleapis.com`
Stackdriver Logging API	Writes log entries and manages your Logging configuration.	`logging.googleapis.com`

4. Verify you have enabled all the APIs listed above.

   You can use the GCP APIs and Services Dashboard (screenshot below) to verify or use the command **`gcloud services list`** on the Google Command Line Interface.

© 2019 Palo Alto Networks, Inc.

STEP 6 | Associate additional GCP projects with the service account and create a custom role within each project.

Because the service account and custom roles are associated with a GCP project, if you plan to add more than one GCP project to Prisma Cloud but not the GCP organization, you must associate each project with the service account and then connect your service account to Prisma Cloud.

This step is not required if you want to add just one project, you can continue to Add Your GCP Project to Prisma Cloud. *If you want to ensure that all current and future projects and cloud resources within your organization are automatically monitored by Prisma Cloud, you can configure Prisma Cloud to Automatically onboard projects that are accessible by this service account. when you* Add Your GCP Organization to Prisma Cloud.

1. Copy the service account member address.

   To copy the service account member address, first select the project that you used to set up the service account, then find the service account member address from **IAM & admin** > **IAM**.

2. Select the project you want to add (from the Project drop-down), and click **Add**.
3. Add the service account member address you copied as **New members**, and **Select a role**.
4. Select **Project** > **Viewer**, and click **+ ADD ANOTHER ROLE**.
5. Select **Compute Engine** > **Compute Security Admin**.

© 2019 Palo Alto Networks, Inc.

6. **Save** your changes.
7. Create a Prisma Cloud Viewer custom role on the GCP console for this project.

   If you do not want to add all your GCP projects within the GCP Organizational level grouping, you need to create the custom Prisma Cloud Viewer role for each project.
8. Add the custom role to the service account.
   1. Select **IAM & Admin** > **IAM**, and select the service account.
   2. Edit the permissions to **+ ADD ANOTHER ROLE**
   3. Select **Custom** > **Prisma Cloud Viewer**, and click **Save**.

9. Repeat the steps above for any additional projects you want to onboard to Prisma Cloud.

STEP 7 | (Optional) Enable Flow Logs for GCP Projects or Enable Flow Logs for GCP Organization.

When you enable flow logs, the service ingests flow log data for the last seven days. Then if flow logs become unavailable for any reason such as if you manually disabled flow logs, modified API permissions, or an internal error occurred, when access is restored, logs from the preceding seven days only are ingested.

STEP 8 | Add Your GCP Project to Prisma Cloud or Add Your GCP Organization to Prisma Cloud.

Add Your GCP Project to Prisma Cloud

After you have Set Up Your GCP Account for Prisma Cloud and associated your projects to a service account, you can add your project or projects to Prisma Cloud.

© 2019 Palo Alto Networks, Inc.

After you start monitoring your project using Prisma Cloud, if you delete the project on GCP, Prisma Cloud learns about it and automatically deletes the account from the list of monitored accounts on Settings > Cloud Accounts. To track the automatic deletion of the project, an audit log is generated with information on the name of the deleted account and the date that the action was performed.

STEP 1 | Log in to Prisma Cloud to add your GCP project or projects.

1. Click Settings and select **Cloud Accounts**.
2. Click **+ Add New** and then enter the **Cloud Account Name** and select **GCP** as the **Cloud Type**.
3. Select **Project** for **Onboard Using**.
4. Enter the name of the Cloud Storage bucket configured when you Enabled Flow Logs for your GCP Projects and click **Next**.

5. Upload your **Service Account Key (JSON)** file, review the GCP onboarding configuration displayed on screen to verify that it is correct, and click **Next.**

If you have multiple GCP projects, enable Automatically onboard projects that are accessible by this service account. to allow Prisma Cloud to monitor all current and future GCP projects associated with the Service Account.

© 2019 Palo Alto Networks, Inc.

6. Click **Confirm** to allow Prisma Cloud to monitor all current and future GCP projects associated with the service account.

7. Select the account groups to associate to your project and click **Next**.

   Account groups are comprised of selected Prisma Cloud users with permission to access Cloud accounts.
8. **Save** the changes.

STEP 2 | Verify the onboarding status of your GCP project to Prisma Cloud.

You can review the status and take necessary actions to resolve any issues encountered during the onboarding process by viewing the **Cloud Accounts** page. It takes between 4-24 hours for the flow log data to be exported and analyzed before you can review it on Prisma Cloud. To verify if the flow log data from your GCP project has been analyzed, you can run a network query on the **Investigate** page.

1. Go to **Cloud Accounts**, locate your GCP project and view the status.

© 2019 Palo Alto Networks, Inc.

ACCOUNT ID	CLOUD	NAME	TYPE	ACCOUNT GROUPS	STATUS	LAST MODIFIED BY
		Redlock Rocks		dummy	NA	
		gcp-redlock-qa-static		dummy, gcp-redlock-qa-static	NA	
		RedLock Sandbox		Temporary All Accounts Group	Error	
		ev-aws-5390		ev-account-group	Error	
		ev-aws-9491		ev-account-group	Error	
		ev-azure-d23			Error	
		Redlock GCP Dev Playgroundd		Temporary All Accounts Group	Success	
		Redlock QA Automation		dummy, Redlock QA Automation	Warning	
		Azure-Microsoft Azure Sponsorship		Temporary All Accounts Group	Warning	

2. Go to **Investigate**, replace the name with your GCP Cloud Account name and enter the following network query.

   This query allows you to list all network traffic from the Internet or from Suspicious IP addresses with over 0 bytes of data transferred to a network interface on any resource on any cloud environment.

```
network where cloud.account = ‘{{cloud account name}}’ AND
source.publicnetwork IN (‘Internet IPs’, ‘Suspicious IPs’) AND bytes >
0
```

Enable Flow Logs for GCP Projects

With VPC flow logs, Prisma Cloud helps you visualize flow information for resources deployed in your GCP projects. VPC flow logs on GCP provide flow-level network information of packets going to and from network interfaces that are part of a VPC, including a record of packets flowing to a source port and destination port, the number of distinct peers connecting to an endpoint IP address and port, so that you can monitor your applications from the perspective of your network. On the **Investigate** page, you can view the traffic flow between virtual machines in different service-projects and/or host-projects that are using shared VPC network and firewall rules.

To analyze these logs on Prisma Cloud you must enable VPC flow logs for each VPC subnet and export the logs to a *sink* that holds a copy of each log entry. Prisma Cloud requires you to export the flow logs to a single Cloud Storage bucket, which functions as the sink destination that holds all VPC flow logs in your environment. When you then configure Prisma Cloud to ingest these logs, the service can analyze this data and provide visibility into your network traffic and detect potential network threats such as crypto mining, data exfiltration, and host compromises.

© 2019 Palo Alto Networks, Inc.

If your Prisma Cloud tenant is on https://app.prismacloud.io, please contact Palo Alto Networks Support to enable GCP flow logs.

STEP 1 | Enable flow logs for your VPC networks on GCP.

To analyze your network traffic, you must enable flow logs for each project you want Prisma Cloud to monitor.

1. Log in to GCP console and select your project.
2. Select **Navigation menu** > **VPC network** > **VPC networks**.

3. Select VPC network and click **EDIT**.
4. Select **Flow logs On** to enable flow logs.

5. Set the **Aggregation Interval** to **15 min**.

© 2019 Palo Alto Networks, Inc.

6. Set the **Sample rate** to 100%.

   As a best practice, setting the aggregate interval and the sample rate as recommended above generates alerts faster on Prisma Cloud and reduces network costs you incur.

7. **Save** your changes.

STEP 2 | Create a Sink to export flow logs.

You must create a sink and specify a Cloud Storage bucket as the export destination for VPC flow logs. You must configure a sink for every project that you want Prisma Cloud to monitor and configure a single Cloud Storage bucket as the sink destination for all projects. When you Add Your GCP Project to Prisma Cloud, you must provide the Cloud Storage bucket from which the service can ingest VPC flow logs. As a cost reduction best practice, set a lifecycle to delete logs from your Cloud Storage bucket.

1. Select **Navigation menu** > **Logging** > **Logs**

2. Select **GCE Subnetwork**.
3. Change **All logs** to **compute.googleapis.com/vpc_flows** and click **OK**.
4. Click **CREATE EXPORT**.

© 2019 Palo Alto Networks, Inc.

5. Enter a name and select **Cloud Storage** as the **Sink Service**.
6. Select an existing Cloud Storage bucket or create a new Cloud Storage bucket as the **Sink Destination**, and click **Create Sink**.

© 2019 Palo Alto Networks, Inc.

7. Add a lifecycle rule to limit the number of days you store flow logs on the Cloud Storage bucket.

   By default, logs are never deleted. To manage cost, specify the threshold (in number of days) for which you want to store logs.

   1. Select **Navigation Menu** > **Storage** > **Browser**.
   2. Select the **Lifecycle** link for the storage bucket you want to modify.

   3. **Add rule** and Select object conditions to set **Age** to 30 days and Select Action as **Delete**.

      Logs that are stored on your Cloud Storage bucket will be deleted in 30 days.
   4. Select **Continue** and **Save** your changes.

STEP 3 | Add the name of the Cloud Storage bucket you referenced above in **Flow Logs Storage Bucket** when you Add Your GCP Project to Prisma Cloud.

Add Your GCP Organization to Prisma Cloud

After configuring your Google Cloud Platform account, associate your GCP Organization with your service account to automatically enable Prisma Cloud to onboard all GCP current and future projects.

© 2019 Palo Alto Networks, Inc.

If you have added a GCP project to Prisma Cloud and you now want to add the GCP Organization to which the project belongs, the existing GCP project is moved under the Organization in Prisma Cloud.

STEP 1 | Complete steps 1-5 in Set Up Your GCP Account for Prisma Cloud.

You must enable the APIs mentioned in Step 5 in the link above for all projects under the GCP Organization.

STEP 2 | Create the custom role at the GCP Organization level.

See 1 Make sure to select your GCP Organization in the drop-down.

STEP 3 | Associate your service account to the GCP Organization.

A service account is an identity to which you can grant granular permissions instead of creating individual user accounts. To monitor all the GCP projects that are within the GCP Organizational hierarchy, the service account requires four roles. Of the four roles, three are common for granting permissions at the GCP project level too; the Organization Viewer role is additionally required to grant access to the Organization's properties:

- Viewer—Primitive role.
- Compute Security Admin—Predefined role.
- RedLock Viewer—Custom role.
- Organization Viewer—Predefined role.

1. Copy the service account member address.

   Select the project that you used to create the service account, and select **IAM & admin** > **IAM** to copy the service account member address.

© 2019 Palo Alto Networks, Inc.

2. Select your Organization, select **IAM & admin** > **IAM** to **Add** members to the service account.
3. Paste the service account member address you copied as **New members**, and **Select a role**.
4. Select **Project** > **Viewer**, and click **+ ADD ANOTHER ROLE**.

   The Project Viewer role enables read-only access to the resources or data in your Organization.
5. Select **Compute Engine** > **Compute Security Admin**.

   The Compute Security Admin role includes the permissions to remediate any incidents or policy violations.
6. Select **Custom** > **RedLock Viewer**, and click **+ ADD ANOTHER ROLE**.

   This custom role enables permissions to read storage bucket metadata and IAM policies associated with your Organization.
7. Select **Resource Manager** > **Organization Viewer**, and click **Save**.

   The Organization Viewer role enables permissions to view the Organization name without granting access to all resources in the Organization.

STEP 4 | Log in to Prisma Cloud to add your GCP Organization.

After you add the GCP Organization to Prisma Cloud, you must create a support request to delete the GCP Organization or the projects within your GCP Organization. You cannot delete the account from Prisma Cloud.

Because Prisma Cloud has access to all projects associated with a Service Account, if you want to remove access to a project that is associated with the Service Account, you must remove the project from the Service Account on the GCP IAM console. In the next scanning cycle, the project is excluded and Prisma Cloud no longer has access to the project.

© 2019 Palo Alto Networks, Inc.

1. Click Settings and select **Cloud Accounts** and click **+ Add New**.
2. Enter the **Cloud Account Name**.
3. Select **GCP** as the**Cloud Type**.
4. Select **Organization** for **Onboard Using** and click **Next**.

5. Enter the name of the Cloud Storage bucket you configured when you Enabled Flow Logs for your GCP Organization in **Flow Logs Storage Bucket** and click **Next**.
6. Enter your **Organization Name** and **Organization ID**.

   To find your GCP Organization ID, log in to the GCP console and select your organization.

7. Upload your **Service Account Key (JSON)** file, and verify that the GCP onboarding configuration displayed on screen is accurate before you click **Next.**

© 2019 Palo Alto Networks, Inc.

8. Click **Confirm** to allow Prisma Cloud to automatically onboard current and future GCP projects under the GCP Organization hierarchy.

9. Select the account groups to associate to the GCP Organization and click **Next**.

   Account groups are comprised of selected Prisma Cloud administrators who have permission to access cloud accounts.

10. **Save** your changes.

STEP 5 | Verify the onboarding status of your GCP Organization to Prisma Cloud.

Click Settings and select **Cloud Accounts** to review the status and take necessary actions to resolve any issues that my occur during the onboarding process. It takes between 4-24 hours for Prisma Cloud to ingest the flow log data.

1. From the **Cloud Accounts** page, locate your GCP organization and view the status.

© 2019 Palo Alto Networks, Inc.

ACCOUNT ID	CLOUD	NAME	TYPE	ACCOUNT GROUPS	STATUS	LAST MODIFIED B
		Redlock Rocks		dummy	NA	
		gcp-redlock-qa-static		dummy, gcp-redlock-qa-static	NA	
		RedLock Sandbox		Temporary All Accounts Group	Error	
		ev-aws-5390		ev-account-group	Error	
		ev-aws-9491		ev-account-group	Error	
		ev-azure-d23			Error	
		Redlock GCP Dev Playgroundd		Temporary All Accounts Group	Success	
		Redlock QA Automation		dummy, Redlock QA Automation	Warning	
		Azure-Microsoft Azure Sponsorship		Temporary All Accounts Group	Warning	

2. Select **Investigate**, replace the name with your GCP Cloud Account name and enter the following network query.

   To verify if the flow log data from your GCP organization has been successfully ingested, use the following network query

```
network where cloud.account = 'GCP Cloud Account Name' AND
 dest.publicnetwork IN ('Internet IPs' , 'Suspicious IPs' ) and bytes > 0
```


© 2019 Palo Alto Networks, Inc.

Enable Flow Logs for GCP Organization

Prisma Cloud uses the traffic data in flow logs for your GCP organization to detect network threats such as cryptomining, data exfiltration, and host compromises. Before Prisma Cloud can analyze your flow log data, you must create a sink to export the flow logs to a Cloud Storage bucket. To configure a sink for your whole GCP organization, use the gcloud command line tool.

If your tenant is hosted on https://app.prismacloud.io, please contact Palo Alto Networks Support to enable GCP flow logs.

STEP 1 | Gather the following information from your GCP account:

- Cloud Storage bucket name
- Organization ID

STEP 2 | Download and install the Google Cloud SDK.

During the SDK install, you must log in to your GCP account. This account must have these three permissions enabled at the organization level:

- Billing Account Administrator
- Logging Admin
- Organization Administrator

STEP 3 | Run this command to create a service account needed to configure the sink for your Cloud Storage bucket but replace the **Bucket-name** with your Cloud Storage bucket name and **Organization ID** with your organization ID.

```
$ gcloud logging sinks create rl-org-level-sink
storage.googleapis.com/<Bucket-name> --include-children --
```


© 2019 Palo Alto Networks, Inc.

```
organization=<Organization ID> --log-filter="resource.type=
\"gce_subnetwork\""
```

STEP 4 | Grant the service account permission to access your Cloud Storage bucket.

1. Select **Navigation menu** > **Storage** and select your Cloud Storage bucket.
2. Select **Permissions** > **Add members**.
3. Add the service account email address for **Members**, select **Storage** > **Storage Admin** and select **Add**.

STEP 5 | Add the name of Cloud Storage bucket you created above in **Flow Logs Storage Bucket** when you Add Your GCP Organization to Prisma Cloud.

Manage Prisma Cloud Administrators

Role-based access controls allow you to restrict access to the cloud accounts based on a user's role in the organization. For example, you can assign groups of accounts to a line of business cloudOps, DevOps, and SecOps owners to restrict their access to Prisma Cloud for the accounts they own.

> Prisma Cloud Administrator Roles
> Create Account Groups
> Manage Prisma Cloud Account Groups
> Create Prisma Cloud Roles
> Manage Roles in Prisma Cloud
> Add Administrative Users On Prisma Cloud
> Create and Manage Access Keys
> Manage your Prisma Cloud Profile
> Set up SSO Integration on Prisma Cloud
> Define Prisma Cloud Enterprise Settings

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Administrator Roles

A *user* on Prisma Cloud is someone who has been assigned administrative privileges, and a *role* defines the type of access that the administrator has on the service. When you define a role, you specify the *permission group* and the account groups that the administrator can manage. Prisma Cloud has four types of permission groups built-in for administrators.

