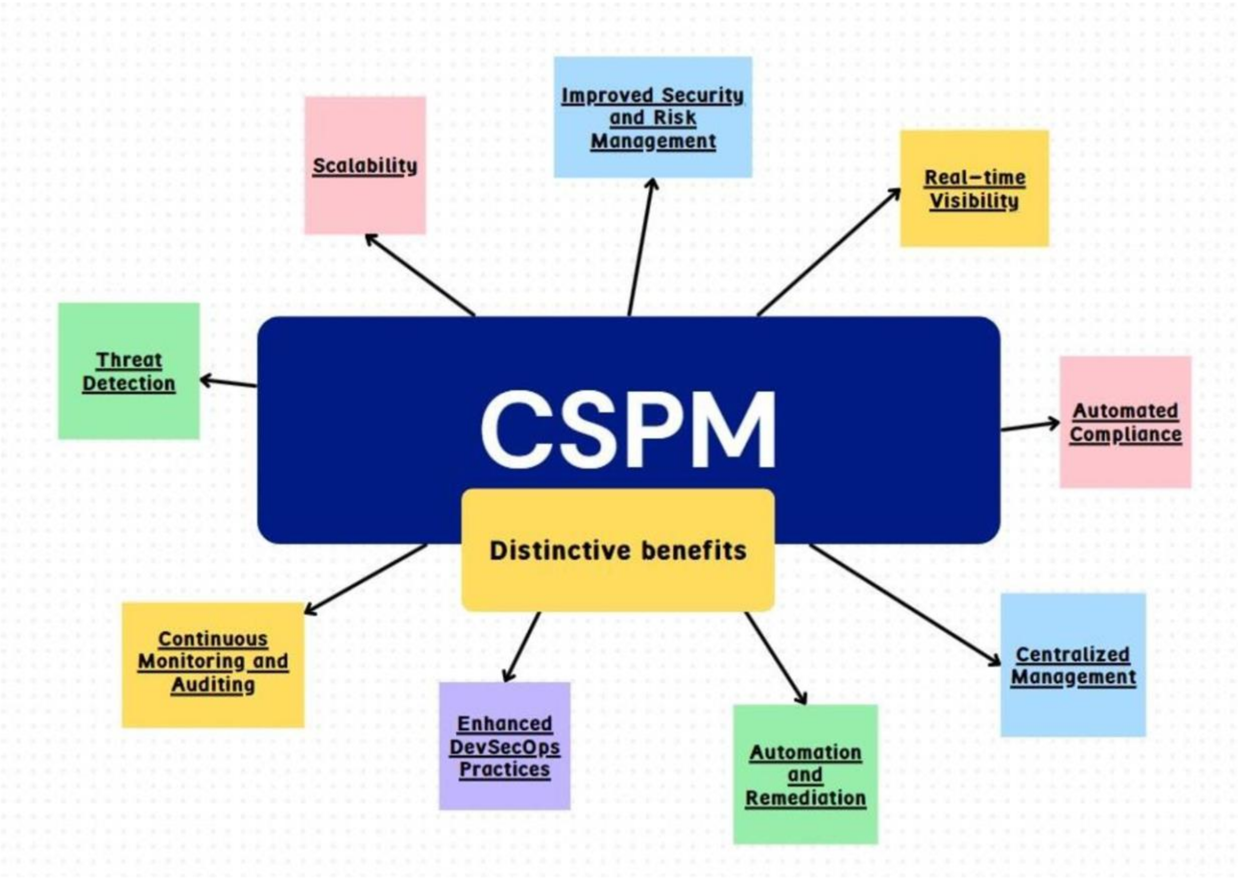
Arij Johri

AWS Runbook
For Cloud Security Posture Management (CSPM) Small

INTRODUCTION

OVERVIEW

Cloud Security Posture Management (CSPM) refers to the practice of continuously monitoring and managing the security posture of cloud resources and services within an organization's cloud infrastructure. The main goal of CSPM is to identify and address misconfigurations, security risks, and compliance violations across cloud environments. It helps ensure that cloud resources are set up and maintained in a secure and compliant manner.


CSPM
Distinctive benefits
Scalability
Improved Security and Risk Management
Real-time Visibility
Threat Detection
Automated Compliance
Continuous Monitoring and Auditing
Enhanced DevSecOps Practices
Automation and Remediation
Centralized Management

Let's take a closer look at the benefits outlined in the diagram above:

- **Improved Security and Risk Management**: CSPM tools help organizations identify security gaps and misconfigurations in their cloud environment. By addressing these issues proactively, organizations can significantly reduce the risk of data breaches, unauthorized access, and other security incidents.

- **Real-time Visibility**: CSPM provides real-time visibility into the security status of cloud assets. Security teams can quickly identify potential security issues, unauthorized changes, and potential threats as they arise.

- **Automated Compliance**: CSPM tools can help organizations adhere to various industry standards and compliance regulations by continuously monitoring cloud configurations and policies. They offer automated checks to ensure alignment with best practices and regulatory requirements.

- **Centralized Management**: CSPM platforms offer a centralized dashboard to view and manage the security posture of multiple cloud accounts and services from different cloud providers. This centralization simplifies security management and monitoring across complex cloud infrastructures.

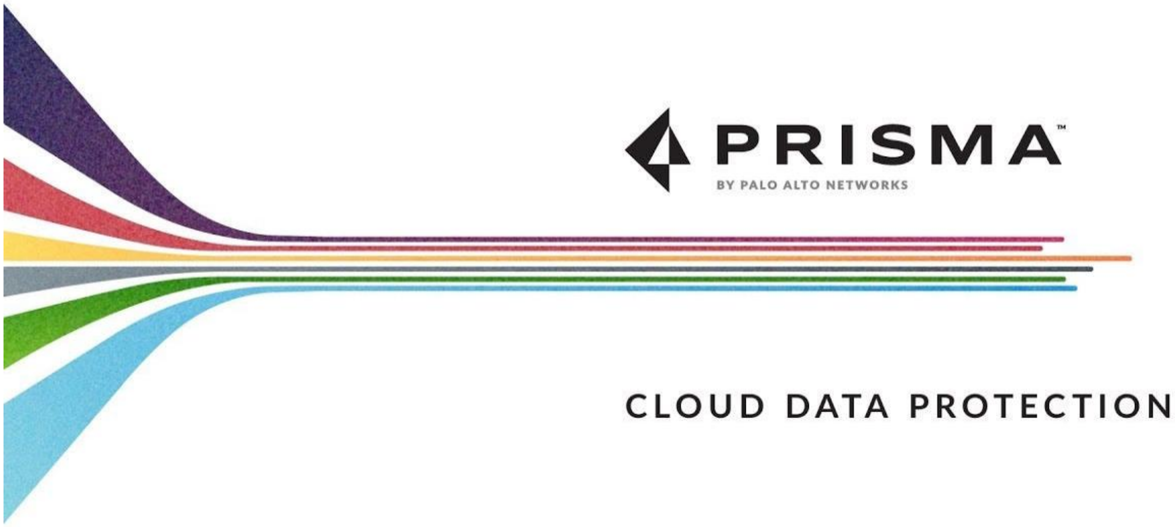
- **Automation and Remediation**: Many CSPM solutions provide automated remediation capabilities. When misconfigurations are detected, these tools can automatically apply fixes or provide actionable steps for remediation, reducing the time required to address security issues.

- **Enhanced DevSecOps Practices**: CSPM integrates security into the DevOps and cloud development lifecycle. By offering real-time feedback and security assessments during development and deployment, organizations can prioritize security from the outset.

- **Continuous Monitoring and Auditing**: CSPM tools continuously monitor cloud environments, making it easier for organizations to perform audits and demonstrate compliance to internal and external stakeholders.

- **Threat Detection**: CSPM platforms can also help detect potential security threats, anomalous behaviors, and suspicious activities within the cloud environment, enabling proactive response to potential security incidents.

- **Scalability**: As cloud environments scale and evolve, CSPM tools can adapt to accommodate new resources and services, ensuring that security policies remain effective across the expanding infrastructure.



ONBOARDING AWS ACCOUNT

STEP 1 - Sign Up and Log In: If you don't already have an account on Prisma Cloud, sign up for one using your email and other required details. After signing up, log in to the Prisma Cloud console using your credentials.

STEP 2 - Add AWS Account in Prisma Cloud: Enter the required details, such as the AWS account number and the External ID in the Prisma Cloud console to add your AWS account to Prisma Cloud. This will establish a connection between your AWS account and Prisma Cloud.

A. Enable Remediation (optional) to grant permissions to remediate misconfigured resources from Infrastructure as Code (IaC) templates. After you enable it, the Prisma Cloud role gets read-write access permissions to your AWS organization to successfully execute remediation commands.

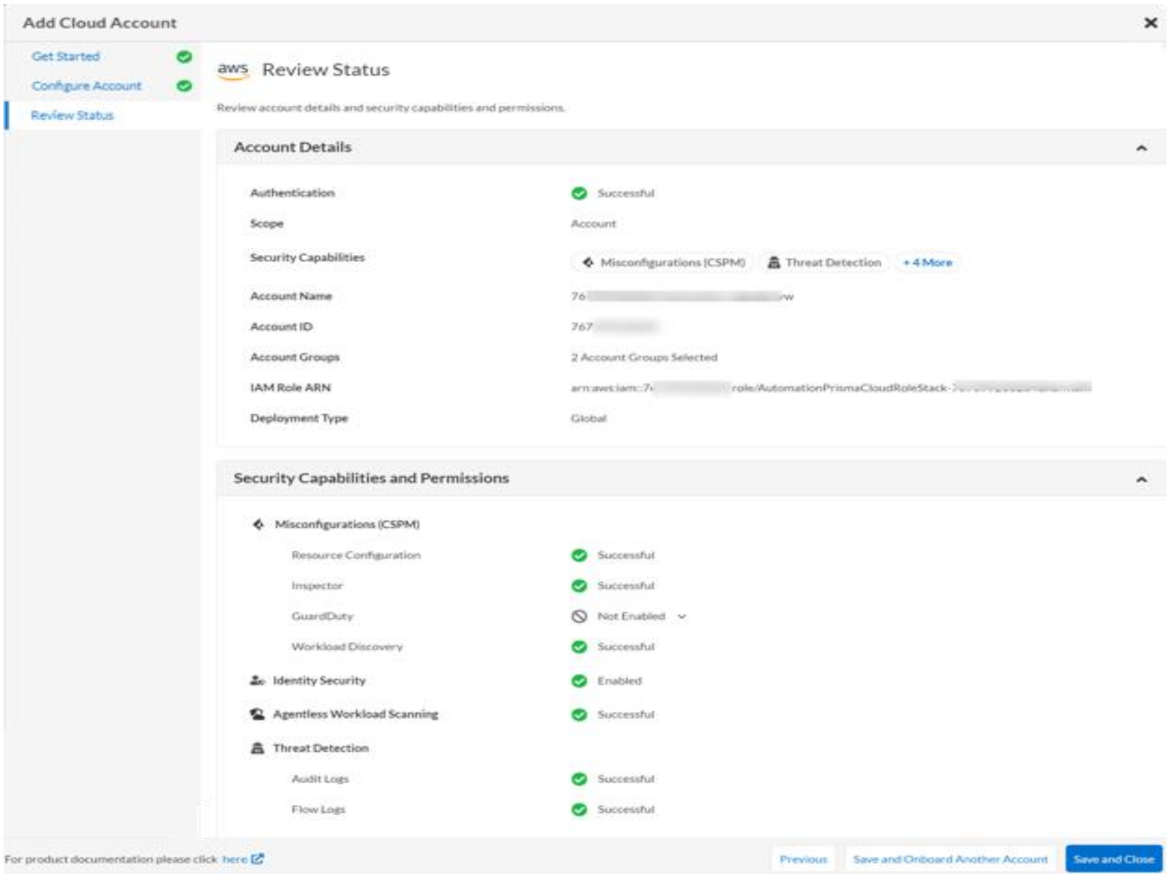
B. Click Create IAM Role only if your role has permissions to log in to your AWS management console to create a stack, else Download IAM Role CFT. Depending on your selection, click View Steps under each to follow the steps to generate **IAM Role ARN**. To automate the process of creating the Prisma Cloud role that is trusted and has the permissions required to retrieve data on your AWS deployment, Prisma Cloud uses a **CFT**. The CFT enables the ingestion of configuration data, **S3 flow logs**, and AWS **CloudTrail logs** (audit events) only, and it does not support the ability to enable VPC flow logs for your AWS account. Make sure that you are already logged in to your AWS management console before you click Create IAM Role. Prisma Cloud creates a dynamic link that opens the Quick create stack page in your AWS management console based on the Security Capabilities and Permissions you selected. The details are uploaded automatically, make sure you complete the onboarding process within 1 hour, else the link will expire, in which case you will have to click Create IAM Role again. If you have installed browser plugins and have pop-ups blocked, first allow pop-up and then click Create IAM Role to continue the process.

C. Once you Download IAM Role CFT, it is valid for 30 days. Even if you close the dialog before completing the onboarding process, you can onboard again within 30 days using the same Account ID and Role ARN created with the previously downloaded CFT.

D. Paste the IAM Role ARN. Select one or more account groups or select Default Account Group. You must assign each cloud account to an account group and create an Alert Rule for run-time checks to associate with that account group to generate alerts when a policy violation occurs.