- **System Admin**—Full control (read/write permissions) to the service, and they can create, edit, or delete account groups or cloud accounts. Only System administrators have access to all **Settings** on Prisma Cloud and can view audit logs to analyze actions performed by other users who have been assigned administrative privileges.
- **Account Group Admin**—Read/write permissions for the cloud accounts and account groups to which they are granted access.

  An account group administrator can only view resources deployed within the cloud accounts to which they have access. Resources deployed on other cloud accounts that Prisma Cloud monitors are excluded from the search or investigation results.
- **Account Group Read Only**—Read only permissions to view designated sections of Prisma Cloud. This role does not have permissions to modify any settings.
- **Account and Cloud Provisioning Admin**—Combines the permissions for the **Account Group Admin** and the **Cloud Provisioning Admin** to enable an administrator who is responsible for a line of business. With this role, in addition to being able to onboard cloud accounts, the administrator can access the dashboard, manage the security policies, investigate issues, view alerts and compliance details for the designated accounts only.
- **Cloud Provisioning Admin**—Permissions to onboard and manage cloud accounts from Prisma Cloud and the APIs, and the ability to create and manage the account groups. With this role access is limited to **Settings** > **Cloud Accounts** and **Settings** > **Account Groups** on the admin console.

Add Administrative Users On Prisma Cloud. You can **View permissions** associated with each role on **Settings** > **Roles** > **+Add New**

© 2019 Palo Alto Networks, Inc.

Create Account Groups

You can use Account Groups to combine access to multiple cloud accounts with similar or different applications that span multiple divisions or business units, so that you can manage administrative access to these accounts from Prisma Cloud.

When you onboard a cloud account to Prisma Cloud, you can assign the cloud account to one or more account groups, and then assign the account group to Prisma Cloud Administrator Roles. Assigning an account group to an administrative user on Prisma Cloud allows you to restrict access only to the resources and data that pertains to the cloud account(s) within an account group. Alerts on Prisma Cloud are applied at the cloud account group level, which means you can setup separate alert rules and notification flows for different cloud environments.

STEP 1 | Select **Settings** > **Account Groups** and click **+ Add New**.

STEP 2 | Enter a **Name** and **Description** for the Account Group.

STEP 3 | Select the cloud accounts that you want to group together in this account group and click **Save**.

© 2019 Palo Alto Networks, Inc.

Manage Prisma Cloud Account Groups

To view and manage account groups:

STEP 1 | Select **Settings** > **Account Groups**.

STEP 2 | To edit the details of an Account Group, click the record and change any details.

STEP 3 | To clone an Account Group, hover over the account group and click **Clone**.

Cloning an account group is creating a copy of an existing account group. Cloning serves as a quick method of creating a new account group if you choose to change few details of the source account group.

STEP 4 | To delete an Account Group, hover over the account group and click **Delete**.

© 2019 Palo Alto Networks, Inc.

Create Prisma Cloud Roles

Roles on Prisma Cloud enable you to specify what permissions an administrator has, and to which cloud accounts they have read or read-write access.

When you create a cloud account, you can assign one or more cloud account to account group(s) and then attach the account group to the role you create. This flow allows you to ensure the administrator who has the role can access the data related to only the cloud account(s) to which you have authorized access.

STEP 1 | Select **Settings** > **Roles** and click **+ Add New**.

STEP 2 | Enter a name and a description for the role.

STEP 3 | Select a permission group.

- Select **System Admin** to allow full access and control over all sections of Prisma Cloud including overall administration settings and permissions management.
- Select **Account Admin** to allow full access over permissible accounts including a subset of administration settings and permissions management.
- Select **Account ReadOnly** to allow read access to permissible accounts excluding any administration settings and permissions management.
- Select **Cloud Provisioning Admin** to onboard and manage cloud accounts from the admin console and through APIs. They can also create and manage the Account Groups. They do not have access to any other Prisma Cloud features.

STEP 4 | Click **View Permissions** to see the permissions associated with every permission group. The Permission matrix shows what permissions each permission group has within Prisma Cloud.

All Accounts: Has access to all the accounts.

Designated Accounts: Has access to only designated accounts.

No: Has no access to the page.

Owners or users in the same role: Has access to the page.

Yes: Has access to the page.

STEP 5 | (Optional) Restrict the ability dismiss or resolve alerts.

If you would like to ensure that only the System Admin role can manage alerts associated with a policy defined by a system administrator, select **Restrict alert dismissal**. When enabled, an administrator with any other role such as Account Group Admin or Account and Cloud Provisioning Admin roles cannot dismiss or resolve alerts.

STEP 6 | Select Account Groups that you want to associate with this role and click **Save**.

© 2019 Palo Alto Networks, Inc.

Manage Roles in Prisma Cloud

Use roles to define the permissions for a specific account group.

STEP 1 | To view roles, select **Settings** > **Roles**.

STEP 2 | To edit the details of a role, click the record and change any details.

STEP 3 | To clone a role, hover over the role and click **Clone**.

Cloning a role is creating a copy of an existing role. Cloning serves as a quick method of creating a new role if you choose to change few details of the source role.

STEP 4 | To delete a role, hover over the role and click **Delete**.

© 2019 Palo Alto Networks, Inc.

Add Administrative Users On Prisma Cloud

To provide administrative access to Prisma Cloud—admin and API—you must add *users* locally on Prisma Cloud. You can choose whether you want these administrators to use Palo Alto Networks Customer Support Portal (CSP) credentials to log in or SSO using a third-party Identity Service Provider.

If you want to use Palo Alto Networks Customer Support Portal (CSP) credentials, when you add the email address for a user who already has a support account with Palo Alto Networks, they can just log in to Prisma Cloud using the Prisma Cloud URL or from the Prisma Cloud tile on hub.If you Set up SSO Integration on Prisma Cloud with an Identity Service Provider who supports SAML, you can configure Just-in-Time Provisioning (JIT) to create a local account on the fly, instead of creating the account in advance on Prisma Cloud. With JIT, you do not need to manually create a local user account.

The following instructions are for manually adding a local user account on Prisma Cloud.

STEP 1 | Select **Settings** > **Users** and click **+ Add New**.

STEP 2 | Enter **First Name**, **Last Name**, and **Email** of the user.

For a user who has a Palo Alto Networks CSP account, you must enter that the email address that is associated with the CSP account so that they can log in as soon as you save the changes. If the user does not have a CSP account, as soon as you add them here and save your changes, they will receive two emails. One email to activate the CSP account and another email with a link to get started with Prisma Cloud.

STEP 3 | Assign a **Role** to the user.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Administrator Roles can be System Admin, Account Admin, Account Read Only, and Cloud Provisioning Admin.

STEP 4 | Specify a **Time Zone** for the user and click **Save**.

STEP 5 | Decide whether to enable **API Access**.

By default, API access is enabled for the System Admin role only. When you add a new administrator, decide whether or not you want to enable API access for the other roles; the key icon in the API Access column indicates that the administrator has API access, and can create up to two access keys on Prisma Cloud. See Create and Manage Access Keys for more information.

STEP 6 | After you add an administrator, you can edit or delete the user.

- To edit the details of an user, click the record and change any details.
- To disable an user, toggle the **Status** of the user.

- To delete an user, hover over the user and click **Delete**.

© 2019 Palo Alto Networks, Inc.

Create and Manage Access Keys

Access Keys are a secure way to enable programmatic access to the Prisma Cloud API, if you are setting up an external integration or automation. By default, only the System Admin has API access and can enable API access for other administrators.

You can enable API access either when you Add Administrative Users On Prisma Cloud, you can modify the user permissions to enable API access. If you have API access, you can create up to two access keys. Create an access key for a limited time period and regenerate your API keys periodically to minimize exposure and follow security best practices.

On the **Settings** > **Audit Logs**, you can view a record of all access key related activities such as an update to extend its validity, deletion, or a revocation.

STEP 1 | Select **Settings** > **Access Keys** > **+ Add New**

If you do not see the option to add a new key, it means that you do not have the permissions to create access keys.

STEP 2 | Enter a descriptive **Name** for the key.

STEP 3 | Set the **Key Expiry** term.

Select the checkbox and specify a term—date and time for the key validity—that adheres to your corporate compliance standards. If you do not select key expiry, the key is set to never expire; if you select it, but do not specify a date, the key expires in a month. In the event a key is compromised, you can administratively disable (Make Inactive) the key.

STEP 4 | **Create** the key.

Copy or download the Access Key ID and the Secret Key as a CSV file. After you close the window, you cannot view the secret key again, and must delete the existing key and create a new key.

© 2019 Palo Alto Networks, Inc.

STEP 5 | View the details for your keys.

You can verify the expiry date for the key and can update it here, review when it was last used and the status —Active or Expired.

© 2019 Palo Alto Networks, Inc.

Manage your Prisma Cloud Profile

Manage your Prisma Cloud profile.

STEP 1 | To view your profile information, click the icon on the Right hand top corner.

STEP 2 | Edit your **Name**, **Last Name**, or **Time zone** and click **Save**.

© 2019 Palo Alto Networks, Inc.

Set up SSO Integration on Prisma Cloud

On Prisma Cloud, you can enable single sign-on (SSO) using an Identity Provider (IdP) that supports Security Assertion Markup Language (SAML), such as Okta, Azure Active Directory, or PingID. You can configure only one IdP for all the cloud accounts that Prisma Cloud monitors.

To access Prisma Cloud using SSO, every administrative user requires a local account on Prisma Cloud. You can either Add Administrative Users On Prisma Cloud to create the local account in advance of enabling SSO, or use Just-In-Time (JIT) Provisioning on the SSO configuration on Prisma Cloud if you prefer to create the local account automatically. With JIT Provisioning, the first time a user logs in and successfully authenticates with your SSO IdP, the SAML assertions are used to create a local user account on Prisma Cloud.

To enable SSO, you must first complete the setup on the IdP. Then, log in to Prisma Cloud using an account with System Admin privileges to configure SSO and redirect login requests to the IdP's login page, so that your Prisma Cloud administrative users can log in using SSO.

After you enable SSO, you must access Prisma Cloud from the IdP's portal. Prisma Cloud supports IdP initiated SSO, and it's SAML endpoint supports the POST method only.

As a best practice, enable a couple administrative users with both local authentication credentials on Prisma Cloud and SSO access so that they can log in to the admin console and modify the SSO configuration when needed, without risk of account lockout. Also, any administrator who needs to access the Prisma Cloud API cannot use SSO and must authenticate directly to Prisma Cloud using the email address and password registered with Prisma Cloud.

STEP 1 | Decide whether you want to first add Add Administrative Users On Prisma Cloud or you prefer to add users on the fly with JIT Provisioning when you Configure SSO on Prisma Cloud.

If you want to enable JIT provisioning for users, Create Prisma Cloud Roles before you continue to the next step. When you configure SSO on the IdP, you must attach this role to the user's profile so that the user has the appropriate permissions and can monitor the assigned cloud accounts on Prisma Cloud.

STEP 2 | Copy the Audience URI, for Prisma Cloud, which users need to access from the IdP.

1. Log in to Prisma Cloud and select **Settings** > **SSO**.
2. Copy the **Audience URI (SP Entity ID)** value. This is a read-only field in the format: https://app.prismacloud.io?customer=<string> to uniquely identify your instance of Prisma Cloud. You require this value when you configure SAML on your IdP.

STEP 3 | Set up the Identity Provider for SSO.

1. This workflow uses Okta as the IdP. Before you begin to set up Okta configuration, login to your Prisma Cloud instance and copy the Audience URI (SP Entity ID) from Prisma Cloud. See For example: https://app.prismacloud.io/settings/sso.
2. Login to Okta as an Administrator and click **Admin**.

© 2019 Palo Alto Networks, Inc.

3. Click **Add Applications**.

4. Search for **Prisma Cloud** and **Add**.

5. On **Create a New Application Integration**, select **Web** for **Platform** and **SAML 2.0** for **Sign on method**.

© 2019 Palo Alto Networks, Inc.

6. Click **Create**.
7. On **General Settings**, use these values and click **Next**.

   App Name - Prisma Cloud SSO app

   App Logo - Use the Prisma Cloud logo

   App Visibility - Do not check these options

8. To **Configure SAML**, specify the **Sign On URL**.

   The format for Sign On URL uses the URL for Prisma Cloud, but you must replace app with api and add saml at the end. For example, if you access Prisma Cloud at https://app2.prismacloud.io,

© 2019 Palo Alto Networks, Inc.

your Sign On URL should be **`https://api2.prismacloud.io/saml`** and if it is https://app.eu.prismacloud.io, it should be **`https://api.eu.prismacloud.io/saml`**.

9. For **Audience URI** - Use the value displayed on Prisma Cloud **Settings** > **SSO** that you copied in the first step.

10. Select **Name ID format** as **EmailAddress** and **Application username** as **Email**.

11. For **Advanced Section**, select **Response** as **Unsigned**, **Assertion Signature** as **Signed**, **Assertion Encryption** as **UnEncrypted**.

© 2019 Palo Alto Networks, Inc.

12. Assign users who can use the Prisma Cloud SSO app to log in to Prisma Cloud.

13. (Required only for JIT provisioning of a local user account automatically on Prisma Cloud) Specify the attributes to send with the SAML assertion.

    For more details, see Set up Just-in-Time Provisioning on Okta.

14. (Required only for JIT provisioning of a local user account automatically on Prisma Cloud) Assign the role you created on Prisma Cloud to the user profile.

    You have now successfully created an application for the SAML integration. This application will have the details of the **IdP URL** and **Certificate** which you'll need to add on Prisma Cloud to complete the SSO integration.

STEP 4 | Configure SSO on Prisma Cloud.

1. Log in to Prisma Cloud and select **Settings** > **SSO**.
2. **Enable SSO**.
3. Enter the value for your **Identity Provider Issuer**.

© 2019 Palo Alto Networks, Inc.

This is the URL of a trusted provider such as Google, Salesforce, Okta, or Ping who act as your IdP in the authentication flow. On Okta, for example, you can find the Identity Provider issuer URL at **Applications** > **Sign On** > **View Setup Instructions**.

In the setup instructions, you have Identity Provider Issuer and Prisma Cloud Access SAML URL.

4. Enter the **Identity Provider Logout URL** to which a user is redirected to, when Prisma Cloud times out or when the user logs out.
5. Enter your IdP **Certificate** in the standard X.509 format.

   You must copy and paste this from your IdP.

© 2019 Palo Alto Networks, Inc.

6. Enter the **Prisma Cloud Access SAML URL** configured in your IdP settings.

   For example, on Okta this is the Identity Provider Single Sign-On URL. When you click this URL, after authentication with your IdP, you are redirected to Prisma Cloud. This link along with the Relay State Parameter is used for all the redirection links embedded in notifications like email, slack, SQS, and compliance reports.
7. **Relay State Param name** is SAML specific Relay State parameter name. If you provide this parameter along with Prisma Cloud Access SAML URL, all notification links in Splunk, Slack, SQS, email, and reports can link directly to the Prisma Cloud application. The relay state parameter or value is specific to your Identity Provider. For example, this value is **`RelayState`** for Okta.

   When using RelayState functionality, make sure your Prisma Cloud Access SAML URL corresponds to Identity Provider Single Sign-On URL ending in '/sso/saml'.
8. (Optional) Clear the **Enforce DNS Resolution for Prisma Cloud Access SAML URL**.

   By default, Prisma Cloud performs a DNS look up to resolve the Prisma Cloud SAML Access URL you entered earlier. If your IdP is on your internal network, and you do not need to perform a DNS look up, you can clear this option to bypass the DNS lookup.
9. (Optional) Enable Just-in-Time Provisioning for SSO users.

   Enable JIT Provisioning, if you want to create a local account for users who are authenticated by the IdP.
10. Provide the user attributes in the SAML assertion or claim that Prisma Cloud can use to create the local user account.

    You must provide the email, role, first name, and last name for each user. Timezone is optional.

© 2019 Palo Alto Networks, Inc.

The role that you specify for the user's profile on the IdP must match what you created on Prisma Cloud in Step 1.

11. Select **Allow select users to authenticate directly with Prisma Cloud** to configure some users to access Prisma Cloud directly using their email address and password registered with Prisma Cloud, in addition to logging in via the SSO provider.

    When you enable SSO, make sure to select a few users who can also access Prisma Cloud directly using the email and password that is registered locally on Prisma Cloud to ensure that you are not locked out of the console in the event you have misconfigured SSO and need to modify the IdP settings. For accessing data through APIs, you need to authenticate directly to Prisma Cloud.
12. Select the **Users** who can access Prisma Cloud either using local authentication credentials on Prisma Cloud or using SSO.

    The whitelisted users can log in using SSO and also using a local account username and password that you have created on Prisma Cloud.

13. **Save** your changes.
14. Verify access using SSO.

    Administrative users for whom you have enabled SSO, must access Prisma Cloud from the Identity Provider's portal. For example, if you have integrated Prisma Cloud with Okta, administrative users must login to Okta and then click on the Prisma Cloud app icon to be logged in to Prisma Cloud.
15. Using **View last SSO login failures**, you can see details of last five login issues or errors for SSO authentication for any users.

© 2019 Palo Alto Networks, Inc.

If the user is logged in already using a username/password and then logs in using SSO, the authentication token in the browser's local storage is replaced with the latest token.

Set up Just-in-Time Provisioning on Okta

To successfully set up local administrators on the fly with Just-in-Time (JIT) provisioning, you need to configure the Prisma Cloud app for Okta to provide the SAML claims or assertions that enable Prisma Cloud to add the authenticated SSO user on Prisma Cloud. Then to ensure that the SSO user has the correct access privileges on Prisma Cloud, you need to assign a Prisma Cloud role to the user; if this role is not a default role on Prisma Cloud, you must define the role before you assign the role to the user on Okta.

STEP 1 | Create the Prisma Cloud App for Okta.

STEP 2 | For JIT, create a custom attribute on the Prisma Cloud Okta app.

1. Go to **Directory** > **Profile Editor** > **App**.
2. Find the Prisma Cloud app and select **Profile**, and **Add Attribute**.

© 2019 Palo Alto Networks, Inc.

Enter a display name, a variable name, and an attribute length that is long enough to accommodate the role names on Prisma Cloud.

STEP 3 | Configure the **Attribute Statements** on the Prisma Cloud Okta app.

Specify the user attributes in the SAML assertion or claim that Prisma Cloud can use to create the local user account.

1. Select **Applications** > **Applications**
2. Select the Prisma Cloud app, **General** and edit the **SAML Settings** to add the attribute statements.

   You must provide the email, role, first name, and last name for each user. Timezone is optional.

STEP 4 | Assign the Prisma Cloud role for each SSO user.

Each SSO user who is granted access to Prisma Cloud, must have a Prisma Cloud role assigned. This role determines the permissions and account groups that the user has on Prisma Cloud.

1. Select **Applications** > **Applications**
2. Select the Prisma Cloud app and Assignments.

   For existing users, click the pencil icon to add the Prisma Cloud Role you want to give this user. For example, System Admin.

   For new users, select **Assign** > **Assign to People**, click **Assign** for the user you want to give access to Prisma Cloud and define the Prisma Cloud Role you want to give this user.

STEP 5 | Continue with 4.

© 2019 Palo Alto Networks, Inc.

View Audit Logs

As part of compliance requirement for organizations, companies need to demonstrate they are pro-actively tracking security issues and taking steps to remediate issues as they occur. Prisma Cloud Audit Logs section enables companies to prepare for such audits and demonstrates compliance. The Audit logs section lists out the actions performed by the users in the system.

STEP 1 | Select a **Time Range** to view the activity details by users in the system.

STEP 2 | Select the columns in the table and **Download** all administrator activity.

The user activity details are in a CSV format.

© 2019 Palo Alto Networks, Inc.

Define Prisma Cloud Enterprise Settings

Set the enterprise level settings to build standard training models for Unusual User Activity (UEBA), alert disposition, browser, and user attribution for alerts.

Training Model Threshold - To set an ideal behavior based intensity, so that any activity is analyzed against this baseline. Set the intensity to **High** to analyze 300 events over 90 days and define a standard baseline. Set the intensity to **Medium** to analyze 100 events over 30 days and define a standard baseline. Set the intensity to **Low** to analyze 25 events over seven days to define a standard baseline.

For production environments, set the Training Model Threshold to High so that you give the system more time and data to analyze the behavior.

Alert Disposition - You can profile every activity by location or user activity. The activity-based anomalies identify any activities which have not been consistently performed in the past. The location based anomalies identify locations from which activities have not been performed in the past. Set the disposition to **Conservative** to profile both location and activity to classify an anomaly. Set the disposition to **Moderate** to profile only location to classify an anomaly. Set the disposition to **Aggressive** to profile only activity to classify an anomaly.

Set the Alert Disposition to Conservative to reduce false positives.

When you change **Training Model Threshold** or **Alert Disposition** the existing alerts are resolved and new ones are regenerated based on the new setting. It might take a while for the new anomaly alerts to show on the Alerts page.

Browser Session Timeout—Specify a timeout period after which an inactive user will be logged out of Prisma Cloud.

Auto enable new default policies of the type - Use this option to automatically granularly enable new **Default** policies of severity **High**, **Medium** or **Low**. By default, Default policies are in a disabled state if your Prisma Cloud instance was provisioned before March 2019 and automatically enabled for instances provisioned after that date.

Make Alert Dismissal Note Mandatory - Select this option to mandate the users to dismiss alerts only after specifying a reason.

Populate User Attribution in Alerts Notifications - Select this option to make sure that the alerts generated have user attribution data in the Alert Payload. This is applicable for alerts which have user attribution data identified for certain resources. This might result in a delay in the generation of Alerts.

Manage Prisma Cloud Alerts

> Prisma Cloud Alerts and Notifications
> Whitelist IP Addresses on Prisma Cloud
> Enable Prisma Cloud Alerts
> Create an Alert Rule
> Configure Prisma Cloud to Automatically Remediate Alerts
> Send Prisma Cloud Alert Notifications to Third-Party Tools
> View and Respond to Prisma Cloud Alerts
> Alert Payload
> Prisma Cloud Risk Ratings

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Alerts and Notifications

Prisma Cloud continually monitors all of your cloud environments to detect misconfigurations (such as an exposed cloud storage instance), advanced network threats (for example, cryptojacking or data exfiltration), stolen access keys or account compromise, and vulnerable hosts. Prisma Cloud then correlates configuration data with user behavior and network traffic to provide context around misconfigurations and threats, in the form of actionable alerts.

Although Prisma Cloud begins monitoring and correlating data as soon as you onboard the cloud account, there are a couple of steps you need to take before you can start seeing alerts generated by policy violations in your cloud environments. The first thing you need to do to Enable Prisma Cloud Alerts is to add the cloud account to an *account group* during onboarding. Next, you must create an *alert rule* that associates all of the cloud accounts in an account group with the set of policies for which you want Prisma Cloud to generate alerts. You can view the alerts for all of your cloud environments directly from Prisma Cloud, and drill down to get a view into specific policy violation. If you have internal networks that you would like to exclude from being flagged in an alert, you can Whitelist IP Addresses on Prisma Cloud.

In addition, Prisma Cloud provides out-of-the box Configure External Integrations on Prisma Cloud with third-party technologies—for example, SIEM platforms, ticketing systems, messaging systems, and automation frameworks—so that you can continue to use your existing operational, escalation, and notification tools. This allows you to monitor your cloud infrastructures more efficiently and enables visibility into actionable events across all of your cloud workloads. When you create an alert rule, you can optionally enable all alerts generated by the alert rule to send the Alert Payloadto the selected third-party tool.

© 2019 Palo Alto Networks, Inc.

Whitelist IP Addresses on Prisma Cloud

If you have internal networks that connect to your public cloud infrastructure, you can whitelist these IP ranges (or CIDR blocks) on Prisma Cloud. IP whitelisting is a way to create a label to your identify internal networks, which are not in the private IP address space, and make alert analysis easier. With whitelisting, when you visualize network traffic on the Prisma Cloud **Investigate** tab, instead of flagging your internal IP addresses as internet or external IP addresses, the service can identify these networks with the labels you provide.

Prisma Cloud default network policies that look for internet exposed instances do not generate alerts when the source IP address is included in the whitelist, and the account hijacking anomaly policy filters out activities from known IP addresses. Also, when you use RQL to query network traffic, you can filter out traffic from known networks that are included in the IP whitelist.

To add a network to the IP whitelist:

STEP 1 | Select **Settings** > **IP Whitelisting** > **+ Add New**.

STEP 2 | Enter name or label for the network.

STEP 3 | Enter the **CIDR** and a **Description** and **Save**.

Enter the CIDR block for IP addresses that are routable through the public internet. You cannot whitelist private CIDR blocks.

STEP 4 | Select **Done**.

The whitelisted IP addresses in the network graph are appropriately classified when you run a Network Query.

© 2019 Palo Alto Networks, Inc.

Enable Prisma Cloud Alerts

Although Prisma Cloud begins monitoring your cloud environments as soon as you onboard a cloud account, in order to receive alerts you must first enable alerting for each cloud account you onboard. Prisma Cloud gives you the flexibility to group your cloud accounts into account groups so that you restrict access to information about specific cloud accounts to only those administrators who need it. Then, you must assign each account group to an alert rule that allows you to select a group of policies and designate where you want the Prisma Cloud Alerts and Notifications associated with those policies to display. This allows you to define different alert rules and notification flows for different cloud environments, such as a Production and a Dev cloud environment. In addition, you can set up different alert rules for sending specific alerts to your existing SOC visibility tools. For example, you could send one set of alerts to your SIEM and another set to Jira for automated ticketing.

STEP 1 | Make sure you have associated all onboarded cloud accounts to an account group.

If you did not associate a cloud account with an account group during the onboarding process, do it now so that you can see alerts associated with the account.

1. Click Settings and then select **Cloud Accounts**.
2. For each cloud account, verify that there is a value in the Account Groups column.

3. For any cloud account that isn't yet assigned to an account group, select the cloud account to edit it and select an Account Group to add it to.

STEP 2 | Create an Alert Rule.

Alert rules define what policy violations trigger alerts for cloud accounts within the selected account group and where to send the alert notifications.

STEP 3 | Verify that the alert rule you just created is triggering alert notifications.

As soon as you save your alert rule, any violation of a policy you selected to alert on results in an alert notification on the **Alerts** page, as well as in any third-party integrations you designated in the alert rule. Make sure you see the alerts you are expecting on the **Alerts** page as well as in your third-party tools.

© 2019 Palo Alto Networks, Inc.

Create an Alert Rule

Alert rules allow you to define what policy violations in a selected set of cloud accounts you want to trigger alerts. When you create an alert rule, you select the account groups to which the rule applies and the corresponding set of policies you want to trigger alerts. You can add more granularity to the rule by excluding some cloud accounts from the selected account group(s), specifying specific region(s) for which to send alerts, and even narrowing the rule down to the specific cloud resources identified by resource tags. This gives you a lot of flexibility in how you manage alerts and ensures that you can adhere to the administrative boundaries you have defined. You can create a single alert rule that alerts on all policy rules, or you can define granular alert rules that send very specific sets of alerts for specific cloud accounts, regions, and even resources to specific destinations.

When you create an alert rule you can Configure Prisma Cloud to Automatically Remediate Alerts, which enables Prisma Cloud to automatically run the CLI command required to remediate the policy violation directly in your cloud environments. Automated remediation is only available for Default policies (Config policies only) that are designated as Remediable on the **Policies** page.

In addition, if you have Configure External Integrations on Prisma Cloud with third-party tools, defining granular alert rules allows you to send exactly the alerts you need to enhance your existing operational, ticketing, notification, and escalation workflows with the addition of Prisma Cloud alerts on policy violations in all of your cloud environments. To see any existing integrations, click Settings and then select **Integrations**.

STEP 1 | Select **Alerts** > **Alert Rules** and click **+Add New**.

STEP 2 | Enter an **Alert Rule Name** and optionally a **Description** to communicate the purpose of the rule and then click **Next**.

STEP 3 | Select the **Account Groups** that you want this alert rule to apply to and then click **Next**.

1. Toggle **View Advanced Settings** to see advanced settings for setting a target.
2. Exclude any cloud accounts from your selected Account Group in **Exclude Cloud Accounts**.
3. Choose your region from **Region**.
4. Add any tags in **Tags** to easily manage or identify type of your resources.

   Tags apply only to Config and Network policies.
5. Click **Next**.

STEP 4 | (Optional) If you want to add more granularity to what cloud resources trigger alerts for this alert rule, **View Advanced Settings** and then provide more criteria in any of the following fields:

- **Exclude Cloud Accounts**—If there are some cloud accounts in the selected account groups that you do not want to trigger alerts for, select the account(s) from the list.
- **Regions**—To trigger alerts only for specific regions for the cloud accounts in the selected account group, select one or more regions from the list.
- **Resource Tags**—To trigger alerts only for specific resources in the selected cloud accounts, enter the **Key** and **Value** of the resource tag you created for the resource in your cloud environment.

© 2019 Palo Alto Networks, Inc.

Tags apply only to Config and Network policies.

When you finish defining the target cloud resources, click **Next**.

STEP 5 | Select the policies that you want this alert rule to trigger alerts for and, optionally, Configure Prisma Cloud to Automatically Remediate Alerts.

© 2019 Palo Alto Networks, Inc.

1. Either **Select All Policies** or select the specific policies that you want to trigger alerts for this alert rule.

   If you enable Automated Remediation, the list of policies only shows Remediable policies

   .

   To help you find the specific group of policies you want to this rule to alert on, use one of the following tools:

   - Filter Results—Enter a search term to filter the list of policies to those with specific keywords.
   - Column Picker—Click to modify what columns display.
   - Sort—To sort on a specific column, click the corresponding icon.
   - Column Filter—To filter on a specific values in a column, click the corresponding column filter icon and then select values from the filter menu. For example, to filter on compliance standards related to NIST, click the filter for the Compliance Standard column, select the NIST standards and then click **Set**.

© 2019 Palo Alto Networks, Inc.

2. Click **Next**.

STEP 6 | (Optional) Send Prisma Cloud Alert Notifications to Third-Party Tools.

By default, all alerts triggered by the alert rule display on the **Alerts** page. You can also send Prisma Cloud alerts triggered by this alert rule to third-party tools that you have Configure External Integrations on Prisma Cloud, such as Send Alert Notifications to Amazon SQS or Send Alert Notifications to Jira

In addition, you can configure the alert rule to Send Alert Notifications via Email.

STEP 7 | (Optional) If you want to delay the alert notifications for Config alerts, enter the number of minutes in**Trigger notification for Config Alert only after the Alert is Open for** to specify how long you want Prisma Cloud to wait after an alert is generated.

STEP 8 | **Save** the alert rule.

STEP 9 | To verify that the alert rule is triggering the expected alerts, select **Alerts** > **Overview** and make sure you see the alerts you expect to see.

If you configured the rule to Send Prisma Cloud Alert Notifications to Third-Party Tools make sure you also see the alert notifications in those tools.

© 2019 Palo Alto Networks, Inc.

Configure Prisma Cloud to Automatically Remediate Alerts

If you want Prisma Cloud to automatically resolve policy violations, such as misconfigured security groups, you can configure Prisma Cloud for automated remediation. In order to automatically resolve a policy violation, Prisma Cloud runs the CLI command associated with the policy in the cloud environments where it discovered the violation. On Prisma Cloud, you can enable auto-remediation for Default policies (Config only) that are designated as remediable (as indicated by the in the Remediable column), and for any cloned or custom policies that you add.

To enable this option, you must identify the set of policies that you want to automatically remediate and verify that Prisma Cloud has the required permissions in the associated cloud environments. You must then Create an Alert Rule that enables automated remediation for the set of policies you have identified.

Use caution when enabling automated remediation because it requires Prisma Cloud to make changes in your cloud environments, which could have an adverse affect on your applications.

STEP 1 | Verify that Prisma Cloud has the required privileges to remediate the policies you plan to configure for automated remediation.

1. To view remediable policies, select **Policies**and set the filter to **Remediable** > **True**.

   If the Remediable column is not showing on the Policies page, use the Column Picker to display it.

© 2019 Palo Alto Networks, Inc.

2. Select a policy that you want to enable for auto remediation and go to the Remediation page.

   Review the required privileges in the CLI Command Description to identify what permissions Prisma Cloud requires in the associated cloud environments to be able to remediate violations of the policy.

© 2019 Palo Alto Networks, Inc.

STEP 2 | Create an Alert Rule or modify an existing alert rule.

STEP 3 | On the Select Policies page, enable **Automated Remediation** and click **Continue** to acknowledge the impact of automated remediation on your application.

The list of available policies updates to show only those policies that are remediable (as indicated by the ✓ in the Remediable column).

If you are modifying an existing alert rule that includes non-remediable policies, those policies will no longer be included in the rule. When you modify the rule, Prisma Cloud notifies all account administrators who have access to the rule.