E. Click Next.

STEP 3 - Verify and Monitor Resources: Once the onboarding process is complete, Prisma Cloud will start scanning and monitoring your AWS resources. You can view the status of your AWS account and the security findings on the Prisma Cloud console.



Add Cloud Account

aws Review Status

Review account details and security capabilities and permissions.

Account Details

Authentication	✓ Successful
Scope	Account
Security Capabilities	Misconfigurations (CSPM) · Threat Detection · + 4 More
Account Name	76[redacted]w
Account ID	767[redacted]
Account Groups	2 Account Groups Selected
IAM Role ARN	arn:aws:iam::7[redacted]role/AutomationPrismaCloudRoleStack-[redacted]
Deployment Type	Global

Security Capabilities and Permissions

Misconfigurations (CSPM)	
Resource Configuration	✓ Successful
Inspector	✓ Successful
GuardDuty	⃠ Not Enabled
Workload Discovery	✓ Successful
Identity Security	✓ Enabled
Agentless Workload Scanning	✓ Successful
Threat Detection	
Audit Logs	✓ Successful
Flow Logs	✓ Successful

For product documentation please click here

Verify the Details of the AWS Account and the status checks for the Security Capabilities you selected while onboarding the account on Prisma Cloud.

A. Ensure that all the security capabilities you selected display a green Successful or Enabled checkmark.

B. For the security capabilities that display a red Checks Failed (icon, click the corresponding drop-down to view the cause of failure. To resolve the issue, see Troubleshoot AWS Onboarding Errors.

C. Click Save and Close to complete onboarding or Save and Onboard Another Account. After you successfully onboard your AWS account on Prisma Cloud, the account is automatically available in Compute and enabled for Workload Discovery and Serverless function scans. For agentless scans, you must complete the configuration to trigger the scan. You can view the newly onboarded AWS account on the Cloud Accounts page.

ALERTS

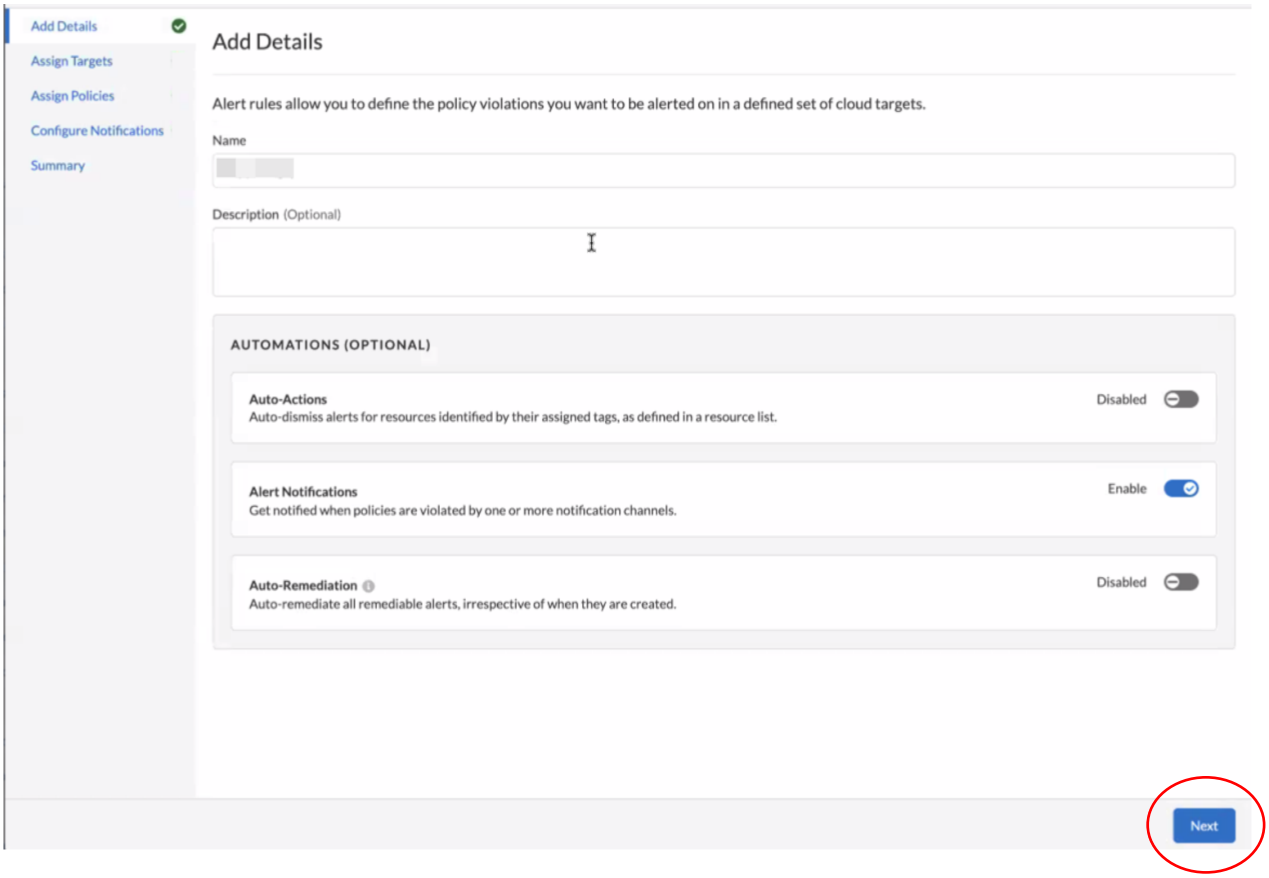
Alert Rules

Alert rules are predefined or custom configurations that trigger notifications or alerts when specific security events, vulnerabilities, or compliance violations are detected within the cloud environment. These rules help security teams quickly identify and respond to potential threats or issues, enhancing the overall security posture of the cloud infrastructure.

How To Create Alert Rules?

STEP 1 - Alerts > Alert Rules and Add Alert Rule

STEP 2 - In Add Details, enter a Name for the alert rule and, optionally a Description to communicate the purpose of the rule.
You can enable the optional **Auto-Action, Alert Notification and Auto-Remediation** settings up front. If you enable any of these options they are displayed as additional steps in the alert rule creation process, for example, if you enable **Alert Notifications**, the **Configuration Notification** step is displayed.
After Completing these click **Next**



Add Details

Alert rules allow you to define the policy violations you want to be alerted on in a defined set of cloud targets.

Name

[redacted]

Description (Optional)

AUTOMATIONS (OPTIONAL)

Auto-Actions — Disabled

Auto-dismiss alerts for resources identified by their assigned tags, as defined in a resource list.

Alert Notifications — Enable

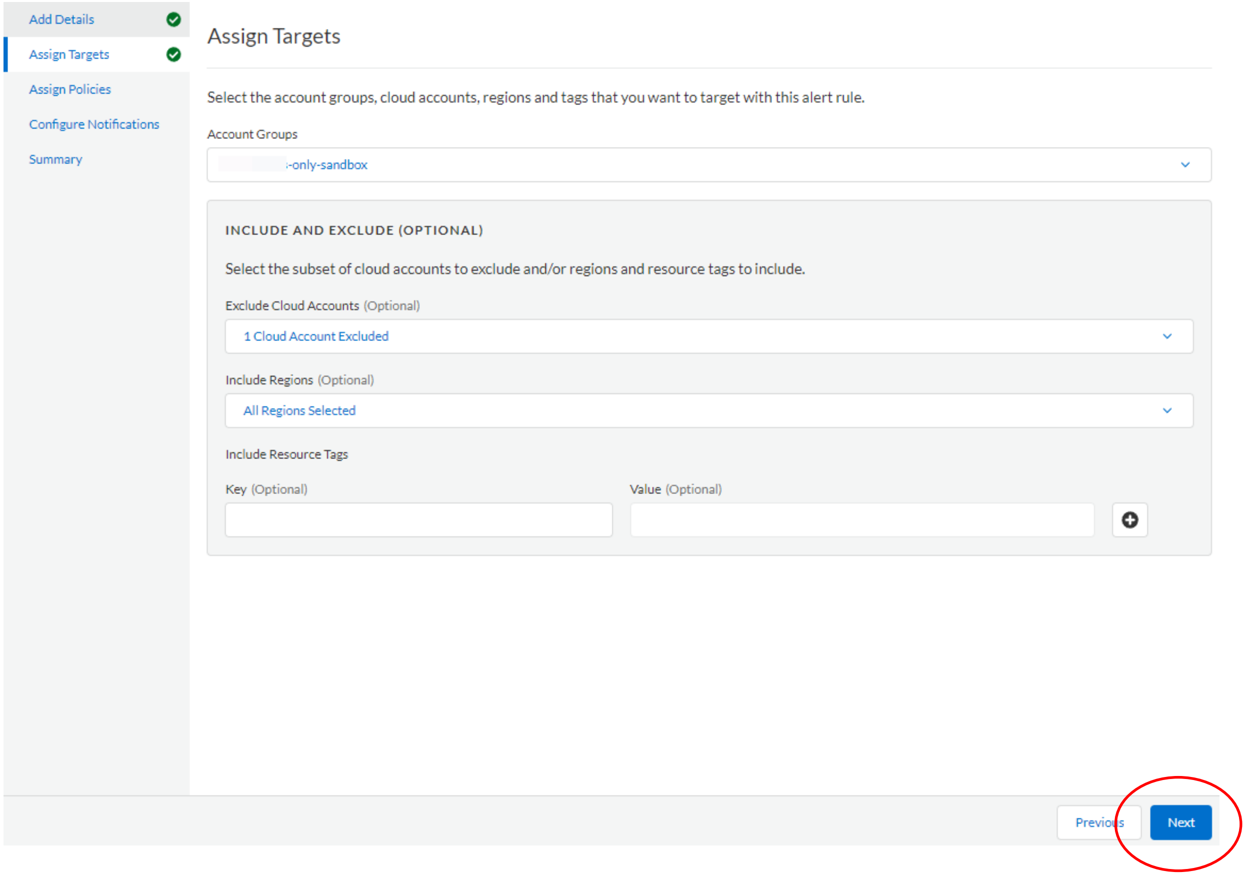
Get notified when policies are violated by one or more notification channels.

Auto-Remediation — Disabled

Auto-remediate all remediable alerts, irrespective of when they are created.

Step 3 - Assign Targets to add more granularity for which cloud resources trigger Alerts for this Alert Rule, and then provide more criteria.

- **A.** Select the Account Groups to which you want this alert rule to apply.
- **B.** Exclude Cloud Accounts and Regions from your selected Account Group—If there are some cloud accounts and regions in the selected account groups for which you do not want to trigger alerts, select the accounts and regions from the list.
- **C.** Select Include Tag Resource Lists to easily manage or identify the type of your resources—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. Tags apply only to Config and Network policies. When you add multiple resource tags, it uses the Boolean logical OR operator.
- **D.** After defining the target cloud resources, click Next.



Assign Targets

Select the account groups, cloud accounts, regions and tags that you want to target with this alert rule.

Account Groups: -only-sandbox

INCLUDE AND EXCLUDE (OPTIONAL)

Select the subset of cloud accounts to exclude and/or regions and resource tags to include.

Exclude Cloud Accounts (Optional): 1 Cloud Account Excluded

Include Regions (Optional): All Regions Selected

Include Resource Tags

Key (Optional)

Value (Optional)

ALERT REPORTS

In Prisma Cloud, alert reports provide a concise summary of security alerts and notifications generated by the system. These reports offer a clear overview of security incidents, misconfigurations, policy violations, and other potential threats detected within the cloud environment. Security teams can use alert reports to quickly assess the nature and severity of alerts, prioritize response actions, and track the status of remediation efforts effectively.

1. CLOUD ASSESSMENT REPORT

The Cloud Assessment Report is a detailed assessment of an organization's cloud environment, identifying potential security risks, misconfigurations, compliance issues, and vulnerabilities present in their cloud infrastructure.

The report is generated based on continuous monitoring and analysis of the cloud resources and services across various cloud platforms like AWS, Azure, and GCP. It provides insights into the security posture of the entire cloud environment, helping organizations understand their risk exposure and take necessary steps to improve security and compliance.

The Cloud Assessment Report typically includes the following information:

- **Security Posture**: An overview of the overall security posture of the cloud environment, highlighting areas that need attention.

- **Misconfigurations**: Detailed information about any misconfigurations found in cloud resources, such as exposed storage buckets, open security groups, or insecure access controls.

- **Compliance Violations:** Information about any violations of regulatory or industry compliance standards.

- **Threat Detection:** Details about any security threats, anomalies, or suspicious activities identified within the cloud environment.

- **Remediation Recommendations:** Actionable steps and recommendations to address the identified security issues and vulnerabilities.

- **Trends and Historical Data:** Historical data and trends to understand the security posture over time and track improvements.

2. DETAILED BUSINESS REPORT

The Detailed Business Report aims to bridge the gap between technical security data and business context, enabling business leaders to understand the impact of cloud security on their organization's

operations, compliance, and overall risk posture.

Key aspects of the Detailed Business Report may include:

1. **Executive Summary**: A high-level summary of the cloud security posture, highlighting critical risks and notable achievements in the cloud environment.

2. **Risk Overview**: An overview of the security risks and compliance posture of the organization's cloud infrastructure, providing an easy-to-understand risk score or rating.