STEP 4 | Finish configuring and **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

© 2019 Palo Alto Networks, Inc.

Send Prisma Cloud Alert Notifications to Third-Party Tools

Alert rules define what policy violations trigger an alert in a selected set of cloud accounts. When you Create an Alert Rule, you can also configure the rule to send the Alert Payload that the rule triggers to one or more third-party tools. For all channels except email, to enable notification of policy violations in your cloud environments into your existing operational workflows you must Configure External Integrations on Prisma Cloud. You can either set up the integration before you create the alert rule or use the inline link in the alert rule creation process to set up the integration just when you need it.

On some integrations such as Google CSCC, AWS Security Hub, PagerDuty and ServiceNow, Prisma Cloud can send a state change notification to resolve an incident when the issue that generated the alert is resolved manually or if the resource was updated in the cloud environment and the service learns that the violation was fixed.

Refer to the following topics to enable an alert notification channel with third-party tools:

- Amazon SQS
- Email
- Slack
- Splunk
- Jira
- Google CSCC
- ServiceNow
- Webhooks
- PagerDuty
- AWS SecurityHub
- Microsoft Teams

Send Alert Notifications to Amazon SQS

To send Prisma Cloud alert notifications to Amazon Simple Queue Service (SQS):

STEP 1 | Integrate Prisma Cloud with Amazon SQS.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **SQS**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Select the SQS **Queues** to which you want to send alerts triggered by this alert rule.

STEP 5 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications via Email

You can send notification of alerts triggered by an alert rule by email.

© 2019 Palo Alto Networks, Inc.

STEP 1 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 2 | On the Set Alert Notification page of the alert rule, select **Email**.

STEP 3 | Enter or select the **Emails** to which to send the alert notifications.

You can only send email notifications to email addresses in your domain. You can specify multiple email addresses.

STEP 4 | Set the **Frequency** at which to send email notifications.

- **As it Happens**—Sends an email to the recipient list each time the alert rule triggers an alert.
- **Daily**—Sends a single email to the recipient list once a day with all alerts triggered by the alert rule that day.
- **Weekly**—Sends a single email to the recipient list once a week with all alerts triggered by the alert rule that week.
- **Monthly**—Sends a single email to the recipient list once a month with all alerts triggered by the alert rule that over the month.

STEP 5 | Click into the **Emails** field and then enter or select the email addresses to which you want to send email notification of alerts triggered by this alert rule.

© 2019 Palo Alto Networks, Inc.

STEP 6 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

STEP 7 | Verify the alert notification emails.

The email alert notification specifies the alert rule, account name, cloud type, policies that were violated, the number of alerts each policy violated, and the affected resources. Clicking the number of alerts takes you to the Prisma Cloud **Alerts** > **Overview** page.

Send Alert Notifications to a Slack Channel

To send alert notifications associated with an alert rule to a Slack channel:

STEP 1 | Integrate Prisma Cloud with Slack.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **Slack**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Select the Slack **Channels** to which you want to send alerts triggered by this alert rule.

STEP 5 | Set the **Frequency** at which to send email notifications.

- **As it Happens**—Sends a notification to the selected slack channels each time the alert rule triggers an alert.
- **Daily**—Sends a single notification to the selected Slack channels once a day with all alerts triggered by the alert rule that day.
- **Weekly**—Sends a single notification to the selected Slack channels once a week with all alerts triggered by the alert rule that week.
- **Monthly**—Sends a single notification to the selected Slack channels once a month with all alerts triggered by the alert rule that over the month.

© 2019 Palo Alto Networks, Inc.

STEP 6 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to Splunk

To send alert notifications associated with an alert rule to a Splunk event collector:

STEP 1 | Integrate Prisma Cloud with Splunk.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **Splunk**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Select the Splunk **Event Collectors** to which you want to send alerts triggered by this alert rule.

STEP 5 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to Jira

To configure alert notifications triggered by an alert rule to create Jira tickets:

STEP 1 | Integrate Prisma Cloud with Jira.

© 2019 Palo Alto Networks, Inc.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **Jira**.

STEP 4 | Select the Jira **Templates** to use to create tickets using the alert payload data for alerts triggered by this alert rule.

STEP 5 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

© 2019 Palo Alto Networks, Inc.

Send Alert Notifications to Google CSCC

To send alert notifications to Google Cloud Security Command Center (CSCC):

STEP 1 | Integrate Prisma Cloud with Google Cloud Security Command Center.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **CSCC**.

STEP 4 | Select the **Google CSCC Integrations** to use to send notifications of alerts triggered by this alert rule.

© 2019 Palo Alto Networks, Inc.

STEP 5 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to ServiceNow

To send alert notifications to ServiceNow.

STEP 1 | #unique_81.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **now**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Select the ServiceNow **Templates** to use to send notifications of alerts triggered by this alert rule.

STEP 5 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to Webhooks

To send alert notifications to Webhooks.

STEP 1 | Integrate Prisma Cloud with Webhooks.

© 2019 Palo Alto Networks, Inc.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **webhooks**.

STEP 4 | Select the Webhook **Channels** to use to send notifications of alerts triggered by this alert rule.

STEP 5 | Set the **Frequency** at which to send POST notifications.

- **As it Happens**—Sends a notification to the selected Webhook channels each time the alert rule triggers an alert.
- **Daily**—Sends a single notification to the selected Webhook channels once a day with all alerts triggered by the alert rule that day.
- **Weekly**—Sends a single notification to the selected Webhook channels once a week with all alerts triggered by the alert rule that week.
- **Monthly**—Sends a single notification to the selected Webhook channels once a month with all alerts triggered by the alert rule that over the month.

© 2019 Palo Alto Networks, Inc.

STEP 6 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to PagerDuty

To send alert notifications to PagerDuty.

STEP 1 | Integrate Prisma Cloud with PagerDuty.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **pagerduty**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Select the **Integration Key**.

STEP 5 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to AWS SecurityHub

To send alert notifications to AWS SecurityHub.

STEP 1 | Integrate Prisma Cloud with AWS Security Hub.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | Select your AWS account from **AWS Security Hub**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

Send Alert Notifications to Microsoft Teams

To send alert notifications to Microsoft Teams.

STEP 1 | Integrate Prisma Cloud with Microsoft Teams.

STEP 2 | Select **Alerts** > **Alert Rules** and either select an existing rule to edit or Create an Alert Rule.

STEP 3 | On the Set Alert Notification page of the alert rule, select **Microsoft Teams**.

© 2019 Palo Alto Networks, Inc.

STEP 4 | Select the **Teams** channel(s) to send notifications for alerts triggered by this alert rule.

STEP 5 | Set the **Frequency** at which to send POST notifications.

- **As it Happens**—Sends a notification to the selected channels each time the alert rule triggers an alert.
- **Daily**—Sends a single notification to the selected channels once a day with all alerts triggered by the alert rule that day.
- **Weekly**—Sends a single notification to the selected channels once a week with all alerts triggered by the alert rule that week.
- **Monthly**—Sends a single notification to the selected channels once a month with all alerts triggered by the alert rule that over the month.

STEP 6 | **Save** the new alert rule or **Confirm** your changes to an existing alert rule.

When a policy rule is violated, a message card displays on the Microsoft teams conversation. The message card is formatted with a red (high), yellow (medium) or gray (low) line to indicate the severity of the alert. For example, the following screenshot is a daily notification summary.

© 2019 Palo Alto Networks, Inc.

© 2019 Palo Alto Networks, Inc.

View and Respond to Prisma Cloud Alerts

As soon as you Enable Prisma Cloud Alerts, Prisma Cloud generates an alert when it detects a violation in a policy that is included in an active alert rule. To secure your cloud environments, you must monitor alerts, either from Prisma Cloud or using a third-party tool to which you are Send Prisma Cloud Alert Notifications to Third-Party Tools and ensure that the policy violations in your cloud environments are resolved. The status of an alert can be one the following:

- **Open**—Prisma Cloud identified a policy violation that triggered the alert and the violation has not yet been resolved.
- **Resolved**—Alerts automatically transition to the Resolved state when the issue that caused the policy violation is resolved. An alert could also change to the Resolved state due to a change in the policy or alert rule that triggered the alert. Note that a resolved alert can also transition back to the open state if the issue resurfaces or there is a policy or alert rule change that causes the alert to trigger again.
- **Snoozed**—A Prisma Cloud administrator temporarily dismissed an alert for a specified time period. When the timer expires, the alert is automatically in an open or resolved state depending on whether or not the issue is fixed.
- **Dismissed**—A Prisma Cloud administrator manually dismissed the alert, although the underlying issue may not have been resolved. You can manually reopen a dismissed alert, if you need.

If you manually dismiss an alert for a Network policy rule violation, Prisma Cloud automatically reopens the alert when it detects the same violation again.

- **View alerts from within Prisma Cloud, select Alerts.**

  All alerts you have permission to see based on your role are displayed. You can sort and filter the alerts as follows:

  - To modify what columns display, click and add or remove columns.
  - To sort on a specific column, click the corresponding icon.
  - To filter on specific alert criteria, click to show the filter pane and add and remove filters. You can also clear filters or save a filter for future use.
  - To modify what filters are available or to perform a keyword search, click and then either enter search term to **Filter Results**, or add additional filters. You can filter on: Account Group, Alert ID, Alert Rule Name, Alert Status, Cloud Account, Cloud Region, Cloud Service, Cloud Type, Compliance Requirement, Compliance Section, Compliance Standard, Policy Label, Policy Name, Remediable, Resource ID, Resource Name, Resource Type, and Risk Grade.

© 2019 Palo Alto Networks, Inc.

- To download the filtered list of alert details to a CSV file, click the Download icon.

- **Resolve alerts.**

  Prisma Cloud generates an alert any time it finds a policy violation in one or more of your cloud environments that is associated with an alert rule. You can monitor alerts in the cloud accounts you are responsible for to see what security risks you have and to ensure that any critical issues get resolved, either through an Send Prisma Cloud Alert Notifications to Third-Party Tools, through Configure Prisma Cloud to Automatically Remediate Alerts, or by manually resolving the issue. By reviewing the alerts you can also decide whether you need to make a change in a policy or alert rule. Depending on the policy type that triggered the alert, you can go directly from the alert to the cloud resource with the violation, or even resolve an issue from the Prisma Cloud **Alerts** page:

  1. Filter the alerts to show only **Open** alerts that are **Remediable**.

  2. Select the policy for which you want to resolve alerts.

     Review the recommendations for resolving the policy violation. You can also click the policy name to go directly to the policy.
  3. Select the individual alerts you want Prisma Cloud to resolve and click **Resolve**.

© 2019 Palo Alto Networks, Inc.

- Pivot from an alert into the cloud resource that triggered the alert to manually resolve the issue.

  Prisma Cloud allows you to pivot directly from an alert and view the violating cloud resource so that you can resolve the issue.

  1. Filter the alert list to show alerts with Alert Status **Open** and select the Policy Type, for example **Network** or **Config**.
  2. Select the policy for which you want to resolve alerts.

     Review the recommendations for resolving the policy violation.
  3. Click the icon to pivot to the cloud resource containing the violation you want to resolve and follow the recommended steps.

     When you click the resource icon, Prisma Cloud redirects the request to the cloud platform. To view the resource details in the cloud platform, you must be logged in to Prisma Cloud with the same account as the resource you are investigating.

© 2019 Palo Alto Networks, Inc.

© 2019 Palo Alto Networks, Inc.

Alert Payload

A Prisma Cloud alert payload is a JSON data object that contains detailed information about an alert such as the cloud account, resource, compliance standard, and policy.

Alert Payload Field	Description
Account ID	The ID of the cloud account where the violation that triggered the alert occurred.
Account Name	Name of the cloud account where Prisma Cloud detected the policy violation.
Alert ID	Identification number of the alert.
Alert Rule Name	Name of the alert rule that triggered this alert.
Callback URL	The URL for the alert in Prisma Cloud.
Cloud Type	Type of cloud account: AWS, Azure, or GCP.
Policy Description	Description of the policy as shown within Prisma Cloud.
Policy ID	Universally unique identification number of the policy.
Policy Labels	Labels associated with the policy.
Policy Name	Name of the policy.

© 2019 Palo Alto Networks, Inc.

Alert Payload Field	Description
Policy Recommendation	Remediation recommendations for this policy.
Saved Search UUID	Universally unique identification number of the saved search.
Remediation CLI	The CLI commands that you can use to resolve the policy violation.
Compliance Standard name	Name of the compliance standard.
Compliance Standard description	Description of the compliance standard.
Requirement ID	Identification number of the requirement in the compliance standard.
Requirement Name	Name of the requirement in the compliance standard.
Section ID	Identification number of the section in the compliance standard
Section Description	Description of the section in the compliance standard
Compliance ID	ID number of the compliance standard.
System Default	Indicates if the compliance standard is Prisma Cloud System Default.
Custom assigned	Indicates if this compliance standard is assigned to a policy.
Resource Cloud Service	Cloud service provider of the resource that triggered the alert.
Resource Data	The JSON data of the resource.
Resource ID	ID of the resource that triggered the alert.
Resource Name	Name of the resource that triggered the alert.
Resource Region	Name of the cloud region the resource belongs to.
Resource Region ID	ID of the region the cloud resource belongs to.
Resource Type	Type of resource that triggered the alert, for example EC2 instance or S3 bucket.
Risk Rating	Risk score defined for the resource: A, B, C, or F.
Severity	Severity of the alert: High, Medium, or Low.

© 2019 Palo Alto Networks, Inc.

Alert Payload Field	Description
User Attribution data	Data about the user who created or modified the resource the caused the alert. *In order for alert notifications to include user attribution data, you must enable Populate User Attribution In Alerts Notifications (Settings > Enterprise Settings). Including user attribution data may delay alert notification because the information may not be available from the cloud provider when Prisma Cloud is ready to generate an alert.*

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Risk Ratings

A Prisma Cloud risk rating is a letter grade from A through F that indicates the severity of the alerts that are associated with a resource. The rating is the collective score of all the policy violations for a resource. Each policy is assigned a severity rating of Low, Medium, High, and when a resource violates the policy, the corresponding alert accrues the score that matches the severity rating on the policy.

The classification is as follows:

- **N/A** - No risk score is associated with the resource. A resource may not have a risk score either because you have not applied policies to scan the resource or because the policies that the resource is being scanned against do not apply to the resource.
- **A** - No Alerts
- **B** - 1 low Alert or more.
- **C** - 2 medium alerts or more
- **F** - Multiple alerts, need to assess.

You must review resources that are rated **F** right away as these resources are violating policies with high severity. Because the rating is a cumulative score, a **F** grade may include violations of medium and low severity policies also.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Dashboards

The interactive Asset Inventory and SecOps dashboards give you visibility into the health and security posture of your cloud infrastructure. The dashboards provide a summarized and graphical view of all your Prisma Cloud cloud accounts and resources, and you can use the predefined or custom time range to view current trends or historical data.

> Prisma Cloud Asset Inventory
> SecOps Dashboard
> Export Data and Customize the SecOps Dashboard

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Asset Inventory

The Asset Inventory dashboard provides up-to-date information of all cloud resources or *assets* that you are monitoring and securing using Prisma Cloud. From the dashboard you gain operational insight over all our cloud IT infrastructure, including assets and services such as Compute Engine instances, Virtual machines, Cloud Storage buckets, Accounts, Subnets, Gateways, and Load Balancers.

Assets are displayed by default for all account groups, which the service monitors, for the last seven day time range. The interactive dashboard provides filters to change the scope of data displayed, so that you can analyze information you want to view in greater detail. You can group the results by account name, cloud region, or service name and then drill down to view granular information on the resource types within your cloud accounts. All global resources for each cloud are grouped under AWS Global, Azure Global, and GCP Global.

At a glance the Asset Inventory dashboard includes

- **Resources** - Shows current active total number of resources. Click the link for resources and you will be redirected to the Investigate page which will show the config RQL query associated with these resources.
- **Pass** - Displays the resources without any open alerts. Click the link for the passed resources and you will be redirected to the Investigate page which will show the config RQL query associated with these resources.
- **Fail** - Displays the total number of resources that have generated at least one open alert. Click the link for the failed resources and you will be redirected to the alerts page which will show the alerts associated with these resources.
- **Trend Line** - The trend line on the dashboard helps you to monitor the overall health of cloud infrastructure in your organization. When there are more resources that are passing policy, audit checks, and not generating alerts because of mis-configurations, or risks arising from violation of security best practices the passed resources trend line is in green and pointing upwards; the failed resources is in red and pointing downwards. An upward trend line for passed resources and a downward trend line for failed resources indicates good health of the resources.
- **Percentages in the trend line** - The Percentages depend on the value selected in the Time Range field. For example, over a seven day time period, you can view the summary of all resources monitored, passed, and failed. The percentage is calculated by comparing this seven day data with the previous seven day data and displays the difference in percentages.

© 2019 Palo Alto Networks, Inc.

If there is no data in the previous time range, the difference in percentages is calculated with whatever data is available. For example, if you want to see the percentages for the last 3 months, and the data is available for only 4 months, the 3 months data is compared with previous one-month data and the displays the difference in percentages. If you select All Time, there is no prior all-time period to compare against, and it will present 0% change for trending data.

© 2019 Palo Alto Networks, Inc.

SecOps Dashboard

Use the SecOps dashboard to get insights into Accounts and Account Types, Resources, Alerts, Resources by Risk Ranking, Risk Rating by Account, Policy Violations, etc. The dashboard provides a view of the performance of resources, traffic, connections, and user actions in a graphical or tabular format.

Monitored Accounts

This graph shows the number of accounts Prisma Cloud is monitoring.

Monitored Resources

Prisma Cloud considers any cloud entity that you work with as a resource. Examples of resources include AWS Elastic Compute Cloud, Relational Databases, AWS RedShift, Load Balancers, Security Groups, NAT Gateways The Resources graph shows the total number of resources that you currently manage. It gives you a view into the potential growth in the number of resources in your enterprise over a period of time. Hover over the graph to see data as per the timeline.

Open Alerts

Whenever a resource violates a policy, Prisma Cloud generates alerts flagging these policy violations. The Open Alerts graph shows the number of alerts that were generated. The purpose of this graph is to demonstrate risk trends over a timeline. Click on the alert number to go to the 'Alerts' section and get the detailed view of the alerts.

Risk Rating by Scanned Accounts

Each resource in Prisma Cloud belongs to a specific account. The intent of this graph is to show all the accounts and their associated resources with their risk scoring. This graph is very useful in telling which accounts are the most vulnerable at any given time (in other words, have the most number of resources with an F or C score), and need to be fixed first. For details on how risk rating is calculated see Risk Rating of a Resource in Prisma Cloud.

Top Instances by Role

This graph summarizes top open ports in your cloud environments and the percentage of the traffic directed at each type of port. The purpose of this graph is to show what types of applications (web server, database) the top workloads are running.

Alerts by Severity

Alerts are graphically displayed and classified based on their severity into High, Medium, and Low. By clicking on the graph, you can directly reach the alerts section.

Policy Violations by Type over Time

This graph displays the type of policy violations (network, config, audit event) over a period of time.

Top Policy Violations

This graph displays the alerts generated by each type of policy over a period of time.

© 2019 Palo Alto Networks, Inc.

Top Internet Connected Resources

This graph displays top internet connected workloads by role, so you know which workloads are connecting to the Internet most of the time and are prone to malicious attacks. For this report, ELB & NAT Gateway data are filtered out, but includes data from other roles. The data in this chart is based on the account and the time filter.

Connections from the Internet

On a world map, you can see the internet traffic to different workloads from different geographical locations, so that you know where the connections are originating from. Workloads are shown as roles, and roles are defined in the Network query. The roles are: RDS, RedShift, NAT Gateway, ELB, EC2 broken down into: Generic (Generic EC2), FTP, SSH, Database etc. Use Time and Account filters to customize your views.

You can see a world map with total inbound+outbound connections from Internet to all the workloads. Each location on the map shows total # of bytes to that location across all workloads. Regular internet traffic, suspicious traffic and all accepted traffic from suspicious IP addresses are color coded.

By default, the map shows aggregated numbers by specific regions in the map but you can zoom in on any of the regions in the map a get more granular detail on the specific location.

You can use the multi-select filter option available on the map to only present information for the type of workload(s) you are interested in viewing traffic for. The filter options include: EC2, AWS RDS, AWS RedShift, ELB, NAT Gateway. anything else that is classified as database), ELB, S3, NAT Gateway. By default, traffic hitting destination resources with role NAT Gateway, ELB, Web Server, HTTP is filtered out, but includes traffic for any of those roles.

To see the network graph representing connections, click on any of the connections from a specific region and get redirected to the Investigate page to see the network graph. The resultant network query will have the IP address, dest roles as well as the time filters carried forward so you can pin point to a specific incident.

© 2019 Palo Alto Networks, Inc.

Export Data and Customize the SecOps Dashboard

You can export SecOps dashboard data to a PDF or a png to have an offline PDF copy of a chart. You can also choose to view the data in a table.

- Select **Dashboard** > **SecOps** and click **Customize**.
- Toggle **Show**

or **Hide** to view or hide a widget.
- Select the icons on the screen to choose whether you want to maximize the screen space for a widget or fit two or three widgets in a row.
- Select a widget and click **View as table** to view the data in a tabular format.

- Select a widget and click **Download PNG image** or **Download PDF document** to save an offline PNG image or PDF document of your data.

© 2019 Palo Alto Networks, Inc.

RedLock
Dashboard
Investiga
Asset Inventory
SecOps
Time Range
Last 24 hours
Top Instances by Role
Download PNG image
Download PDF document
61
Instances
Database
Web Server
Generic (445)
Web (80)
RDP

Prisma Cloud Policies

In Prisma Cloud, a policy is a set of one or more constraints or conditions that must be adhered to. Prisma Cloud provides predefined policies for configurations and access controls that adhere to established security best practices such as PCI, GDPR, ISO 27001:2013,and NIST. These Prisma Cloud default polices cannot be modified.

In addition to these, you can create custom policies to monitor for violations and enforce your own organizational standards. You can use the Default policies as templates to create custom policy. After you set up the policies, any new or existing resources that violate these policies are automatically detected.

> Create a Policy on Prisma Cloud
> Manage Prisma Cloud Policies
> Anomaly Policies

© 2019 Palo Alto Networks, Inc.

Create a Policy on Prisma Cloud

Create a custom policy with remediation rules that are tailored to meet the requirements of your organization. When creating a new policy, you can either build the query using RQL or you use a saved search to automatically populate the query you need to match on your cloud resources. If you want to enable auto-remediation, Prisma Cloud requires write access to the cloud platform to successfully execute the remediation commands.

You can create three types of policies:

- **Config**—Configuration policies monitor your resource configurations for potential policy violations.
- **Network**—Network policies monitor network activities in your environment.
- **Event**—Event policies monitor audit events in your environment for potential policy violations. You create audit policies to flag sensitive events such as root activities or configuration changes that may potentially put your cloud environment at risk.

When creating a custom policy, as a best practice do not include cloud.account, cloud.account.group or cloud.region attributes in the RQL query. If you have a saved search that includes these attributes, make sure to edit the RQL before you create a custom policy. While these attributes are useful to filter the results you see on the Investigate tab, they are ignored when used in a custom policy.

STEP 1 | Select **Policies** and click **+Add New**.

STEP 2 | Enter a **Policy Name** and **Severity** and optionally a **Description** and **Labels** and click **Next**.

STEP 3 | Build the query to define the match criteria for your policy by using a **New Search** or a **Saved Search** and click **Next**.

If you are building a **Query** using a **New Search**, you can select from predefined options to build the query.

© 2019 Palo Alto Networks, Inc.

Keep in mind that Config queries used in a policy should have some mandatory attributes. It should at a minimum have **`api.name`** in conjunction with **`json.rule`** or it can have **`hostfinding.type`** or it can have two **`api.name`** attributes with a **`filter`** attribute.

```
config where cloud.type = 'azure' AND api.name = 'azure-network-usage' AND
 json.rule = StaticPublicIPAddresses.currentValue greater than 1
```

```
config where hostfinding.type = 'Host Vulnerability'
```

```
config where api.name = 'aws-ec2-describe-internet-gateways' as
 X; config where api.name = 'aws-ec2-describe-vpcs' as Y; filter
 '$.X.attachments[*].vpcId == $.Y.vpcId and $.Y.tags[*].key contains
 IsConnected and $.Y.tags[*].value contains true'; show Y;
```

STEP 4 | Associate compliance standards with your policy.

1. Choose the compliance **Standard**, **Requirement**, and **Section**.
2. Click **+** to add more standards as required and click **Next**.

STEP 5 | Enter details in the remediation section if you want your policy violation alerts to be automatically remediated.

1. Enter steps to remediate your policy in **Recommendation for Remediation**.
2. Enter Command Line remediation commands in **CLI Remediation**.

   The parameters that you can use to create remediation commands are displayed on the interface as CLI variables:

   - **`$account`**—Account is the Account ID of your account in Prisma Cloud.
   - **`$gcpzoneid`**—(GCP only) Allows you to specify the zone in the GCP project, folder, or organization where the resource is deployed.

© 2019 Palo Alto Networks, Inc.

- **`$azurescope`**—(Azure only) Allows you to specify the node in the Azure resource hierarchy where the resource is deployed.
- **`$region`**—Region is the name of the cloud region to which the resource belongs.
- **`$resourceid`**—Resource ID is the identification of the resource that triggered the alert.
- **`resourcegroup`**— (Azure only) Resource Group identifies the Azure Resource Group Name for the resource that triggered the alert.
- **`$resourcename`**—Resource name is the name of the resource that triggered the alert.

3. Click **Validate syntax** to validate the syntax of your code.
4. Click **Save**.

   All your System Administrators and Account Administrators are notified when there is a change to the CLI commands.

© 2019 Palo Alto Networks, Inc.

Manage Prisma Cloud Policies

Use the following workflows to manage your Prisma Cloud policies. You can download policy data, clone, enable, delete, or disable policies from the **Policies** page.

- To enable Prisma Cloud default policies click Settings and select **Enterprise Settings**.

  You can enable policies based on severity—High, Medium, or Low.

When you **Save** your changes, you can choose one of the following options:

- **Enable and Save**—With Enable and Save, you are enabling all existing policies that match your selection criteria and new Prisma Cloud default policies that are periodically added to the service. This option allows you to enable and scan your resources against all existing and new policies to help you stay ahead of threats and misconfigurations.
- **Save**—With Save, you are saving your selection criteria and enabling new Prisma Cloud default policies only as they are periodically added to the service. New policies that match your selection, are automatically enabled and your resources are scanned against them after you made the change.

© 2019 Palo Alto Networks, Inc.

The audit logs include a record of all activities performed in Prisma Cloud. To view the audit logs click Settings and select Audit Logs.

- To view policies, select **Policies**.

- To filter **Policies** enter a keyword in the **Filter Results** search box or click **Add Filters** and select the filtering criteria.

© 2019 Palo Alto Networks, Inc.

- To download the details of your policies (or a filtered set of policies) in CSV format so that you can have an offline copy, click Download.

- To enable or disable any policy toggle the **Status**.

- To edit a custom policy, click the policy and you can edit the details.

You cannot edit a Prisma Cloud Default policy.

- To delete a policy, select the policy and click **Delete**.

© 2019 Palo Alto Networks, Inc.

- To clone a policy, select the policy and click **Clone**.

  Cloning a policy is creating a copy of an existing policy. Cloning serves as a quick method of creating a new policy if you choose to change few details of the source policy.

  Prisma Cloud comes with default policies. If you want to modify any details, you can clone a policy and then modify details.

- To view Alerts associated with a policy click **View Alerts**.

© 2019 Palo Alto Networks, Inc.

Anomaly Policies

Anomaly policies help with identifying unusual user activity. These policies rely on a third-party feed to resolve IP addresses to geo-locations and perform user entity behavior analysis (UEBA). Before the service can detect unusual activity for your enterprise, you must Define Prisma Cloud Enterprise Settings to specify a training threshold and set the baseline for what are normal trends in your network.

Prisma Cloud includes three anomaly policies that are predefined and marked as Default policies:

Account hijacking attempts—Are potential account hijacking attempts discovered by identifying unusual login activities. These can happen if there are concurrent login attempts made in short duration from two different geographic locations or from a previously not known browser, operating system, or location.

Excessive login failures—Are potential account hijacking attempts discovered by identifying brute force login attempts.

Unusual user activity—Is an insider threat and an account compromise discovered using advanced data science. The Prisma Cloud machine learning algorithm profiles a user's activities on the console, as well as the usage of access keys based on the location and the type of cloud resources.

NAME	CLOUD	SEVERITY	POLICY TYPE	LABELS	REMEDIABLE	POLICY MODE	COMPLIANCE STANDARD	STATUS
Unusual user activity		Low	Anomaly	zz		RedLock Default	GDPR, HIPAA & 2 More	
Excessive login failures		High	Anomaly			RedLock Default	GDPR, NIST CSF & 1 More	
Account hijacking attempts		Medium	Anomaly			RedLock Default	GDPR, NIST CSF & 1 More	

Alerts generated by these anomaly policies are grouped by policy and then by user. Because the same IP address can resolve to different locations at different points in time and lead to false positives, if there is an unusual user activity from a previously unseen location but the IP address has been seen before, Prisma Cloud does not generate an anomaly alert. If you see multiple alerts of the same type (accessing a resource that you have already accessed and one that is flagged as an anomaly), a single alert is generated. However, if the same user accesses another type of resource that the service hasn't ingested before, a distinct alert is generated.

Investigate Incidents on Prisma Cloud

Prisma Cloud helps you visualize your entire cloud infrastructure and provides insights into security and compliance risks.

Prisma Cloud helps you connect the dots between configuration, user activity, and network traffic data, so that you have the context necessary to define appropriate policies and create alert rules.

To conduct such investigations, Prisma Cloud provides you with a proprietary query language called RQL that is similar to SQL.

> Investigate Config Incidents on Prisma Cloud
> Investigate Audit Incidents on Prisma Cloud
> Use Prisma Cloud to Investigate Network Incidents

© 2019 Palo Alto Networks, Inc.

Investigate Config Incidents on Prisma Cloud

Prisma Cloud ingests various services and associated configuration data from AWS, Azure, and GCP cloud services. You can retrieve resource information and identify misconfigurations. You can also gain operational insights and identify policy and compliance violations.

To investigate configurations you can use Config queries. Enter your queries in the Search. If the search expression is valid and complete, you can see a green check mark and results of your query.

You can choose to save the searches that you have created for investigating incidents in **My Saved Searches**. Use these queries for future reuse, instead of typing the queries all over again. You can also use the Saved Searches to create a policy.

Saved Searches has list of search queries saved by any user in the system.

Select a record to view the Audit Trail or Host Findings. The alerts are presented when you select the red exclamation mark.

© 2019 Palo Alto Networks, Inc.

Hover over the config record to see the option to view the details of the resource config.

To analyze your Config events offline, you can download the event search details in a CSV format, click **Download** on the right hand corner.

© 2019 Palo Alto Networks, Inc.

Investigate Audit Incidents on Prisma Cloud

Prisma Cloud ingests various services and associated user and event data from AWS, Azure, and GCP cloud services. You can investigate console and API access, monitor privileged activities and detect account compromise and unusual user behavior in your cloud environment.

To investigate audit data you can use Event queries. To build Event RQL queries, enter your query in the Search; use the auto-suggest for the attribute **`json.rule`** with the operators **=** and **`IN`**, (auto suggestion is not available for array objects). If the search expression is valid and complete, you can see a green check mark and results of your query. You can choose to save the searches that you have created for investigating incidents in **My Saved Searches**. Use these queries for future reuse, instead of typing the queries all over again. You can also use the Saved Searches to create a policy. **Saved Searches** has list of search queries saved by any user in the system.

After you run event search queries, you can view the results in **Table View**, **Trending View**, or in **Map View**. By default you can see the details in the Table view. To pick the columns in the Table view, use the Column Picker on the Right hand corner.

From the table view, select **View Event Details** to see the resource configuration details.

To analyze your Audit events offline, you can download the event search details in a CSV format, click **Download** on the right hand corner.

© 2019 Palo Alto Networks, Inc.

Select **Trending View** to see the results in a timeline. Single click the bubble to view the results for a given timeline. Double click the bubble to drill down further.

Select **Map View** to see a World map with pinpoints to the locations where there are activities and anomalies. You can view usual activities and anomalous activities to their specific locations. Single click on the bubble in the map view to view results for the given location. Double click on the bubble in the map view to drill down further.

© 2019 Palo Alto Networks, Inc.

Use Prisma Cloud to Investigate Network Incidents

Prisma Cloud ingests and monitors network traffic from cloud services and allows customers to query network events in their cloud environments. You can detect when services, applications or databases are exposed to the internet and if there are potential data exfiltration attempts. Network queries are currently supported for AWS and Azure cloud.

To view network traffic data, you can use Network queries. Enter your queries in the Search. If the search expression is valid and complete, you can see a green check mark and results of your query. You can choose to save the searches that you have created for investigating incidents in **My Saved Searches**. Use these queries for future reuse, instead of typing the queries all over again. You can also use the Saved Searches to create a policy. **Saved Searches** has list of search queries saved by any user in the system.