3. **Compliance Status**: Information about the organization's adherence to relevant compliance standards and regulations, indicating any potential compliance violations.

4. **Trends and Historical Data**: Historical data and trends related to the organization's cloud security performance over time, helping business leaders track improvements or deteriorations.

5. **Security Investment Impact**: Insights into the effectiveness of security investments made by the organization and their impact on reducing risks and improving security.

6. **Remediation Progress**: Information about the progress made in remediating security issues and vulnerabilities identified in the cloud environment.

7. **Cost and Budget Implications**: Data on the cost implications of cloud security measures and how they align with the organization's budget.

8. **Business Impact Analysis**: An assessment of how security incidents or misconfigurations could impact business operations, reputation, and customer trust.

How to Investigate Alerts?

1. Go to Alert Overview tab.
2. Reset Filters
3. Add Time Range Filter and set it to All Time
4. Add Alert Status filter to open
5. Add Policy Type select the policy the user wants to investigate
6. Select Alert
7. Click on Alert ID and Investigate

Alerts of low severity can be snoozed for a set time period and if some alerts are not important at all they can be dismissed however they can be restored but it must be done manually by the user.

COMPLIANCE

Compliance Reports

Compliance reports in Prisma Cloud are documents that provide insights into an organization's adherence to various industry standards and regulatory requirements. These reports help assess the compliance posture of cloud resources and services within the organization's cloud environment.

How To Create a Compliance Report?

Creating compliance reports in Prisma Cloud is a straightforward process:

1. **Access the Compliance Section**: Navigate to the "Compliance" or "Compliance Reports" section in the Prisma Cloud console.

2. **Select Compliance Framework**: Choose the specific compliance framework or regulation for which you want to generate the report. Prisma Cloud supports various compliance standards, such as PCI DSS, HIPAA, GDPR, CIS Benchmark, and more.
3. **Define Scope**: Specify the scope of the compliance assessment. This might include selecting specific cloud accounts, regions, or resource types to include in the report.

4. **Generate Report**: Click on the "Generate Report" or "Create Report" button to initiate the report generation process.

How to Create a custom Compliance Standard?

Prisma Cloud allows users to create custom compliance standards to tailor the assessment of their cloud environment based on specific internal policies or unique security requirements. Here's a brief overview of how to create a custom compliance standard in Prisma Cloud:

1. **Access the Compliance Section**: Navigate to the "Compliance" or "Compliance Standards" section in the Prisma Cloud console.

2. **Select "Create Custom Standard"**: Look for an option to create a custom compliance standard. Click on "Create Custom Standard" or a similar button.

3. **Define the Standard**: Provide a name and description for your custom compliance standard. This should reflect the purpose and scope of the standard you are creating.

4. **Add Controls**: Define specific controls or requirements that must be met for compliance with your custom standard. These controls can be based on internal policies, security best practices, or any other relevant criteria.

5. **Set Parameters**: Configure the parameters for each control. This might include specifying specific resource types, regions, or other attributes for evaluation.

6. **Map to Policies or Regulations**: Optionally, you can map your custom controls to specific policies or regulations, aligning them with existing compliance frameworks for easier management.

Save the Custom Standard: Once you have defined all the controls and parameters, save the custom compliance standard.

POLICY

In Prisma Cloud, policies are a set of rules or configurations that help organizations define and enforce security and compliance standards within their cloud environment. These policies enable administrators to monitor, detect, and prevent potential security risks, misconfigurations, and policy violations in cloud resources and services.

Policy Types in Prisma Cloud are:

- Config Policy
- IAM Policy
- Network Policy
- Data Policy

How to Create a Custom Policy in Prisma Cloud?

- **Access the Policies Section**: Log in to the Prisma Cloud console and navigate to the "Policies" or "Policy Management" section.

- **Create a New Policy**: Look for an option to create a new policy and click on it.

- **Select Policy Type**: Choose the appropriate policy type that aligns with the focus of your custom policy. For example, it could be a compliance policy, network security policy, data security policy, or any other relevant type.

- **Define Policy Rules**: Specify the rules or conditions that the custom policy will evaluate. You can set conditions based on cloud resource attributes, network settings, compliance requirements, or other criteria that reflect your organization's security needs.

- **Set Parameters**: Configure the parameters for each rule to define the desired behavior or outcome when evaluating resources against the policy.

- **Test and Validate**: If possible, test the custom policy in a non-production environment to ensure it functions as expected and generates the desired results.

- **Save the Custom Policy**: Once you have defined all the rules and parameters, save the custom policy.

RBAC Configuration

Step 1 - Access Prisma Cloud Console:
Log in to the Prisma Cloud Console with an account that has administrative privileges.

Step 2 - Create Custom Roles:
Prisma Cloud allows you to create custom roles to define specific access permissions. To create custom roles:

a. Navigate to "Settings" in the Prisma Cloud Console.

b. Under "Access Management," select "Roles."

c. Click on the "Create Role" button.

d. Give your custom role a name and description. Define the permissions for the role by selecting the appropriate policies or creating custom policies. You can choose from predefined policies or create your own.

e. Save the custom role.

Step 3 - Assign Roles to Users or Groups:

Once you have created custom roles, you can assign them to individual users or groups. To assign roles:

a. In the Prisma Cloud Console, go to "Access Management" > "Users" or "Groups," depending on whether you want to assign roles to individual users or groups.

b. Select the user or group to which you want to assign a role.

c. Edit the user or group details to assign one or more roles. You can assign multiple roles to a user or group.

d. Save the changes.

Step 4 - Review and Refine Policies:

It's essential to regularly review and refine the policies associated with custom roles. Ensure that policies align with your organization's security and access control requirements.

Testing and Verification:
After configuring RBAC, it's crucial to test user access to AWS resources and actions through Prisma Cloud. Make sure users and groups have the appropriate permissions and can perform the necessary tasks.

Monitoring and Auditing:
Continuously monitor user activities and access permissions within Prisma Cloud. Prisma Cloud provides auditing and monitoring features that allow you to track user actions and security events.

Maintenance and Updates:
As your AWS environment evolves or your organization's access control requirements change, update and maintain your RBAC configuration in Prisma Cloud accordingly. This may involve modifying roles, policies, or role assignments.

Documentation and Training:
Document your RBAC configuration, including roles, policies, and assignments. Provide training to users and administrators on how RBAC works within Prisma Cloud to ensure efficient and secure access management.

Security Best Practices:
Adhere to security best practices when configuring RBAC. Enforce the principle of least privilege, regularly review access permissions, and follow secure authentication practices.

SSO CONFIGURATION

Step 1 - Prepare Your Prisma Cloud Console:

a. Log in to the Prisma Cloud Console as an administrator.

b. Click on "Settings" and then "Single Sign-On."

c. Click "SAML Configuration" to start configuring SAML SSO.

Step 2 - Configure Your Identity Provider (IdP):

a. You need to configure your chosen IdP (e.g., Okta, Azure AD) to work with Prisma Cloud. This generally involves creating a new SAML application or integration in your IdP.

b. Configuring the IdP with the following information:
ACS (Assertion Consumer Service) URL: This is provided in the Prisma Cloud SAML configuration.
Entity ID: This is typically the Prisma Cloud Console URL.
Attribute mappings (e.g., email, username) from your IdP to Prisma Cloud.

c. Obtain the IdP's metadata XML file.

Step 3 - Configure Prisma Cloud:

In the Prisma Cloud Console:
a. Enter the SAML SSO Configuration settings:
Issuer: This is usually the entity ID from your IdP.
SAML SSO URL: This is typically the IdP's SAML endpoint.
SAML IdP Certificate: Upload the IdP's certificate, often available in the IdP's metadata XML.

b. Configure SAML Attributes:
Map the IdP attributes to Prisma Cloud attributes. For example, map the IdP email attribute to the Prisma Cloud email attribute.

c. Save the SAML configuration.

Step 4 - Test the SSO Configuration:

To ensure that SSO is working correctly, perform the following steps:

a. Log out of the Prisma Cloud Console if you are still logged in.

b. Go to the Prisma Cloud Console URL.

c. You should be redirected to your IdP's login page. Log in with your IdP credentials.

d. Once authenticated, you should be redirected back to the Prisma Cloud Console.

Step - 5 Enable SSO:

After successful testing, enable SSO in Prisma Cloud:

a. In the Prisma Cloud Console, go to "Settings" > "Single Sign-On."

b. Toggle the "Enable SAML Single Sign-On" option to enable SSO.

Step 6 (Optional) - Role Mapping:

You can configure role mapping in Prisma Cloud to map IdP roles or groups to Prisma Cloud roles. This ensures that users get appropriate permissions in Prisma Cloud.

Step 7 - Monitor and Maintain:

Regularly monitor SSO usage and ensure that user provisioning and de-provisioning are managed appropriately through your IdP.

INTEGRATION WITH AMAZON GUARDDUTY

Amazon GuardDuty is a continuous security monitoring service that analyzes and processes Virtual Private Cloud (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 GuardDuty and extends its threat visualization capabilities. Prisma Cloud starts ingesting GuardDuty data, correlates it with the other information that Prisma Cloud already collects, and presents contextualized and actionable information through the Prisma Cloud app.

Step 1. Enable Amazon GuardDuty on your AWS instances.

Step 2. Enable read-access permissions to Amazon GuardDuty on the IAM Role policy.

The Prisma Cloud IAM Role policy you use 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, the Prisma Cloud IAM Role policy already has the permissions required for Amazon GuardDuty.

After Prisma Cloud has access to the Amazon GuardDuty findings, use the following RQL queries for visibility into the information collected from Amazon GuardDuty.

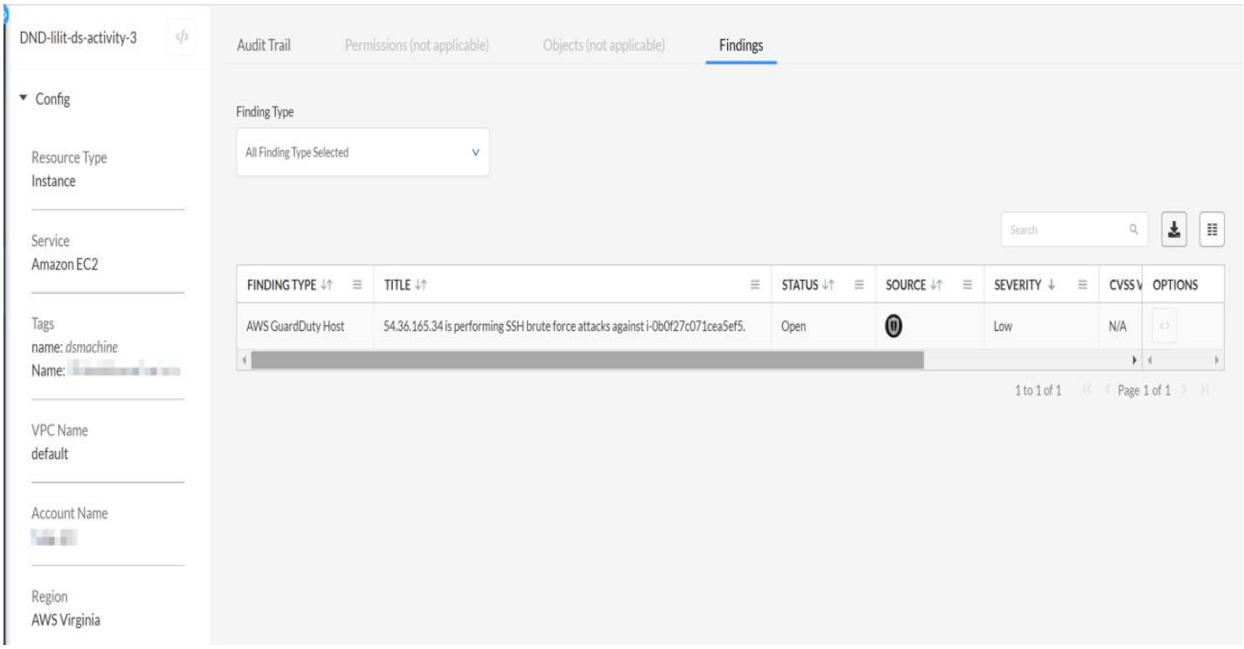
Config Query:

```
config from cloud.resource where cloud.type = 'aws' AND finding.type = 'AWS GuardDuty Host'
```

Network Query:

```
network from vpc.flow_record where dest.resource IN (resource where finding.type =
'AWS GuardDuty Host')
```

Step 3. Click on the resource to see the **Audit Trail.**



DND-lilit-ds-activity-3

Config

Resource Type
Instance

Service
Amazon EC2

Tags
name: *dsmachine*
Name: [redacted]

VPC Name
default

Account Name
[redacted]