Network queries enable you to search for network resources or network flows. By using packets, bytes, source or destination resource, source or destination IP address, and source or destination port information, these queries enable you to monitor traffic and the interconnectivity of the resources that belong to your cloud accounts and regions.

To download network traffic details for your entire network, a node or an instance, or for a specific connection between a source and a destination node in a CSV format, click **Download** on the top right hand corner. This report groups all connection details by port and includes details such as source and destination IP addresses and names, inbound and outbound bytes, inbound and outbound packets, and whether the node accepted the traffic connection

To see the details of a network resource, click the resource and view **Instance Summary**, **Network Summary**, or **Alert Summary**.

© 2019 Palo Alto Networks, Inc.

To see the accepted and rejected traffic, from **Network Summary** click **Traffic Summary**.

To view details of a connection, click the connection and click **View Details**.

Prisma Cloud Compliance

Prisma Cloud enables you to view, assess, report, monitor and review your cloud infrastructure health and compliance posture. You can also create reports that contain summary and detailed findings of security and compliance risks in your cloud environment.

> Compliance Dashboard
> Download Compliance Standards
> Create a Custom Compliance Standard
> Add a New Compliance Report

© 2019 Palo Alto Networks, Inc.

Compliance Dashboard

The Compliance Dashboard provides information related to your compliance posture across various compliance standards. The supported compliance standards are:

Cloud Type	Compliance Standards Supported
AWS	CIS v1.2, CSA CCM v3.0.1,GDPR, HITRUST v9.2, HIPAA, NIST 800.53 R4, NIST CSF v1.1,PCI DSS v3.2, SOC 2
Azure	CIS v1.0, CSA CCM v3.0.1,HIPAA, NIST 800.53 R4, PCI DSS v3.2, SOC 2
GCP	CIS v1.0, CSA CCM v3.0.1, GDPR, HIPAA, NIST 800.53 R4, NIST CSF v1.1,PCI DSS v3.2, SOC 2

Unlike the Asset Inventory Dashboard that aggregates all your resources and displays the pass and fail count for all monitored resources, the Compliance Dashboard only displays the results for monitored resources that match the policies included within a compliance standard. For example, even if you have 30 AWS Redshift instances, if none of the compliance standards include policies that check the configuration or compliance and security standards for Redshift instances, the 30 Redshift instances are not included in the resource count on the Compliance Dashboard. The results on the Compliance Dashboard therefore, help you focus your attention on the gaps in compliance for a standard or regulation that is important to you.

The filters on the Dashboard allow you to view your status across different cloud accounts, regions, and for specific compliance mandates.

At a glance the dashboard includes

- **Compliance Trendline**—The trendline on the compliance dashboard enables you to monitor the overall health of the cloud resources in your organization. The trendline shows you the variance at which your resources are monitored, if they are passing or if they are failing. For example, when you set the time range to the last 7 days, and view the total number of resources monitored, and the number of resources that passed and failed over that time period. Prisma Cloud compares this data with the preceding 7 days

© 2019 Palo Alto Networks, Inc.

and displays the variance as a percentage. The green color of the trendline percentage indicates progress or improvement while the red color indicates a decline.

If there is no data in the previous time period, the variance is calculated using available data. For example, if the last 3 months is selected and the data for only 4 months is available, the 3 months data is compared with one month data and the variance in percentages is displayed. If you select All Time, there is no prior all-time period to compare against, and it will present 0% change for trending data.

- **Passed Resources**—When the number of passed resources go up, the trendline is green and in the upward direction. When the number of passed resources go down, the trendline is in red in color and pointing downwards.
- **Failed Resources**—When the number of failed resources declines, the trendline is green and the arrow points upwards. When the number of failed resources increases, the trendline is red and points downwards.

  An ideal trendline is increasing for passed resources and decreasing for the failed resources. You can see this trendline in your organization across all the compliance standards or you can select any one standard and see the trendline only for it.
- The compliance dashboard is available for offline access as a CSV file. See Download Compliance Standards for information.
- You can associate the compliance standards with policies. The default compliance standards provided by Prisma Cloud have default policy mappings to different articles in the compliance standards like GDPR, NIST, CIS etc. In addition to using the default policy mappings, you can also create custom mappings to meet your specific enterprise needs.

© 2019 Palo Alto Networks, Inc.

Download Compliance Standards

Download compliance standard details in a CSV file so that you can have an offline copy.

STEP 1 | From **Compliance Dashboard** click Download to get a CSV file of all your compliance standards.

This file has details of your compliance standards which include, compliance standard name, description, number of resources that passed and failed for this standard, and also the number of policies associated with it.

STEP 2 | From **Compliance Dashboard** select one standard and click Download to get a CSV file of the selected standard.

This file has details of your selected compliance standard that includes compliance standard requirements, number of resources that passed and failed for the requirements within it, and also the number of policies associated with it.

© 2019 Palo Alto Networks, Inc.

Create a Custom Compliance Standard

You can create your own custom compliance standards that are tailored to your own business needs, standards, and organizational policies. When defining a custom compliance standard, you can add requirements and sections. A custom compliance standard that has a minimum of one requirement and one section can be associated with policies that check for adherence to your standards.

STEP 1 | Create a compliance standard.

1. From Prisma Cloud select **Compliance** > **Standards** > **+ Add New**.

2. Enter a name and description for the new standard and click Save ✓.

STEP 2 | Add requirements to your custom compliance standard.

1. Select the custom compliance standard you just added and click **+ Add New**.

© 2019 Palo Alto Networks, Inc.

2. Enter a requirement, name and a description and click Save ✓.

STEP 3 | Add sections to your custom compliance standard after adding the requirement.

1. Select the requirement for which you are adding the section and click **+Add New**.

2. Enter a name for the **Section** a **Description** and click Save ✓.

   Although you have added the custom standard to Prisma Cloud, it is not listed on the Compliance Standards table on **Compliance** > **Overview** until you add at least one policy to it.

STEP 4 | Add policies to your custom compliance standard.

You must associate Prisma Cloud Default policies or your custom policies to the compliance standard to monitor your cloud resources for adherence to the internal guidelines or benchmarks that matter to you. The RQL in the policy specifies the check for the resource configuration, anomaly or event.

1. Select **Policies**.

   Filter the policies you want to associate with the standard. You can filter by cloud type, policy type and policy severity, to find the rules you want to attach.
2. Select the policy rule to edit, on **3 Compliance Standards** click **+** and associate the policy with the custom compliance standard.

3. **Confirm** your changes.

© 2019 Palo Alto Networks, Inc.

Add a New Compliance Report

If you'd like to share an offline version of a compliance report with an audit agency or a stakeholder who does not have access to Prisma Cloud, you can create a PDF report. While the PDF is not interactive like the admin console, it is a quick and convenient way to share relevant information, highlight issues or provide takeaways. You can generate a report on your current compliance posture for the last 3 months, 6 months, or a year, or specify a custom time period for a historical snapshot of the compliance status of your environment.

STEP 1 | Log in to Prisma Cloud.

STEP 2 | Select **Compliance** > **Compliance Dashboard** and click **+New Report**.

You can also go to **Compliance** > **Reports** and click **+New Report**.

STEP 3 | Enter the following information and **Save** the report.

1. Select a **Cloud Type**.

   You must choose a cloud type—AWS, Azure, or GCP—for which you want to generate the compliance report.
2. Select a **Report Type**.

   See Compliance Dashboard for a list of compliance standards supported for each cloud platform.
3. Enter a descriptive **Name** for the report.
4. Select one or more cloud **Account Groups**.
5. Select one or more **Cloud Accounts**.
6. Select one or more cloud **Regions**.
7. Select the **Time Range** for which you want to generate the report.

STEP 4 | Download the report.

Click the download link to save a local copy of the report. The download will start as soon as the report is ready.

© 2019 Palo Alto Networks, Inc.

© 2019 Palo Alto Networks, Inc.

Configure External Integrations on Prisma Cloud

You can integrate Prisma Cloud with third-party services such as Jira, Slack, Splunk, Google CSCC, Qradar, and ServiceNow to enable you to receive, view and receive notification of Prisma Cloud alerts in these external systems. By integrating Prisma Cloud with third-party services you can have an aggregated view of your cloud infrastructure.

Similarly, Prisma Cloud integration with external systems such as Amazon GuardDuty, AWS Inspector, Qualys, and Tenable allow you to import vulnerabilities and provide additional context on risks in the cloud.

> Prisma Cloud Integrations
> Integrate Prisma Cloud with AWS Inspector
> Integrate Prisma Cloud with Amazon SQS
> Integrate Prisma Cloud with Amazon GuardDuty
> Integrate Prisma Cloud with AWS Security Hub
> Integrate Prisma Cloud with Google Cloud Security Command Center
> Integrate Prisma Cloud with Jira
> Integrate Prisma Cloud with Qualys
> Integrate Prisma Cloud with Slack
> Integrate Prisma Cloud with Splunk
> Integrate Prisma Cloud with Tenable
> #unique_81
> Integrate Prisma Cloud with QRadar
> Integrate Prisma Cloud with Webhooks
> Integrate Prisma Cloud with PagerDuty
> Integrate Prisma Cloud with Microsoft Teams
> Prisma Cloud Integrations—Supported Capabilities

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Integrations

Prisma Cloud provides multiple out-of-the-box integration options so that you can integrate Prisma Cloud into your existing security workflows and with the technologies you already use. The Amazon GuardDuty, AWS Inspector, Qualys, and Tenable integrations are inbound or pull-based integrations where Prisma Cloud polls for the data periodically and retrieves it from the external integration system; all the other integrations are outbound or push-based integrations where Prisma Cloud sends data about an alert or error to the external integration system.

- **Amazon GuardDuty**—Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Prisma Cloud integrates with Amazon GuardDuty and ingests vulnerability data to provide you with additional context on risks in the cloud.
- **AWS Inspector**—Amazon Inspector assesses applications for exposure, vulnerabilities, and deviations from best practices. It also produces a detailed list of security findings prioritized by level of severity. Prisma Cloud integrates with AWS inspector and ingests vulnerability data and security best practices deviations to provide you with additional context on risks in the cloud.
- **AWS SecurityHub**—AWS Security Hub acts as a central console to view and monitor the security posture of your cloud assets directly on the Amazon console. As the Prisma Cloud application monitors your assets on the AWS cloud and sends alerts on resource misconfigurations, compliance violations, network security risks, and anomalous user activities, you have a comprehensive view of all your cloud assets across all your AWS accounts directly to the Security Hub console.
- **Amazon SQS**—Amazon Simple Queue Service helps you send, store, and receive messages between software components at any volume, without losing messages or requiring other services to be always available. Prisma Cloud integrates with Amazon SQS to receive alerts. You can consume them through Splunk add-on or through CloudFormation to enable custom workflows.
- **Email**—Configure Prisma Cloud to send alerts as email to your email inbox.
- **Google Cloud SCC**—Google Cloud Security Command Center (Google Cloud SCC) is the security and data risk database for Google Cloud Platform. Google Cloud SCC enables you to understand your security and data attack surface by providing asset inventory, discovery, search, and management. Prisma Cloud integrates wtih Google Cloud SCC and sends alerts to the Google Cloud SCC console to provide centralized visibility into security and compliance risks of your cloud assets.
- **Jira**—Jira is an issue tracking, ticketing, and project management tool. Prisma Cloud integrates with Jira and sends notifications of Prisma Cloud alerts to your Jira accounts.
- **Microsoft Teams**—Microsoft Teams is a cloud-based team collaboration software that is part of the Office 365 suite of applications and is used for workplace chat, video meetings, file storage, and application integration. The Prisma Cloud integration with Microsoft Teams enables you to monitors your assets and sends alerts on resource misconfigurations, compliance violations, network security risks, and anomalous user activities either as they happen or as consolidated summary cards.
- **PagerDuty**—PagerDuty enables alerting, on-call scheduling, escalation policies and incident tracking to increase uptime of your apps, servers, websites and databases. The PagerDuty integration enables you to send Prisma Cloud alert information to PagerDuty service. The incident response teams can investigate and remediate the security incidents.
- **QRadar**—IBM QRadar is an enterprise security information and event management product. Integrate Prisma Cloud with QRadar to view Prisma Cloud alerts on the QRadar console to help you proactively detect threats and continuously improve detection
- **Qualys**—Qualys specializes in vulnerability management security software. They scan hosts for potential vulnerabilities. Prisma Cloud integrates with the Qualys platform and ingests vulnerability data to provide you with additional context on risks in the cloud.
- **ServiceNow**—ServiceNow is an incident, asset, and ticket management tool. Prisma Cloud integrates with Servicenow and sends notifications of Prisma Cloud alerts as ServiceNow tickets.

© 2019 Palo Alto Networks, Inc.

- **Slack**—Slack is an online instant messaging and collaboration system that enables you to centralize all your notifications. You can configure Prisma Cloud to send notifications of Prisma Cloud alerts through your slack channels.
- **Splunk**—Splunk is a software platform to search, analyze and visualize machine-generated data gathered from the websites, applications, sensors, and devices. Prisma Cloud integrates with cloud-based Splunk deployments and see Prisma Cloud alerts through Splunk event collector. Prisma Cloud can integrate with on-premises Splunk instances through the AWS SQS integration.
- **Tenable**—Tenable.io is a cloud-hosted Vulnerability Management solution designed to provide accurate visibility and insight about dynamic assets and vulnerabilities. Prisma Cloud integrates with the Tenable and ingests vulnerability data to provide you with additional context on risks in the cloud.
- **Webhooks**—The webhooks integration enables you to pass information in a JSON format to any third-party integrations that are not natively supported on Prisma Cloud. With a webhook integration you can configure Prisma Cloud to send alerts to the webhook URL as an HTTP POST request, so that any services or applications that subscribe to the webhook URL can receive alert notifications as soon as Prisma Cloud detects an issue.

For the outbound integrations with the exception of PagerDuty and email, Prisma Cloud performs periodic checks and background validation to identify exceptions or failures in processing notifications. The status checks are displayed on the Prisma Cloud administrator console—red if the integration fails validation checks for accessibility or credentials, yellow if one or more templates associated with the integration are invalid, or green when the integration is working and all templates are valid. Any state transitions are also displayed on the Prisma Cloud administrator console to help you find and fix potential issues.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Slack

Integrate Prisma Cloud with Slack to get instant messages on your Slack channels. This will help you to collaborate and centralize all your notifications.

STEP 1 | Set up Slack to get your application's webhook.

1. Log in to your web slack using your company URL. For example https://xxxxxxx.slack.com/apps/manage.
2. Select **Manage** > **Apps**.

3. Select **Incoming WebHooks**.

4. Click **Add Configuration**.

© 2019 Palo Alto Networks, Inc.

5. Select a channel and click **Add Incoming WebHooks Integration**.

6. Click **Save Settings**.

   Copy the **Webhook URL** from this page. You need to specify this URL in Prisma Cloud.

STEP 2 | Configure Slack in Prisma Cloud and complete setting up the integration channel.

1. Log in to Prisma Cloud.
2. Select **Settings** > **Integrations**.
3. Click **+New Integration** to create new integration.
4. Set the **Integration Type** as **Slack**.
5. Enter a name and a description for this integration.
6. Enter the **WebHook URL**.

© 2019 Palo Alto Networks, Inc.

7. Click **Next** and then click **Test**.

   The status check for Slack displays as red if Prisma Cloud receives any of the following errors —user not found or channel not found, channel is archived, action prohibited, posting to general channel denied, no service or no service ID, or no team or team disabled.

STEP 3 | Create an Alert Rule or modify an existing rule to send alerts to your Slack channels. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Splunk

Splunk is a software platform to search, analyze and visualize machine-generated data gathered from the websites, applications, sensors, and devices.

Prisma Cloud integrates with Splunk and monitors your assets and sends alerts on resource misconfigurations, compliance violations, network security risks, and anomalous user activities to Splunk.

STEP 1 | Set up Splunk HTTP Event Collector (HEC) to view alert notifications from Prisma Cloud in Splunk.

Splunk HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. This helps in the consolidation of alerts notifications from Prisma Cloud into Splunk so that your operations team can review, take action on the alerts.

1. To set up HEC, use instructions in Splunk documentation .
2. For **source type**, choose **_json**.
3. Select **Settings** > **Data inputs** > **HTTP Event Collector** and make sure you see HEC added in the list and that the status is **Enabled**.

STEP 2 | Set up the Splunk integration in Prisma Cloud.

1. Log in to Prisma Cloud.
2. Select **Settings** > **Integrations**.
3. Select **+New Integration** to create a new integration.
4. Set **Splunk** as the **Integration Type**.
5. Enter a name for the integration and a description.
6. Enter **Splunk HTTP Event Collector URL** that you set up earlier.

   Splunk HTTP Event Collector URL is a Splunk endpoint for sending event notifications to your Splunk deployment. You can either use HTTP or HTTPS for the purpose.
7. Enter **Auth Token**.

   The integration uses token-based authentication between Prisma Cloud and Splunk to authenticate connections to Splunk HTTP Event Collector. A token is a 32-bit number that is presented in Splunk.

© 2019 Palo Alto Networks, Inc.

8. Click **Test** and then **Save**.

   The integration status check for Splunk displays as red if the event collector URL is not reachable or times out, or if the authentication token is invalid or gets an HTTP 403 response.

STEP 3 | Create an Alert Rule or modify an existing rule to receive alerts in Splunk. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Amazon SQS

Prisma Cloud supports Amazon Simple Queue Service (SQS) to send alerts. Customers can consume them through Splunk add-on or through CloudFormation to enable custom workflows.

Alert notifications are triggered for each Alert generated as it happens with the entire Alert payload to Amazon SQS and Splunk. The CLI remediation (the actual CLI, any instructions for CLI) are included in the Alert Payload.

STEP 1 | Configure Amazon SQS to receive Prisma Cloud alerts.

1. Log in to Amazon console with necessary credentials to create SQS.
2. Click **Simple Queue Services** under **Messaging services**.
3. Click **Create New Queue** or use an existing queue.

4. Enter a Queue name and choose a Queue Type **Standard** or **FIFO**.
5. Click **Configure Queue**.

   For the attributes specific to the Queue, use either AWS default selection set them as per policies of your company. Select **Use SSE** to keep all messages in Queue encrypted.

© 2019 Palo Alto Networks, Inc.

6. Click **Create Queue**.

   Your SQS Queue is created and listed.
7. Click the Queue that you created and view the **Details** and copy **URL** of this queue.

   You will need to give this value in Prisma Cloud to integrate Prisma Cloud notifications into this Queue.

STEP 2 | If you are using encrypted queues in Amazon SQS, Prisma Cloud Role must be granted explicit permission to read the key.

1. On the Amazon console, select **IAM** > **Encryption Keys** and select **Create Key**

2. Enter Alias and Description. Select **KMS** and click **Next**.
3. Add any required **Tags** and click **Next**.

© 2019 Palo Alto Networks, Inc.

4. Choose IAM users who can use this Key through **KMS** API and click **Next**.
5. Choose IAM users who can use this key to encrypt and decrypt the data.
6. Review the Key policy and click **Finish**.

STEP 3 | Enable read-access permissions to Amazon SQS on the IAM Role policy.

The Prisma Cloud IAM Role policy you used to onboard your AWS setup needs these permissions:

```
"sqs:GetQueueAttributes", "sqs:ListQueues","sqs:SendMessage",
 "tag:GetResources"
```

If you used the CFT templates to onboard your AWS account, Prisma Cloud IAM role policy has the permissions required for Amazon SQS.

STEP 4 | Setup Amazon SQS integration in Prisma Cloud.

1. Log in to Prisma Cloud.
2. Select **Settings** > **Integrations**.
3. Select the **Integration Type** as **Amazon SQS**.
4. Enter a name and description for the Integration.
5. Enter the **Queue URL** that you copied while configuring Prisma Cloud in Amazon SQS.
6. Click **Next** and then click **Test**.

   You should get a success message.

7. Click **Save**.

   After you set up the integration successfully, if the SQS URL becomes unresponsive for any reason, the status transitions to red on **Settings** > **Integrations**, and updates to green if the issue gets resolved.

STEP 5 | Create an Alert Rule or modify an existing rule to enable the Amazon SQS Integration.

STEP 6 | Ingest SQS alerts through Splunk add-on.

1. Create an IAM user (or use AWS role) using the policy given below and store the Access Key ID and Secret Access key generated: E.g.: Value of key ‘Resource’ can be “arn:aws:sqs:us-east-1:123456789101:my_queue”.

© 2019 Palo Alto Networks, Inc.

```
{   "Version": "2012-10-17",   "Statement": [       {
          "Action": [                "sqs:*"
  ],            "Effect": "Allow",            "Resource”:
 [“arn:aws:sqs:<YOUR_SQS_QUEUE_REGION>:<YOUR_AWS_ACCOUNT_NUMBER>:<YOUR_SQS_QUEUE_NAM
          ]        }   ]}
```

2. Install the Prisma Cloud add-on from Splunk Market Place. Use the instructions at Splunk Add-on instructions.
3. Launch the app and from the **Inputs** tab, click **Create New Input**.

4. Add a new input. Each input will pull messages from a single queue in the region specified using Access Key Id and Secret Access Key provided.

   You can see the log messages using **index="_internal" "[RL SQS Poller]"**.

© 2019 Palo Alto Networks, Inc.

You can also see the events created by this poller using **index="<selected index>" source="rl_sqs_json"**

An Alerts CIM mapping is also created that can be accessed only if you have "Splunk Common Information Model" app. (https://splunkbase.splunk.com/app/1621) installed in your Splunk environment. To search using data model type **| datamodel Alerts search** in the search bar to get all the Alerts generated.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Amazon GuardDuty

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes VPC Flow Logs and AWS CloudTrail event logs. GuardDuty uses security logic and AWS usage statistics techniques to identify unexpected and potentially unauthorized and malicious activity.

Prisma Cloud integrates with and extends GuardDuty to provide additional threat visualization capabilities. Prisma Cloud starts ingesting GuardDuty data, correlates it with the other information that Prisma Cloud already collects, and presents a contextualized and actionable information through the Prisma Cloud app.

STEP 1 | Enable Amazon GuardDuty on your AWS instances. See Amazon Documentation.

STEP 2 | Enable read-access permissions to Amazon GuardDuty on the IAM Role policy.

The Prisma Cloud IAM Role policy you used to onboard your AWS setup needs to include these permissions:

```
guardduty:List*,                guardduty:Get*
```

If you used the CFT templates to onboard your AWS account, Prisma Cloud IAM role policy has the permissions required for Amazon GuardDuty.

STEP 3 | After Prisma Cloud has access to the Amazon GuardDuty findings, you can use the following RQL queries for visibility into the information collected from Amazon GuardDuty.

Config Query

```
config where hostfinding.type = 'AWS GuardDuty Host'
```

Network Query

```
network where dest.resource IN ( resource where hostfinding.type = 'AWS
 GuardDuty Host' )
```

Click on the resource to see the **Audit Trail**.

© 2019 Palo Alto Networks, Inc.

Click **Host Findings** for information related to vulnerabilities. Select **AWS GuardDuty Host** or **AWS GuardDuty IAM** in the filter to view vulnerabilities detected by AWS GuardDuty.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with AWS Inspector

Prisma Cloud ingests vulnerability data and security best practices deviations from Amazon Inspector to provide organizations with additional context on risks in the cloud. You can identify suspicious traffic to sensitive workloads such as databases with known vulnerabilities.

STEP 1 | Enable AWS Inspector on your EC2 instances. To set up AWS Inspector see Amazon documentation.

STEP 2 | Enable read-access permissions to AWS Inspector on the IAM Role policy.

The Prisma Cloud IAM Role policy that you used to onboard your AWS setup needs these permissions:

```
inspector:Describe*
      inspector:List*
```

If you used the CFT templates to onboard your AWS account, Prisma Cloud IAM role policy has the permissions required for AWS Inspector.

STEP 3 | After the Prisma Cloud service begins ingesting AWS Inspector data, you can use the following RQL queries for visibility into the host vulnerability information collected from AWS Inspector.

- Config queries

```
config where hostfinding.type = 'AWS Inspector Runtime Behavior Analysis'
```

```
config where hostfinding.type = 'AWS Inspector Security Best Practices'
```

AWS Inspector Runtime Behavior Analysis - Fetches all resources which are in violation of one or more rules reported by the AWS Runtime Behavior Analysis package.

© 2019 Palo Alto Networks, Inc.

AWS Inspector Security Best Practices - Fetches all resources which are in violation of one or more rules reported by the AWS Inspector security best practices package.

- Network queries

```
network where dest.resource IN ( resource where hostfinding.type = 'AWS
 Inspector Runtime Behavior Analysis' )
```

```
network where dest.resource IN ( resource where hostfinding.type = 'AWS
 Inspector Security Best Practices' )
```

Click on the resource to see an Audit trail.

Click **Host Findings** for information related to vulnerabilities.

© 2019 Palo Alto Networks, Inc.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with AWS Security Hub

You can use AWS Security Hub as a central console to view and monitor the security posture of your cloud assets on the Amazon console.

Integrate Prisma Cloud with AWS Security Hub for centralized visibility into security and compliance risks of your cloud assets on the AWS Security Hub console.

As part of the integration, Prisma Cloud monitors your assets on your AWS cloud and sends alerts on resource misconfigurations, compliance violations, network security risks, and anomalous user activities directly to the Security Hub console so that you have a comprehensive view of your cloud assets deployed on your AWS accounts.

STEP 1 | Attach AWS Security Hub read-only policy to your AWS administrator user's role to enable this integration on the Amazon console.

1. Log in to the AWS console and select IAM.
2. Select **Users** and select the AWS administrator who is creating the integration.
3. Click **Add permissions**.

4. Click **Attach existing policies Directly**.

5. Select **AWSSecurityHubReadOnlyAccess** and click **Next:Review**.

© 2019 Palo Alto Networks, Inc.

6. Click **Add Permissions**.

STEP 2 | Sign up for Prisma Cloud on AWS Security Hub.

1. Log in to the AWS console and select **Security Hub**.

2. Select **Settings** > **Integrations** and enter **Palo Alto Networks** as the search term.

© 2019 Palo Alto Networks, Inc.

3. Find **Palo Alto Networks: Prisma Cloud** and **Enable Integration**.

STEP 3 | Set up the AWS Security Hub Integration on Prisma Cloud.

Set up the AWS Security Hub as an integration channel on Prisma Cloud so that you can view security alerts and compliance status for all your AWS services directly on the AWS console.

1. Log in to Prisma Cloud.

© 2019 Palo Alto Networks, Inc.

2. Select **Settings** > **Integrations**.
3. Select **+New Integration**.
4. Select **AWS Security Hub** as the **Integration Type.**.
5. Set the **Integration Name** to the AWS account to which you assigned AWS Security Hub read only access.
6. Enter a **Description** and select a **Region**.

   You will be able to select regions only if you have enabled Prisma Cloud on AWS Security Hub for your cloud account.

7. Click **Next** and then **Test**.

After you set up the integration successfully, if there is a permission exception for the enabled regions, the status transitions to red on Settings > Integrations, and updates to green if the issue gets resolved.

STEP 4 | Modify an existing Alert rule, or create a new Alert Rule to send Alert notifications. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

© 2019 Palo Alto Networks, Inc.

STEP 5 | View Prisma Cloud alerts on AWS Security Hub.

1. Log in to the AWS console and select **Security Hub**.
2. Click **Findings** to view the alerts.
3. Select the **Title** to view details on the alert description.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Jira

Integrate Prisma Cloud with Jira and receive Prisma Cloud alert notifications in your Jira accounts. With this integration, you can automate the process of generating Jira tickets with your existing security workflow.

To set up this integration, you need to coordinate with your Jira administrator and gather the inputs you need to enable communication between Prisma Cloud and Jira.

This integration supports Jira Cloud and Jira On-Prem v7.2.0 and v7.2.13.

STEP 1 | Configure Prisma Cloud in your Jira account.

1. Login to Jira as a Jira Administrator.
2. Locate **Application Links**.

   For Jira Cloud, select **Jira Settings** > **Products** > **Application Links**.

   For Jira On-Prem, select **Settings** > **Applications** > **Application Links**.

© 2019 Palo Alto Networks, Inc.

3. Enter the URL for your instance of Prisma Cloud in **Configure Application Links** and click **Create new link**.

   See Access Prisma Cloud for details on the URL.

4. Disregard the message in **Configure Application URL** and click **Continue**.

5. Enter the **Application Name** and set the **Application Type** as **Generic Application**.
6. Select **Create incoming Link** and click **Continue**.

© 2019 Palo Alto Networks, Inc.

7. In the Link Applications, give any value for **Consumer Key** and specify a **Consumer Name**. Keep the **Consumer Key** handy. You need this value when you enter the information in Prisma Cloud.

8. copy the **Public Key** shown below and click **Continue**.


```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnYoXB
+BZ555jUIFyN+0b3g7haTchsyeWwDcUrTcebbDN1jy5zjZ/vp31//
L9HzA0WCFtmgj5hhaFcMl1bCFY93oiobsiWsJmMLgDyYBghpManIQ73TEHDIAsV49r2TLtX01iRWSW65Cef
+SMj/hyB59LPVin0bf415ME1FpCJ3yow258sOT7TAJ00ejyyhC3igh
+nVQXP+1V0ztpnpfoXUypA7UKvdI0Qf1ZsviyHNwiNg7xgYc
+H64cBmAgfcfDNzXyPmJZkM7cGC2y4ukQIDAQAB
```


© 2019 Palo Alto Networks, Inc.

Prisma Cloud is listed in your JIRA account after successful creation.

STEP 2 | Setup Jira as one of the integration channels in Prisma Cloud.

1. Login to Prisma Cloud.
2. Select **Settings** > **Integrations**.
3. Click **+ Add New**.
4. Set **Integration** to **JIRA**.
5. Specify a meaningful **Integration Name** and optionally a **Description**.
6. Enter the **JIRA Login URL**.

   Make sure the URL starts with https and does not have a trailing slash '/'at the end.

7. Enter the Consumer Key that you created when you created the Prisma Cloud application in Jira and **Generate Token**.

8. After you see the `Token Generated` message, click **Next**.
9. Click the link to retrieve your secret key.

   The URL with the verification code is valid for 10 minutes only.

© 2019 Palo Alto Networks, Inc.

10. When redirected to the **Welcome to JIRA** page, click **Allow** to give Prisma Cloud read and Write access to your data in your JIRA account.

11. Copy the verification code displayed on the page. Paste it in the **Secret Key** field and click **Generate Token**.

© 2019 Palo Alto Networks, Inc.

The integration will be listed on the Integrations page.

STEP 3 | Create JIRA notification templates to configure and customize Prisma Cloud alerts.

The JIRA fields that are defined as mandatory in your project are displayed in the template. The types of fields in Jira like text, list, single select check boxes, and option type fields are supported in Prisma Cloud. If you add any other type of fields in Jira (for example date fields) as mandatory, the template creation fails. Don't make any Date fields as Mandatory and define the text fields in Jira as free-form text so that the alert data is displayed correctly and completely.

1. Log in to Prisma Cloud.
2. From **Alerts**, select **Notification Templates** and click **+Add New**.
3. Enter a **Template Name**.
4. Select an **Integration**.
5. Select your **Project**.

   Select the project where you want to see the Prisma Cloud alerts. Because every alert translates into a Jira ticket, as a best practice create and use a dedicated project for Prisma Cloud ticketing and issue management.
6. Select your **Issue Type** and click **Next**.

© 2019 Palo Alto Networks, Inc.

7. Select the **Configurable Fields** that you would like to populate.

   The JIRA fields that are defined as mandatory in your project are already selected and included in the alert.

8. Select information that goes into **Summary** and **Description** from the alert payload.
9. Select the **Reporter** for your alert from users listed in your Jira project.

   This option is available only if the administrator who set up this integration has the appropriate privileges to modify the reporter settings on Jira.

© 2019 Palo Alto Networks, Inc.

10. Click **Next** to go to review pane and review your selection.

11. Click **Save**.

You can delete or edit the JIRA notification from the Notification Template page.

© 2019 Palo Alto Networks, Inc.

After you set up the integration, Prisma Cloud performs periodic status check with Jira, and the status transitions to red if the Jira Login URL is not reachable or any request to Jira results in an HTTP 400 or 403 response.

STEP 4 | Create an Alert Rule or modify an existing rule to send alerts to JIRA.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Qualys

Prisma Cloud integrates with the Qualys platform to ingest and visualize vulnerability data on your resources deployed on the AWS and Azure cloud platforms.

STEP 1 | Gather the information that you need to set up the Qualys Integration on Prisma Cloud.

- Qualys POD/SOC server API URL.

  To get the API URL, on your Qualys account, click **Help** > **About**. The Qualys API URL is listed under **Qualys Scanner Appliances**. When you enter this URL in to the **Qualys API Server URL**, omit :443.

- Qualys user with Manager or Unit Manager role to have the privileges required to enable the integration. You can modify the Manager role to enable read-only access permissions only. Refer to the Qualys documentation for details on User Roles Comparison (Vulnerability Management).
- The Qualys user requires the Vulnerability Management (VM), Cloud Agent (CA), and Asset View (AV) enabled.
- The Qualys user requires Qualys API and Qualys EC2 API access enabled.
- (For AWS) Qualys Sensors for AWS cloud such as Virtual Scanner Appliances, Cloud Agents, AWS Cloud Connectors, Internet Scanners have to be setup.