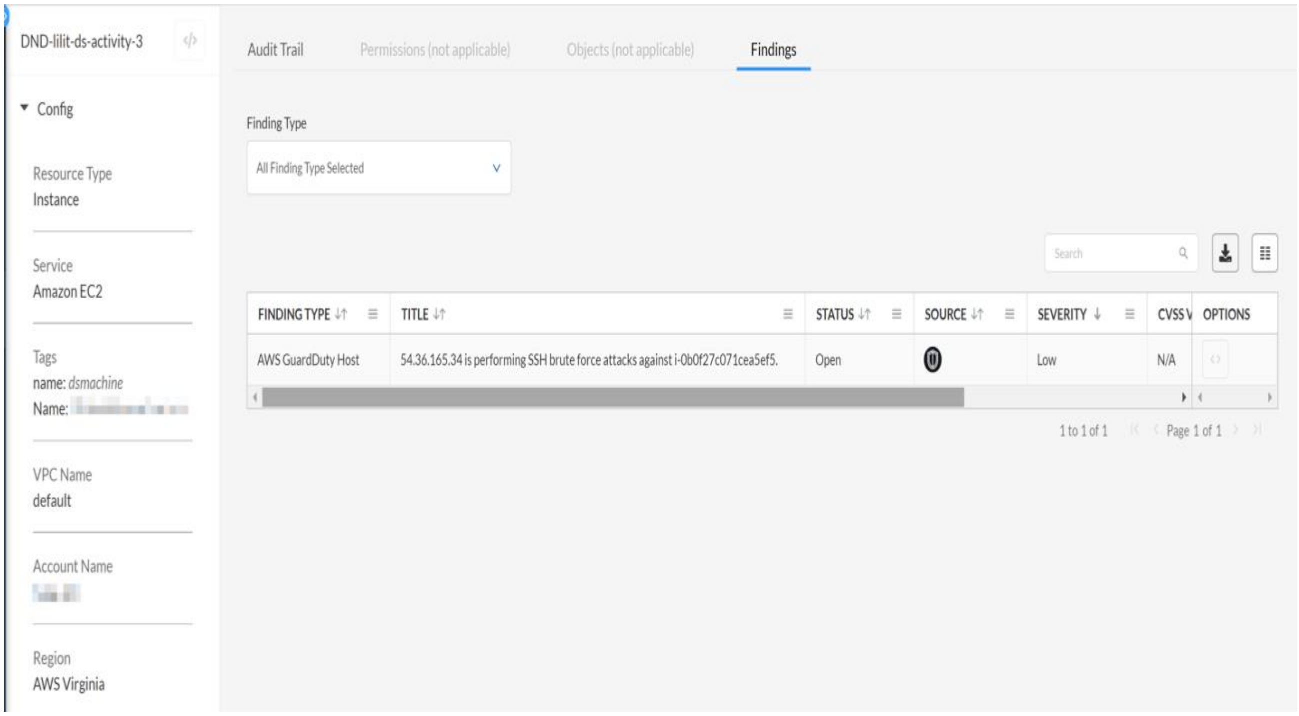
Region
AWS Virginia

Finding Type: All Finding Type Selected

FINDING TYPE	TITLE	STATUS	SOURCE	SEVERITY	CVSS V	OPTIONS
AWS GuardDuty Host	54.36.165.34 is performing SSH brute force attacks against i-0b0f27c071cea5ef5.	Open	ⓤ	Low	N/A	‹›

1 to 1 of 1 Page 1 of 1

Step 4. Click **Findings** for information related to vulnerabilities. Select **AWS GuardDuty Host** or **AWS GuardDuty IAM** in the filter to view vulnerabilities detected by AWS GuardDuty.



DND-lilit-ds-activity-3

Config

Resource Type
Instance

Service
Amazon EC2

Tags
name: *dsmachine*
Name: [redacted]

VPC Name
default

Account Name
[redacted]

Region
AWS Virginia

Finding Type: All Finding Type Selected

FINDING TYPE	TITLE	STATUS	SOURCE	SEVERITY	CVSS V	OPTIONS
AWS GuardDuty Host	54.36.165.34 is performing SSH brute force attacks against i-0b0f27c071cea5ef5.	Open	ⓤ	Low	N/A	‹›

1 to 1 of 1 Page 1 of 1

```
config from cloud.resource where api.name = 'aws-iam-list-access-keys' AND finding.source = 'AWS GuardDuty'
```

Step 5. Enable Amazon Inspector on your EC2 instances. To set up Amazon Inspector and Enable read-access permissions to Amazon Inspector on the IAM Role policy.

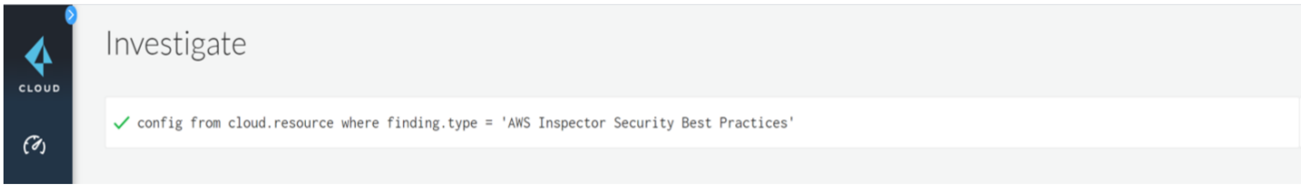
The Prisma Cloud IAM Role policy that you use to onboard your AWS setup needs these permissions:

inspector:Describe*,

inspector:List*

If you used the CFT templates to onboard your AWS account, the Prisma Cloud IAM Role policy already has the permissions required for Amazon Inspector.

After the Prisma Cloud service begins ingesting Amazon Inspector data, you can use the following RQL queries for visibility into the host vulnerability information collected from it.

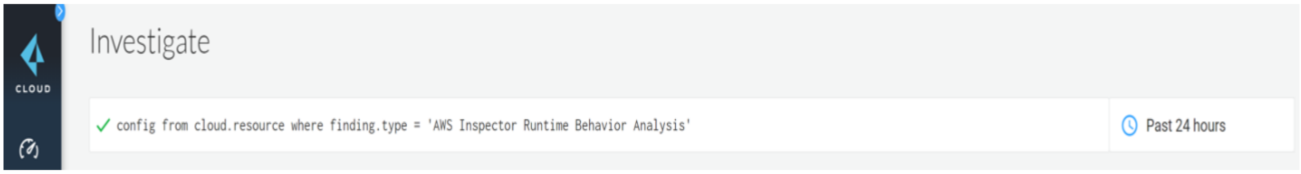


```
✓ config from cloud.resource where finding.type = 'AWS Inspector Security Best Practices'
```

Config queries:

config from cloud.resource where finding.type = 'AWS Inspector Runtime Behavior Analysis'

config from cloud.resource where finding.type = 'AWS Inspector Security Best Practices'



```
✓ config from cloud.resource where finding.type = 'AWS Inspector Runtime Behavior Analysis'
```

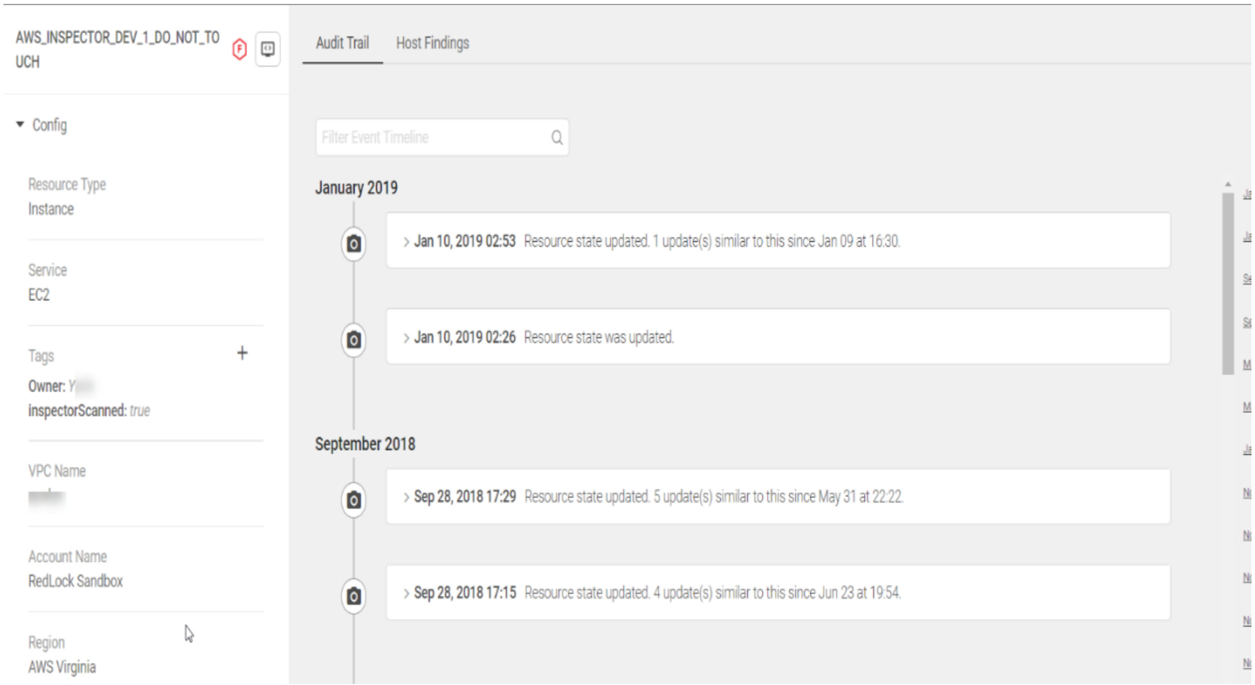
AWS Inspector Runtime Behavior Analysis:
Fetches all resources which are in violation of one or more rules reported by the AWS Runtime Behavior Analysis package.