  The cloud agents or the cloud connectors enable the retrieval of vulnerability data in to Prisma Cloud so that you can correlate this data against your AWS asset inventory. Refer to the Qualys documentation for information.
- (For Azure) For Azure accounts, deploy the Qualys Virtual Scanner Appliance using Microsoft Azure Resource Manager (ARM). See Qualys documentation.

© 2019 Palo Alto Networks, Inc.

You can use Qualys Cloud Agents (Windows and Linux) for Azure instances from the Azure Security Center console and view vulnerability assessment findings within Azure Security Center and your Qualys subscription. See Qualys Documentation .

- (For Azure) Make sure that **Azure VM Information** is visible in Qualys.

STEP 2 | Set up Qualys Integration on Prisma Cloud.

1. Select **Settings** > **Integrations**.
2. Click **+New Integration** to create new integrations.
3. Set the **Integration Type** as **Qualys**.
4. Enter a Integration name and a description.
5. Enter the **Qualys API Server URL (without http[s])**.

   This is the **API URL** for your Qualys account. When you enter this URL in omit the protocol http(s) and the port :443.
6. Enter your Qualys **User Login** and **Password**.
7. Click **Next** and then click **Test**.

© 2019 Palo Alto Networks, Inc.

8. Click **Save**.

   The integration will be listed on the Integrations page. You can enable, disable, or delete your integration from this page.

STEP 3 | View Qualys host vulnerability data in Prisma Cloud.

After Prisma Cloud has access to the Qualys findings, you can use RQL queries for visibility into the host vulnerability information collected from Qualys.

1. Use Config queries for visibility on host vulnerabilities.

   Config Query

```
config where hostfinding.type = 'Host Vulnerability'
```


© 2019 Palo Alto Networks, Inc.

Click on the resource to get information about vulnerabilities. From **Audit Trail**, you can get the CVE numbers.

Click **Host Findings** for information related to vulnerabilities. The Source column in Host Findings displays the Qualys icon to help you easily identify the source for the vulnerability findings.

© 2019 Palo Alto Networks, Inc.

Network Query

```
network where dest.resource IN ( resource where hostfinding.type = 'Host
 Vulnerability' )
```

STEP 4 | Use the Qualys APIs on the CLI to confirm if API access is enabled for your account.

If you have trouble connecting with Qualys API, enter your user name, password and the URL for the Qualys service in the following Curl examples:

```
curl -H “X-Requested-With: Curl Sample” -u “Username:Password”
 “https://qualysapi.qg1.apps.qualys.in/api/2.0/fo/scan/?
action=list&echo_request=1”
```

```
curl -k “https://qualysapi.qg1.apps.qualys.in/msp/
asset_group_list.php” -u “Username:Password”
```


© 2019 Palo Alto Networks, Inc.

```
curl -k -H “X-Requested-With:curl” “https://
qualysapi.qg1.apps.qualys.in/api/2.0/fo/scan/stats/?action=list” -u
 “Username:Password”
```


© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Google Cloud Security Command Center

Integrate Prisma Cloud with Google Cloud SCC for centralized visibility into security and compliance risks of your cloud assets on the Google Cloud Platform.

You can setup this Integration for a GCP Organization that you are monitoring with Prisma Cloud. The alerts generated in Prisma Cloud for GCP accounts by your alert rule will be posted to CSCC. To show the Prisma Cloud alerts for cloud accounts of other cloud types (AWS, Azure) in Google SCC, contact Prisma Cloud Support.

STEP 1 | The Service account used to onboard the GCP Organization into Prisma Cloud should have the roles Viewer, Organization Viewer, and Security Center Findings Editor assigned.

STEP 2 | To view Assets and findings on CSCC console, enable **Cloud Security Command Center API**.

1. Go to the GCP Console API Library and select your GCP project.

   Make sure to enable **Cloud Security Command Center API** in the project which owns the Service Account that is used to onboard the GCP Organization into Prisma Cloud.
2. Select **Enable APIs and Services**.
3. Select **Cloud Security Command Center API** and enable it.

STEP 3 | Sign up for Prisma Cloud CSCC Solution on the Google console.

A Security Center Admin can setup this integration on the Google console.

1. Go to Google Console and search for **Prisma Cloud CSCC**.
2. Click **Visit Palo Alto Networks site to Signup**.

3. Select the organization that you onboarded into Prisma Cloud.
4. Select the **Service account** you used to onboard the GCP Organization.

© 2019 Palo Alto Networks, Inc.

5. Copy the **Source ID**. You need the **Source ID** when you setup this integration in Prisma Cloud
6. Click **Done**.

STEP 4 | Set up CSCC as one of the integration channels in Prisma Cloud.

1. Log in to Prisma Cloud.
2. Select **Settings** > **Integrations**.
3. Click **+New Integration**.
4. Select **CSCC** as the **Integration Type**.
5. Specify a meaningful Integration Name and a Description.
6. Enter the **Source ID** that you copied earlier when you signed up for the Prisma Cloud CSCC.

© 2019 Palo Alto Networks, Inc.

7. Select the **GCP Organization**.
8. Click **Next** and then **Test**.

   The service account must have adequate permissions as listed above for the integration to be successful. After you set up the integration successfully, if the there is an issue subsequently, the status transitions to red on **Settings** > **Integrations**, and updates to green if the issue gets resolved.

STEP 5 | Create an Alert Rule or modify an existing rule to send alerts to Google Cloud SCC. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

STEP 6 | View Alerts in CSCC

1. Go to Google Console and select **Security** > **Security Command Center**.

2. Click **Findings** to view the alerts.

© 2019 Palo Alto Networks, Inc.

3. Select the rule to see the details on the alerts.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Tenable

Prisma Cloud ingests vulnerability data from Tenable to provides you with additional context on risks in the cloud. This integration allows you to, for example, identify suspicious traffic to sensitive workloads such as databases with known vulnerabilities.

The Prisma Cloud integration with Tenable is supported in AWS, Azure, and GCP clouds.

STEP 1 | Tenable.IO provides API access to the assets and their vulnerability information. Configure the Tenable account to use the Tenable AWS, Azure and GCP Connector. Without the connectors, you can not identify the cloud resource.

Tenable's API requires an Access Key and Secret Key sent in the header. Generate Access Key and Secret Key per user on the Tenable.io app. See Tenable documentation for information. Also, make sure that the Tenable role that you use to enable this integration has Administrator permissions (with vulns-request-export and assets-request-export API access).

STEP 2 | Set up Tenable integration on Prisma Cloud.

1. Select **Settings** > **Integrations**.
2. Set the **Integration Type** as **Tenable**.
3. Enter a integration name and a description.
4. Enter the **Access Key** and the **Secret Key** that are generated in Tenable.io.

   See Tenable documentation for information.

5. Click **Test** to verify the integration.

STEP 3 | View vulnerabilities detected by Tenable in Prisma Cloud.

1. After Prisma Cloud has access to the Tenable findings, you can use the following RQL queries for visibility into the host vulnerability information collected from Tenable.

   Config Query

© 2019 Palo Alto Networks, Inc.

```
config where hostfinding.type = 'Host Vulnerability' AND
 hostfinding.source = 'Tenable' AND hostfinding.severity = 'high'
```

Select a resource to get information about vulnerabilities. Select **Audit Trail**, to view the CVE numbers.

Network Query

© 2019 Palo Alto Networks, Inc.

```
network where dest.resource IN ( resource where hostfinding.type = 'Host
 Vulnerability' )
```

Click **Host Findings** to see details.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with QRadar

The Prisma Cloud Qradar integration requires you to get the Prisma Cloud QRadar app on the IBM marketplace, set up an Amazon Simple Queue Service (SQS), and configure Prisma Cloud to send alerts to the SQS. When configured to publish messages to the SQS, Prisma Cloud sends alert messages to the SQS. The Prisma Cloud QRadar app polls the SQS at defined intervals to retrieve the alert messages and uses a custom extension to write the messages and the custom event mapping feeds into QRadar (on UDP port 514). This data is then displayed on the QRadar console to help you proactively detect threats and continuously improve detection.

STEP 1 | Install the Prisma Cloud QRadar app

1. Get the Prisma Cloud QRadar app from the IBM Market Place.
2. Login to QRadar Console.
3. Select **Admin** > **Extensions Management**.
4. Click **Add** and select the app zip file Prisma Cloud(_version).zip
5. Select **Install immediately**.
6. Select **Add** to install the app.

   Wait for validation and installation. On completion, you can view the App name on the screen.

7. Press Install button to add in the QRadar environment. Close the popup and go to Dashboard.

© 2019 Palo Alto Networks, Inc.

8. Select overwrite to install all the components required for this integration.

9. Click **Deploy Changes** on **Admin**.

STEP 2 | Configure the Prisma Cloud.

1. Set up AWS SQS queue. See Integrate Prisma Cloud with Amazon SQS.

   Configure the following permissions in SQS to access the logs from the queue:

```
SQS:DeleteMessage, SQS:GetQueueURL, SQS:GetQueueAttributes,
 SQS:ReceiveMessage, SQS:ChangeMessageVisibility
```


© 2019 Palo Alto Networks, Inc.

2. Login to the Qradar console.
3. From **Menu**, select the Prisma Cloud application that you installed and set these server settings.

	AWS SQS Settings
AWS Access Key	Unique key to access AWS SQS service
AWS Secret Key	Unique secret key to authenticate
AWS Region Name	Enter region name of the AWS SQS service
Queue Name	Target SQS queue name

	Proxy Server Settings
Proxy Host	Server Address / URL to point at for Proxy
Proxy Port	Port number
Proxy User	Proxy authentication user
Proxy Password	Proxy password
HTTP/HTTPS	Select the normal or ssl proxy

4. Click **Process Prisma Cloud logs**.

STEP 3 | Create the dashboard for viewing Prisma Cloud alerts.

1. Login to the Qradar console.
2. Select the following custom filters in a Search: **Log Source** as **RedLock** and **Payload** contains **RedLockLog**.

© 2019 Palo Alto Networks, Inc.

3. Create a dashboard using the Prisma Cloud fields such as **Severity**, **AlertID**, **Risk Rating**, **Alert Rule Name**, **Account Name**, **Resource Type**.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Webhooks

Integrate Prisma Cloud with webhooks to send Prisma Cloud alerts to webhooks and pass information to any third-party integrations that are not natively supported on Prisma Cloud. Your incident response teams can monitor the webhook channels to investigate and remediate security incidents. With a webhook integration, you can configure Prisma Cloud to send information to the webhook as an HTTP POST request, as soon as an alert is generated. And if you have internal services or applications that subscribe to the webhook, these subscribing clients can get data immediately in the JSON format.

STEP 1 | Have your **Webhook URL** and **Auth Code** ready.

STEP 2 | Set up webhooks as an integration channels on Prisma Cloud.

1. Log in to Prisma Cloud and select **Settings** > **Integrations**.
2. Select **+Add New**.
3. Set the **Integration Type** as **webhooks**.
4. Enter your **Webhook URL** and **Auth Code**.
5. Click **Next** and then click **Test**.

6. Click **Save** to save the integration.

   After you set up the integration successfully, if the Webhook URL is not reachable or if Prisma Cloud cannot authenticate successfully to it, the status transitions to red on **Settings** > **Integrations**, and updates to green if the issue gets resolved.

STEP 3 | Modify an existing Alert rule, or create a new Alert Rule to send Alert notifications to Webhook. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

STEP 4 | View the alert POST requests on Webhook.

In one POST request, alerts are sent in a batch of 30.

© 2019 Palo Alto Networks, Inc.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with PagerDuty

Integrate Prisma Cloud with PagerDuty to aid alerting, on-call scheduling, escalation policies and incident tracking to increase uptime of your apps, servers, websites and databases. When integrated, Prisma Cloud sends alerts to the PagerDuty service so that your incident response teams are notified to investigate and remediate the security incidents.

STEP 1 | Add a new service in PagerDuty and get the integration key. You have to provide this integration key in Prisma Cloud.

1. Log in to PagerDuty.
2. Click **Configuration** > **Services** and click **+New Service**.

3. Fill the **Add a Service** form.
4. In the **Integration Settings**, select the **Integration Type** as **Use our API Directly** and select **Events API V2**.

5. Click **Add Service** after filling out all your details.
6. Copy the **Integration Key** from Integrations and have it handy.

   You will need to give this integration key into Prisma Cloude while adding this integration.

© 2019 Palo Alto Networks, Inc.

For more information on integrations in PagerDuty, see PagerDuty Documentation.

STEP 2 | Set up PagerDuty as an integration channel on Prisma Cloud.

1. Log in to Prisma Cloud and select **Settings** > **Integrations**.
2. Select **+Add New**.
3. Set the **Integration Type** as **pagerduty**.
4. Enter the **Integration Key** of your Service on PagerDuty.
5. Click **Next** and then click **Test**.

6. Click **Save** to save this integration.

   Prisma Cloud creates a test incident and sends it to your Service in PagerDuty. To make sure that this integration is successful, look for the test integration in your PagerDuty Service.

© 2019 Palo Alto Networks, Inc.

STEP 3 | Modify an existing Alert rule, or create a new Alert Rule to send Alert notifications to PagerDuty. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

STEP 4 | View Prisma Cloud in PagerDuty.

In Pagerduty, all the open alerts have the incident state as **Triggered** and all the resolved alerts have the incident state as **Resolved**.

© 2019 Palo Alto Networks, Inc.

Integrate Prisma Cloud with Microsoft Teams

Microsoft Teams is a cloud-based team collaboration software that is part of the Office 365 suite of applications and is used for workplace chat, video meetings, file storage, and application integration.

Prisma Cloud integrates with Microsoft Teams and monitors your assets and sends alerts on resource misconfigurations, compliance violations, network security risks, and anomalous user activities either as they happen or as consolidated summary card, depending on how you configure alert notifications. Each alert message is a webhook notification that includes details such as the cloud type, policy name, and the resource that triggered the alert and the message card indicates the severity with a red (high), yellow (medium) or gray (low) line for easy scanning.

STEP 1 | Set up Microsoft Teams to view alert notifications from Prisma Cloud.

You must create an incoming webhook connector on a new channel or an already existing channel on Microsoft Teams to enable the integration with Prisma Cloud. This webhook channel helps in the consolidation of alert notifications from Prisma Cloud into Microsoft Teams so that your operations team can review and take action on the alerts. To enable this integration, you must have administrative privileges or must contact your Microsoft 365 admin who manages Team settings for your organization.

1. In Microsoft Teams, choose **More options (...)** next to the channel name and then choose **Connectors**.
2. Scroll to **Incoming Webhook**, select **Add** and **Install**.
3. Enter a name for the webhook, and **Create**.
4. Copy the webhook URL to the clipboard and save it, before you click **Done**.

STEP 2 | Set up Microsoft Teams on Prisma Cloud.

1. Log in to Prisma Cloud.
2. Select **Settings** > **Integrations**.
3. Select **+Add New** to create a new integration.
4. Set **Microsoft Teams** as the **Integration Type**.
5. Enter a name for the integration and optionally a description.
6. Paste the **Webhook URL** that you copied earlier.
7. Click **Test** and then **Save**.

On successful integration in the Microsoft teams conversation you receive a test message card with a green line.

STEP 3 | Create an Alert Rule or modify an existing rule to receive alerts in Microsoft Teams. See Send Prisma Cloud Alert Notifications to Third-Party Tools.

The message card includes information on the policy rules and the resource names that have violated the policy, and it includes a direct link with the relevant filters to access Prisma Cloud and view the alert or scheduled notification summary directly in the app.

© 2019 Palo Alto Networks, Inc.

Prisma Cloud Integrations—Supported Capabilities

The following table provides the details of features supported on each integration on Prisma Cloud.

Integrati	Integratio Method	User Attributio	Notificati Template	Alert Notificatio Delay	Status Check	State change Notificatio	Alert Notification Grouping	Frequency of Alert Notification
AWS Guard Duty	Pull							
AWS Inspector	Pull							
AWS Security Hub	Push				Supported	Supported		
Amazon SQS	Push	Supported		Supported	Supported			
Email	Push			Supported			Supported	Supported
Google Cloud SCC	Push				Supported	Supported		
Jira	Push	Supported	Supported	Supported	Supported			
Microsift Teams	Push			Supported	Supported		Supported	Supported
PagerDuty	Push					Supported		
ServiceNow	Push		Supported		Supported	Supported		
Slack	Push			Supported	Supported		Supported	Supported
Splunk	Push	Supported		Supported	Supported			
Tenable	Pull							
Qualys	Pull							
Webhook	Push	Supported		Supported	Supported		Batch Support	

© 2019 Palo Alto Networks, Inc.