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 from vpc.flow_record where dest.resource IN (resource where finding.type =
'AWS Inspector Runtime Behavior Analysis')
network from vpc.flow_record where dest.resource IN (resource where finding.type =
'AWS Inspector Security Best Practices')
```

Click on the resource to see an **Audit trail.**



AWS_INSPECTOR_DEV_1_DO_NOT_TOUCH

Resource Type
Instance

Service
EC2

Tags
Owner: Y[redacted]
inspectorScanned: *true*

VPC Name
[redacted]

Account Name
RedLock Sandbox

Region
AWS Virginia

January 2019

> **Jan 10, 2019 02:53** Resource state updated. 1 update(s) similar to this since Jan 09 at 16:30.

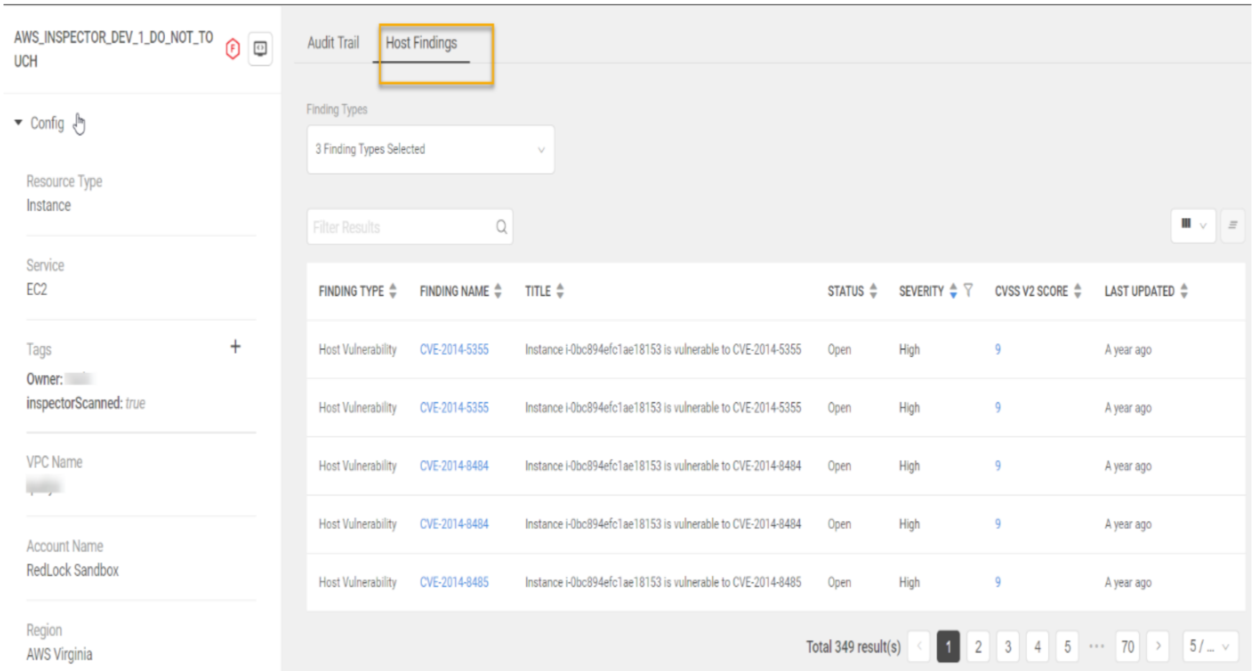
> **Jan 10, 2019 02:26** Resource state was updated.

September 2018

> **Sep 28, 2018 17:29** Resource state updated. 5 update(s) similar to this since May 31 at 22:22.

> **Sep 28, 2018 17:15** Resource state updated. 4 update(s) similar to this since Jun 23 at 19:54.

Click **Host Findings** for information related to vulnerabilities.



Resource Type: Instance

Service: EC2

Tags
Owner: [redacted]
inspectorScanned: *true*

VPC Name: [redacted]

Account Name: RedLock Sandbox

Region: AWS Virginia

Finding Types: 3 Finding Types Selected

FINDING TYPE	FINDING NAME	TITLE	STATUS	SEVERITY	CVSS V2 SCORE	LAST UPDATED
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8485	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8485	Open	High	9	A year ago

Total 349 result(s)

INTEGRATION WITH AMAZON S3

Amazon S3 is widely used for storage and staging data. You can integrate Prisma Cloud with Amazon S3 to get notifications for configuration, audit, and anomaly policy violations.

Using this integration, you can stream the Prisma Cloud alerts to an Amazon S3 bucket or folder. You can also decide how often the notifications should be published to the S3 bucket using **File Roll Up Time.**

Step 1. Configure Amazon S3 to receive Prisma Cloud alerts.

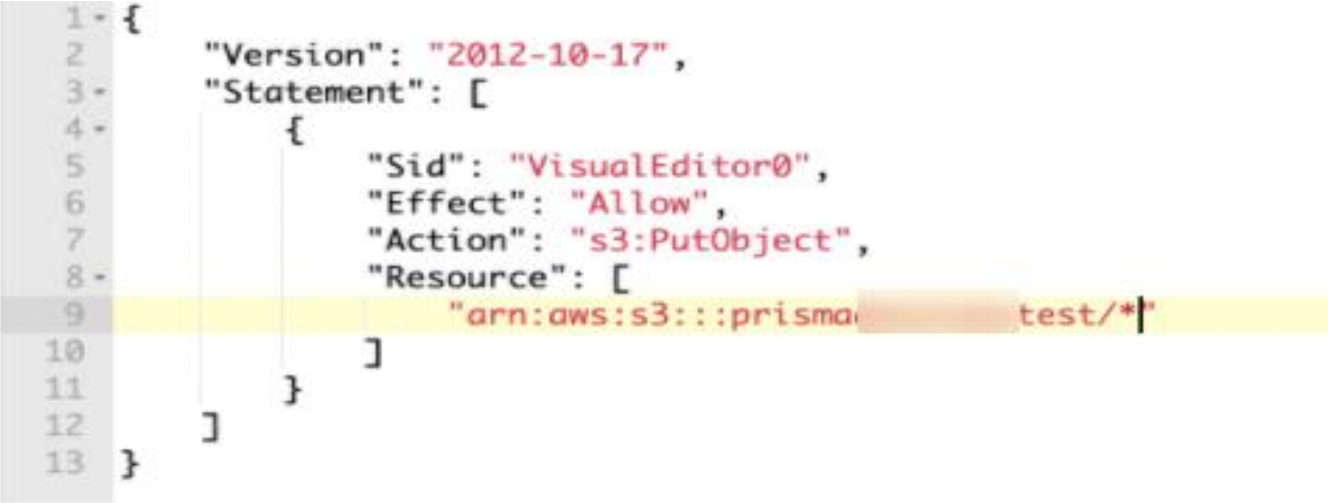
Step 2. Log in to the AWS management console and select S3.

1. Create an S3 bucket in your preferred region.
2. (Optional) Create a folder. If the desired bucket or folder path already exists, you can skip this step.

Step 3. Select IAM and create a role for Prisma Cloud to be able to write notifications to the S3 bucket.

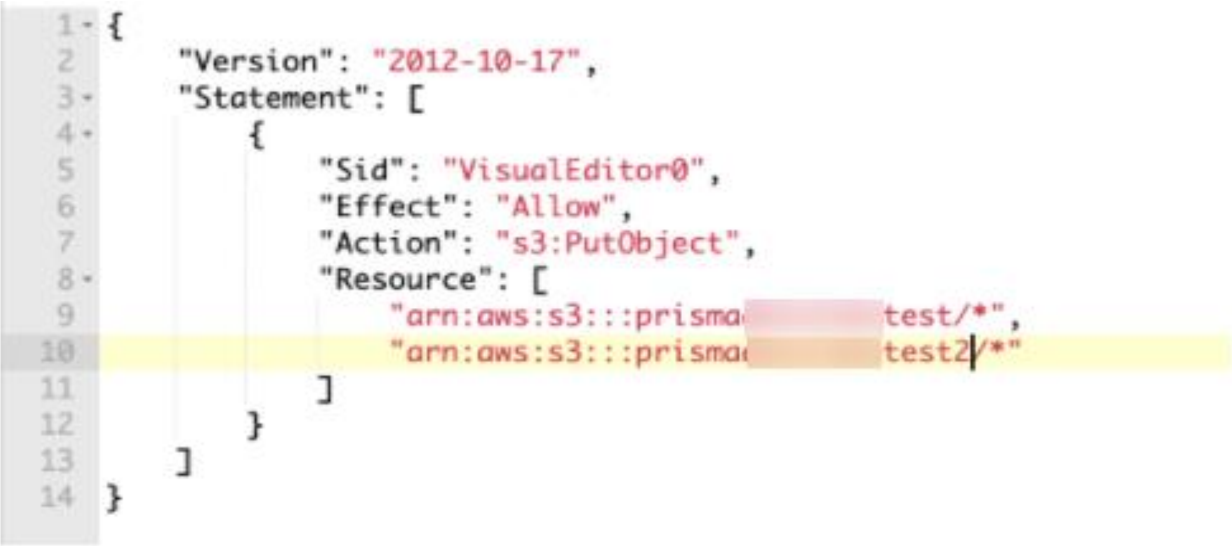
1. Create a new policy with the S3**: PutObject** permission for the bucket you created in

Step 1. The policy document should be similar to:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::prisma[redacted]test/*"
            ]
        }
    ]
}
```

Step 2. To configure multiple S3 integrations with multiple buckets, the policy document should be similar to:

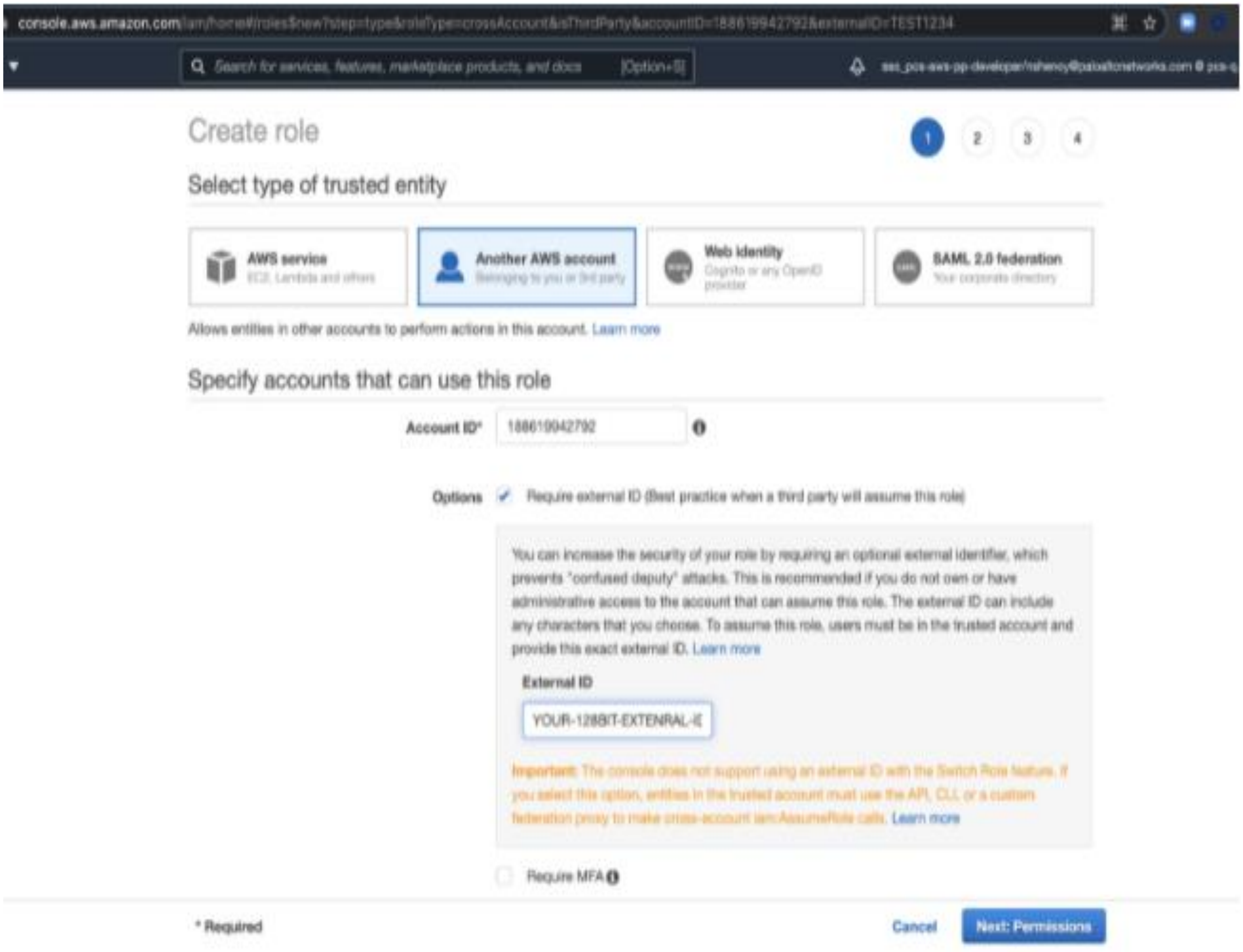


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::prisma[redacted]test/*",
                "arn:aws:s3:::prisma[redacted]test2/*"
            ]
        }
    ]
}
```

Create an IAM role with the following configurations:

- Select type of trusted entity **Another AWS Account.**

- Enter the Account ID* **188619942792**. In case of AWS Gov accounts, enter the Account ID* **342570144056**.
- Configure the External **ID** for IAM role. The External ID associated with the IAM role must be a UUID in a 128-bit format, and not any random string. If you're using the Prisma Cloud web console, click **Generate Token** to generate the External ID while adding the S3 integration. If you're using the Prisma Cloud API, you must manually create the External ID.
-



console.aws.amazon.com/iam/home#/roles$new?step=type&roleType=crossAccount&isThirdParty&accountID=188619942792&externalID=TEST1234

Create role

Select type of trusted entity

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID* 188619942792

Options ☑ Require external ID (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more

External ID: YOUR-128BIT-EXTENRAL-IE

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more

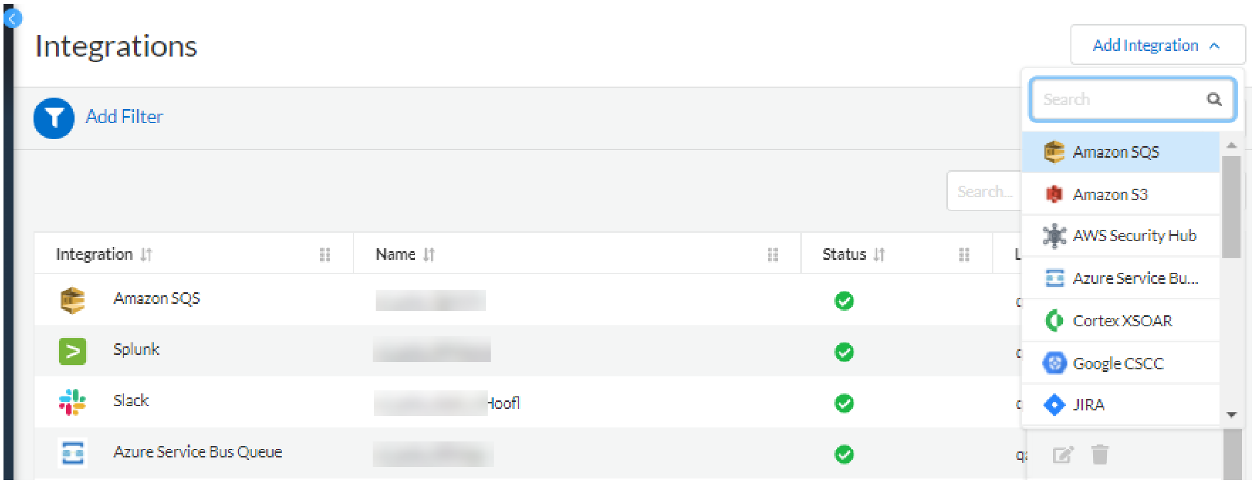
□ Require MFA

* Required

- Select the policy created in Step 2 and follow the steps to configure the IAM role.
- Save.

Set up the Amazon S3 Integration on Prisma Cloud:

- Log in to Prisma Cloud.
- Select **Settings Integrations**.
- **Add Integration Amazon S3**. A modal wizard opens where you can add the S3 integration.



Integration	Name	Status
Amazon SQS	[redacted]	✓
Splunk	[redacted]	✓
Slack	[redacted]	✓
Azure Service Bus Queue	[redacted]	✓

- Enter a **Name** and (optional) **Description.**

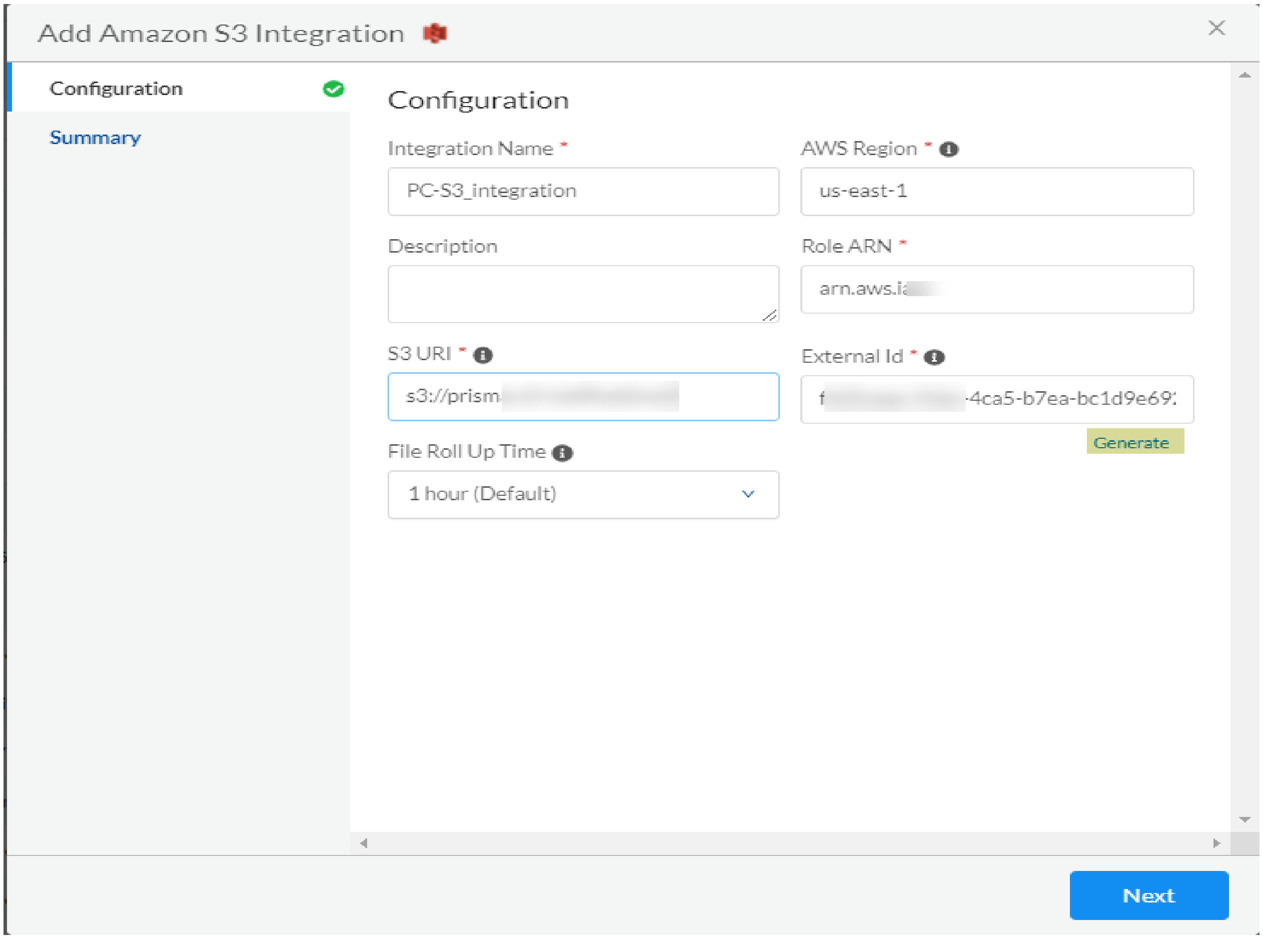
- Enter **S3 URI** for the S3 bucket or folder path from Step 1. The format should be: **s3://bucketname/**or **s3://bucketname/foldername/** .

- Enter the **AWS Region** in which you created the S3 bucket.

- **Generate** the External ID to associate it to the IAM role which is required for Prisma Cloud to be able to write notifications to the S3 bucket.

- Enter the **Role ARN** of the IAM role setup during Step 1.

- Select the **File Roll Up Time** from the drop-down. The default is 1 hour, you can change it to 15 minutes, 30 minutes, or 3 hours.



Add Amazon S3 Integration

Configuration

Integration Name *: PC-S3_integration

AWS Region *: us-east-1

Description:

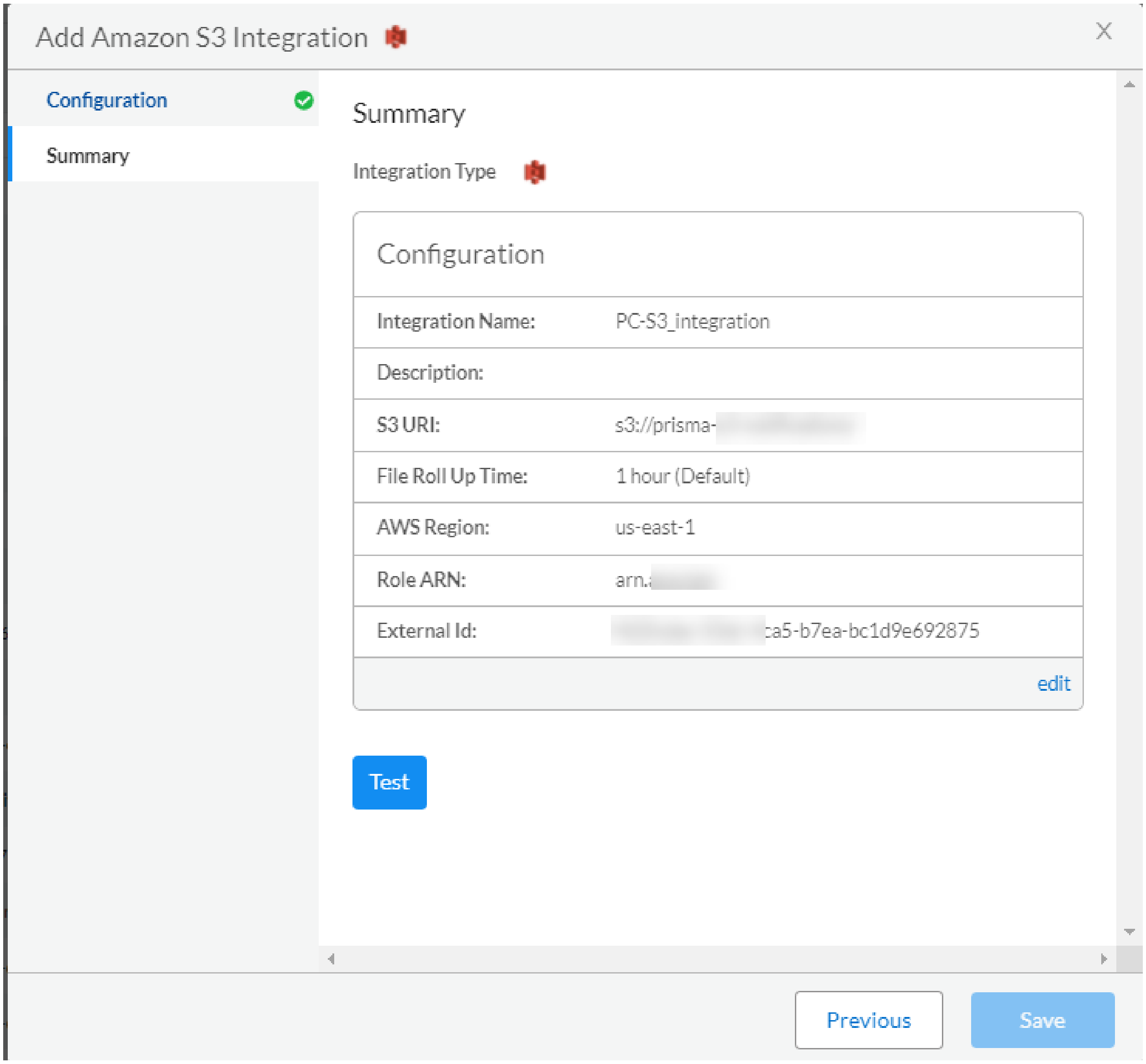
Role ARN *: arn.aws.i[redacted]

S3 URI *: s3://prism[redacted]

External Id *: f[redacted]-4ca5-b7ea-bc1d9e69:

File Roll Up Time: 1 hour (Default)

- **Next**.
- **Test** and **save** the integration.



Add Amazon S3 Integration

Summary

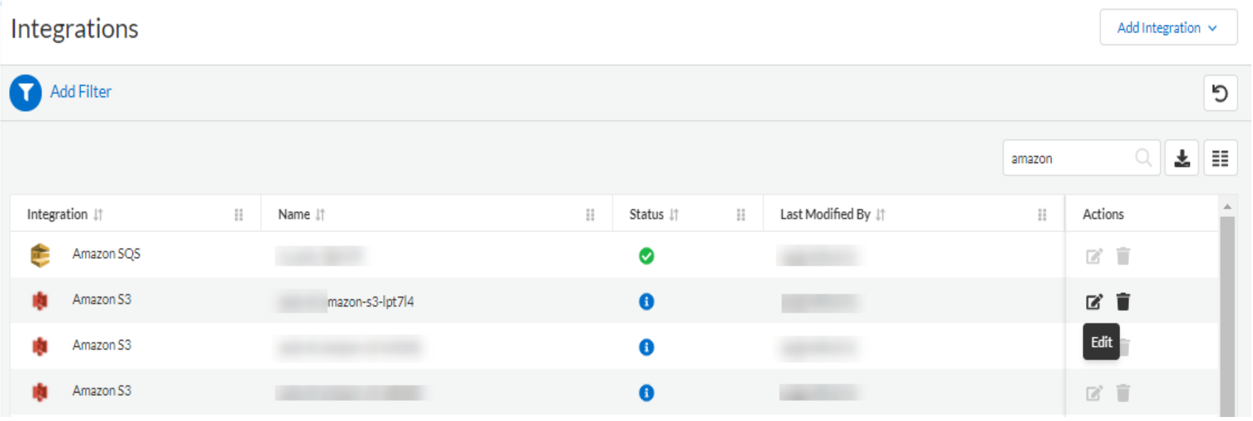
Integration Type

Configuration

Integration Name:	PC-S3_integration
Description:	
S3 URI:	s3://prisma-[redacted]
File Roll Up Time:	1 hour (Default)
AWS Region:	us-east-1
Role ARN:	arn.[redacted]
External Id:	[redacted]ca5-b7ea-bc1d9e692875

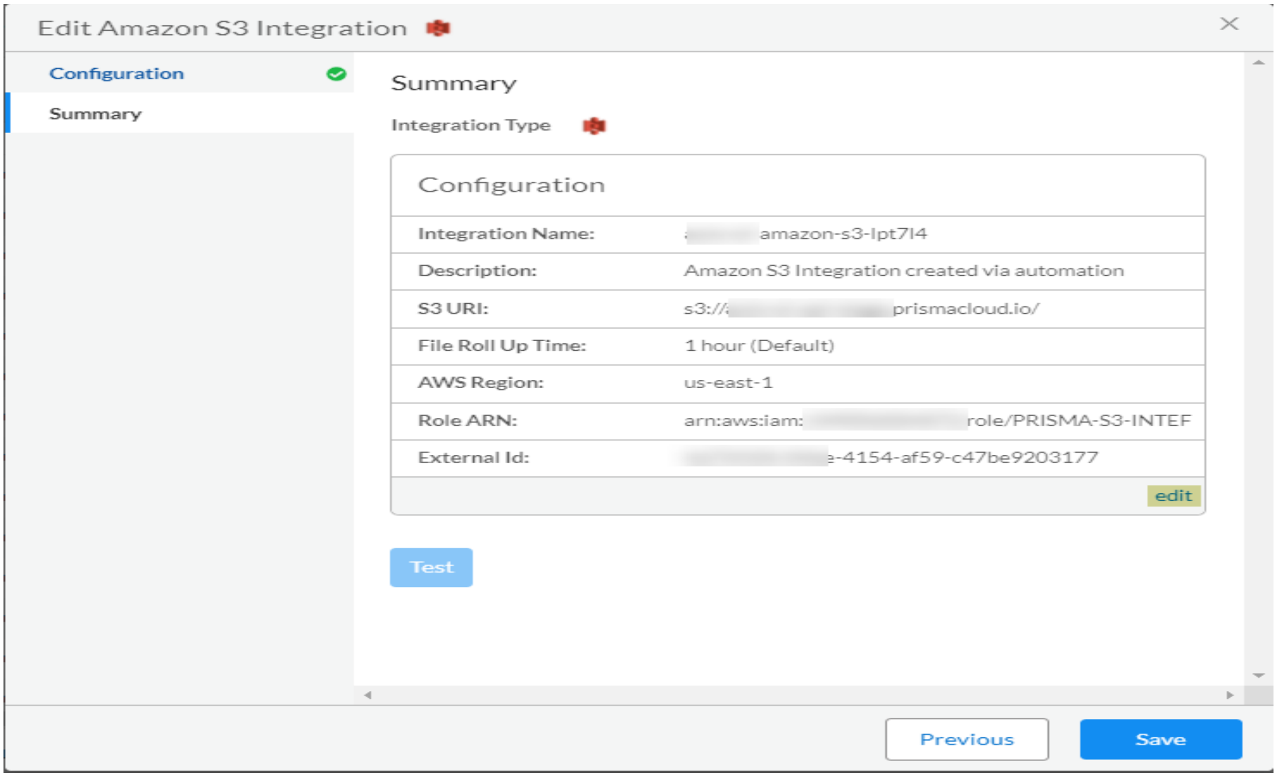
- You should receive a success message and a test file should be created on the specified S3 URI.

- To edit the integration, click the corresponding **Edit** icon. The integration **Summary** page opens.



Integrations

Integration	Name	Status	Last Modified By	Actions
Amazon SQS	[redacted]	✓	[redacted]	
Amazon S3	[redacted]mazon-s3-lpt7l4	ℹ	[redacted]	
Amazon S3	[redacted]	ℹ	[redacted]	Edit
Amazon S3	[redacted]	ℹ	[redacted]	



Edit Amazon S3 Integration

Summary

Integration Type

Configuration

Integration Name:	[redacted]amazon-s3-lpt7l4
Description:	Amazon S3 Integration created via automation
S3 URI:	s3://[redacted]prismacloud.io/
File Roll Up Time:	1 hour (Default)
AWS Region:	us-east-1
Role ARN:	arn:aws:iam:[redacted]role/PRISMA-S3-INTEF
External Id:	[redacted]-4154-af59-c47be9203177

- **Edit** to update the integration as required.
- **Next** to review your edits.
- **Test** and **save** the integration.

Integrate With Amazon Inspector

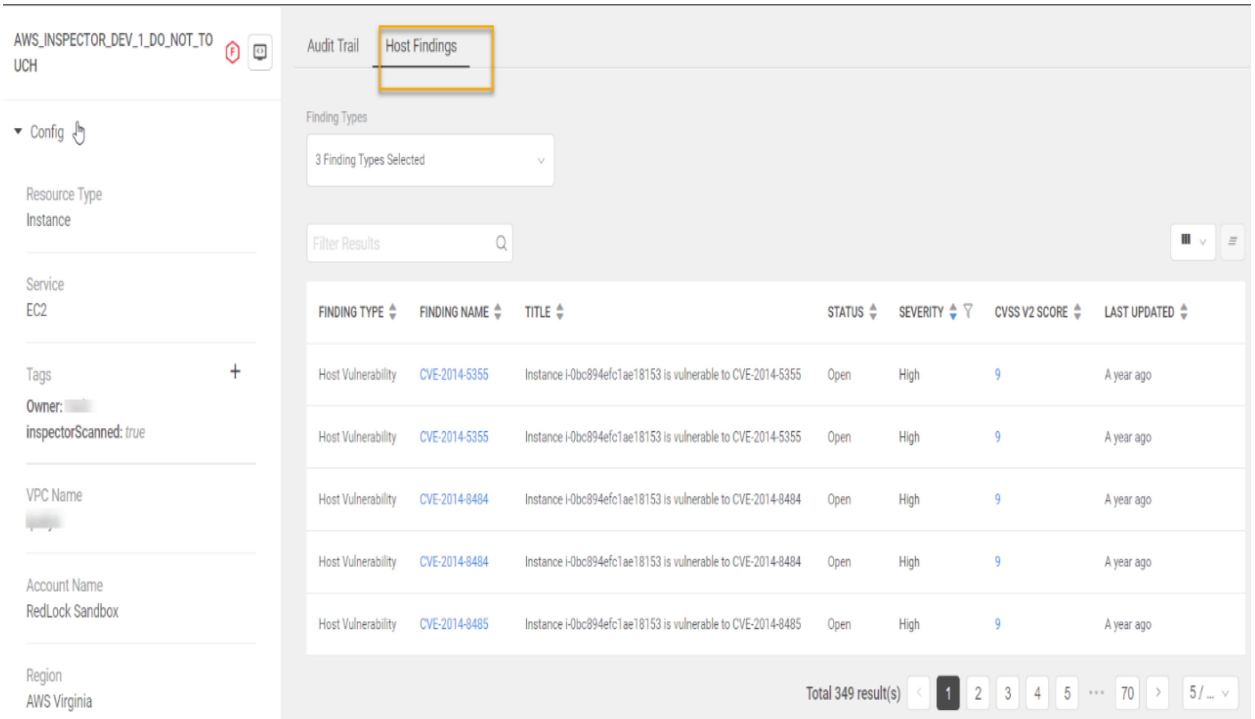
Step 1 - Enable Amazon Inspector on your EC2 instances. To set up Amazon Inspector.

Step 2 - Enable read-access permissions to Amazon Inspector on the IAM Role policy. The Prisma Cloud IAM Role policy that you use to onboard your AWS setup needs these permissions:

```
inspector:Describe*,
inspector:List*
```

If you used the CFT templates to onboard your AWS account, the Prisma Cloud IAM Role policy already has the permissions required for Amazon Inspector.

Step 3 - After the Prisma Cloud service begins ingesting Amazon Inspector data, you can use the following RQL queries for visibility into the host vulnerability information collected from it.



Resource Type
Instance

Service
EC2

Tags
Owner: [redacted]
inspectorScanned: *true*

VPC Name
[redacted]

Account Name
RedLock Sandbox

Region
AWS Virginia

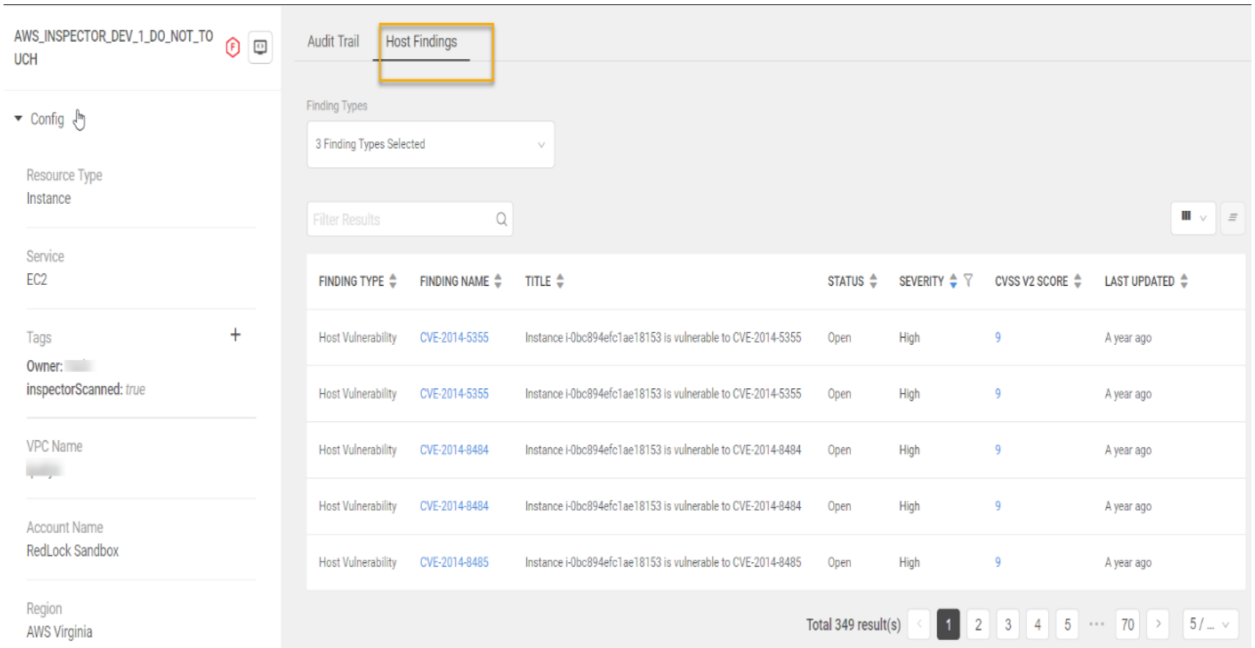
Finding Types
3 Finding Types Selected

FINDING TYPE	FINDING NAME	TITLE	STATUS	SEVERITY	CVSS V2 SCORE	LAST UPDATED
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8485	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8485	Open	High	9	A year ago

Total 349 result(s)

- **Config queries**:

```
config from cloud.resource where finding.type = 'AWS Inspector Runtime Behavior Analysis'
config from cloud.resource where finding.type = 'AWS Inspector Security Best Practices'
```



Resource Type
Instance

Service
EC2

Tags
Owner: [redacted]
inspectorScanned: *true*

VPC Name
[redacted]

Account Name
RedLock Sandbox

Region
AWS Virginia

Finding Types
3 Finding Types Selected

Filter Results

FINDING TYPE	FINDING NAME	TITLE	STATUS	SEVERITY	CVSS V2 SCORE	LAST UPDATED
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8485	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8485	Open	High	9	A year ago

Total 349 result(s)

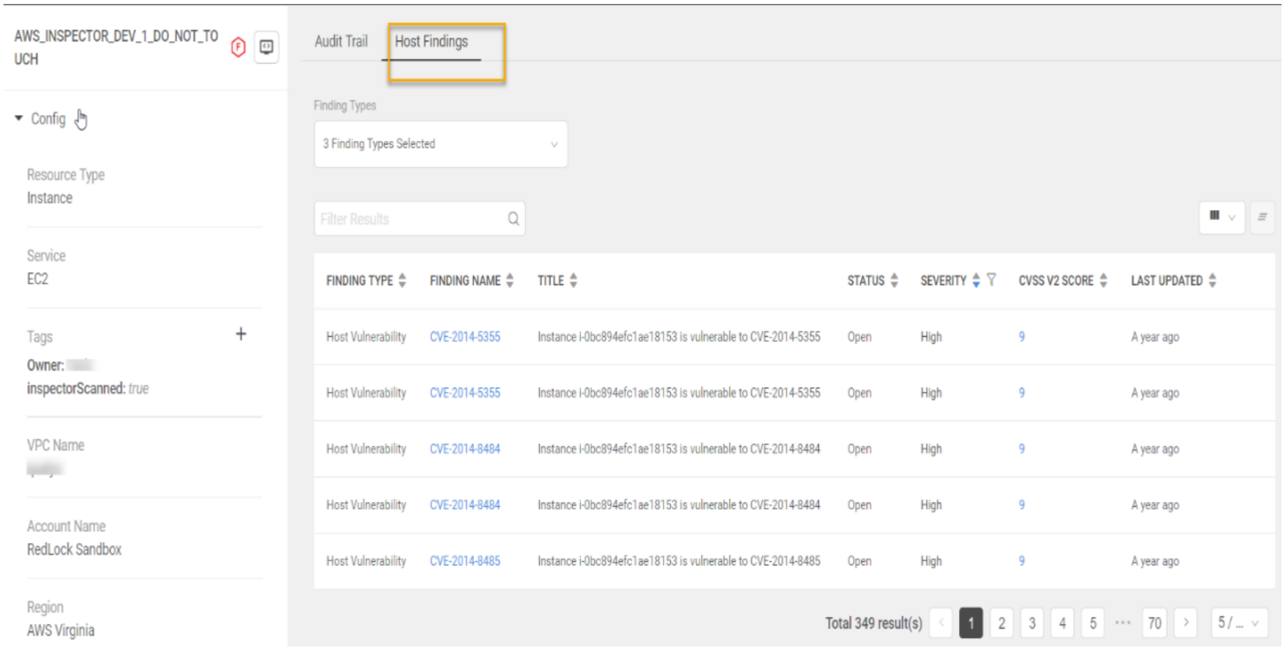
AWS Inspector Runtime Behavior Analysis:
Fetches all resources which are in violation of one or more rules reported by the AWS Runtime Behavior Analysis package.

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 from vpc.flow_record where dest.resource IN ( resource where finding.type = 'AWS Inspector Runtime Behavior Analysis' )
network from vpc.flow_record where dest.resource IN ( resource where finding.type = 'AWS Inspector Security Best Practices' )
```

Click on the resource to see an Audit trail.



AWS_INSPECTOR_DEV_1_DO_NOT_TOUCH

Resource Type
Instance

Service
EC2

Tags
Owner: [redacted]
inspectorScanned: *true*

VPC Name
[redacted]

Account Name
RedLock Sandbox

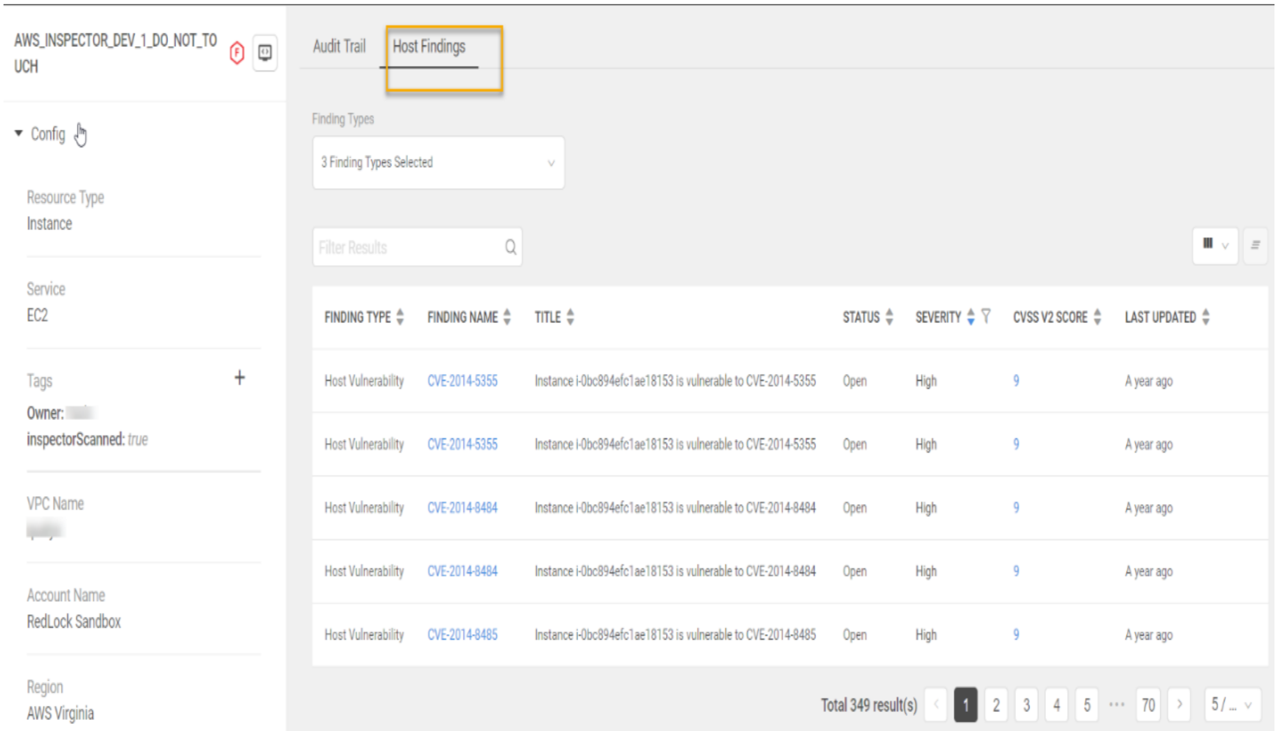
Region
AWS Virginia

Finding Types
3 Finding Types Selected

FINDING TYPE	FINDING NAME	TITLE	STATUS	SEVERITY	CVSS V2 SCORE	LAST UPDATED
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8485	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8485	Open	High	9	A year ago

Total 349 result(s) 1 2 3 4 5 ••• 70 5 / ...

Click Host Findings for information related to vulnerabilities.



AWS_INSPECTOR_DEV_1_DO_NOT_TOUCH

Config

Resource Type
Instance

Service
EC2

Tags
Owner: [redacted]
inspectorScanned: *true*

VPC Name
[redacted]

Account Name
RedLock Sandbox

Region
AWS Virginia

Audit Trail | Host Findings

Finding Types
3 Finding Types Selected

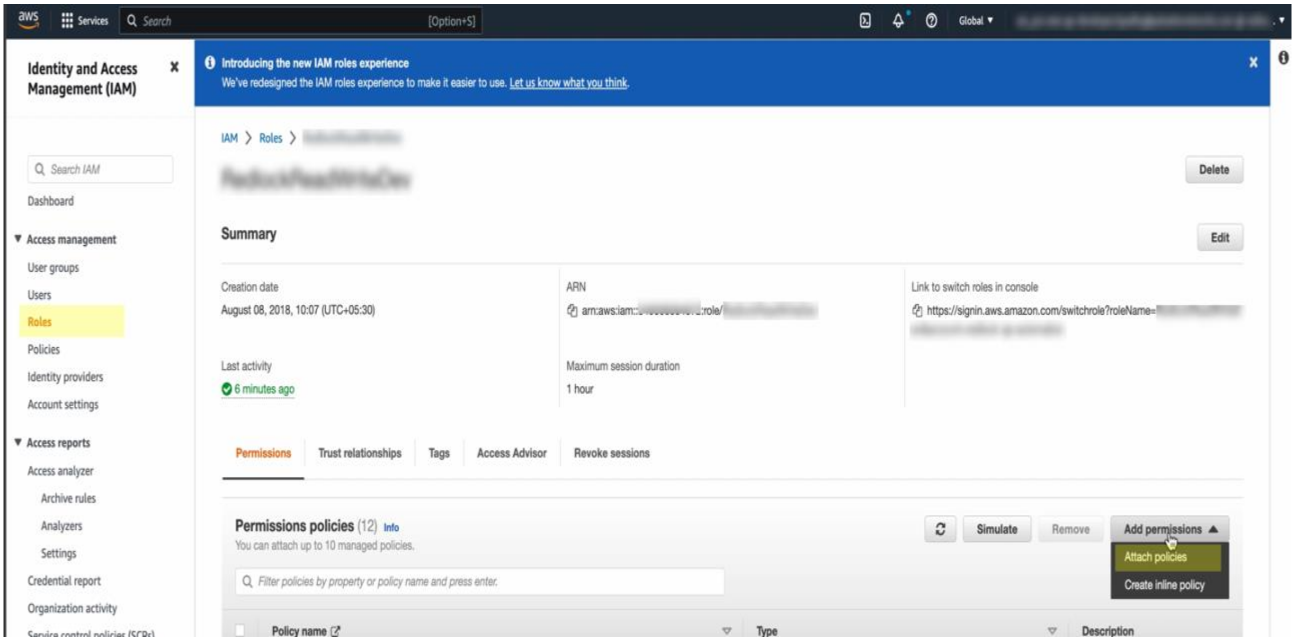
FINDING TYPE	FINDING NAME	TITLE	STATUS	SEVERITY	CVSS V2 SCORE	LAST UPDATED
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-5355	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-5355	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8484	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8484	Open	High	9	A year ago
Host Vulnerability	CVE-2014-8485	Instance i-0bc894efc1ae18153 is vulnerable to CVE-2014-8485	Open	High	9	A year ago

Total 349 result(s)

INTEGRATION WITH AWS SECURITY HUB

Step 1- Attach an AWS Security Hub read-only policy to your AWS role to enable this integration on the AWS console.

1. Log in to the AWS console and select IAM.
2. Select **Roles** and search for the role name which you had used for onboarding your account on Prisma Cloud.
3. Click on that role name and **Add permissions>Attach Policies**



Introducing the new IAM roles experience

We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

[redacted]

Creation date: August 08, 2018, 10:07 (UTC+05:30)

ARN: arn:aws:iam::[redacted]:role/[redacted]

Link to switch roles in console: https://signin.aws.amazon.com/switchrole?roleName=[redacted]

Last activity: 6 minutes ago

Maximum session duration: 1 hour

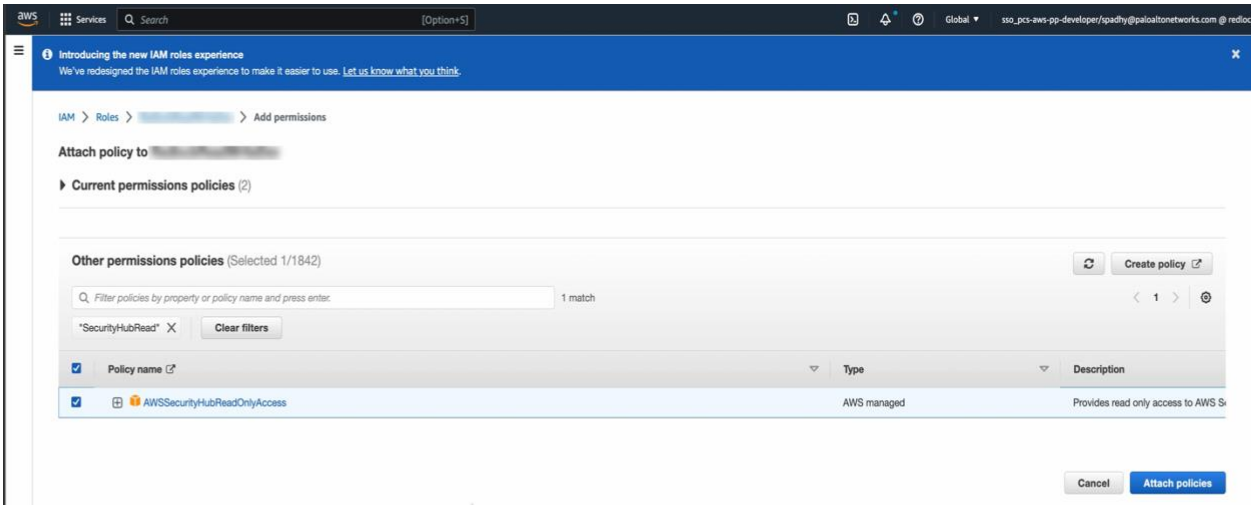
Permissions policies (12) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

4. Enter **SecurityHubRead** as the search term.

5. Select **AWSSecurityHubReadOnlyAccess** and then **Attach Policies**



sso_pcs-aws-pp-developer/spadhy@paloaltonetworks.com @ redloc

Introducing the new IAM roles experience

We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.

Attach policy to [redacted]

Current permissions policies (2)

Other permissions policies (Selected 1/1842)

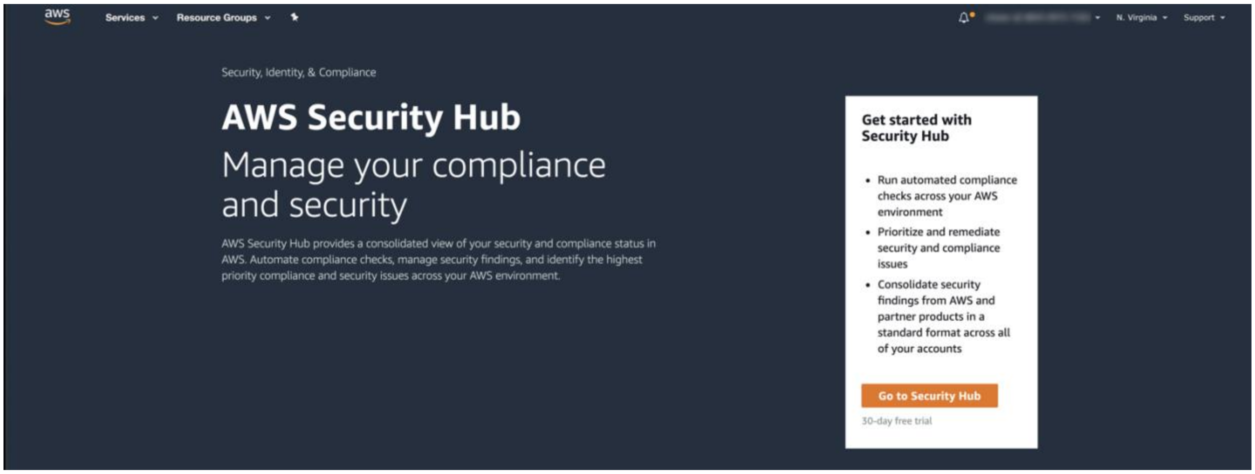
Filter policies by property or policy name and press enter. 1 match

"SecurityHubRead" X

☑	Policy name	Type	Description
☑	AWSSecurityHubReadOnlyAccess	AWS managed	Provides read only access to AWS S

Step 2 - Sign up for Prisma Cloud on AWS Security Hub.

1. Log in to the AWS console and select **Security Hub**



[redacted]

Security, Identity, & Compliance

AWS Security Hub

Manage your compliance and security

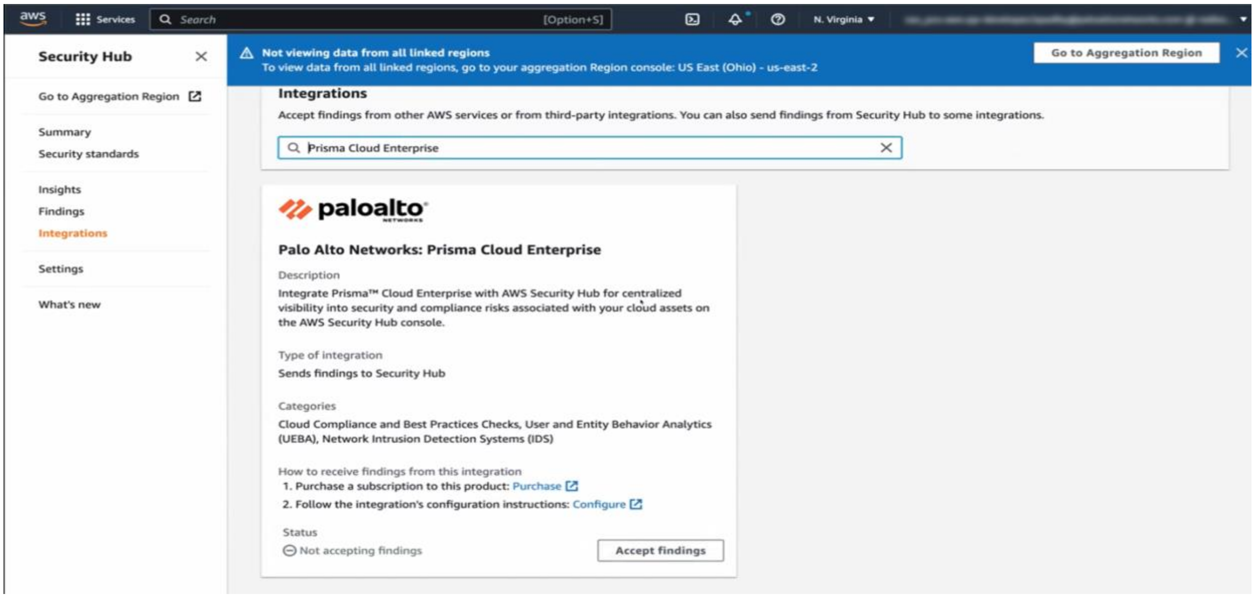
AWS Security Hub provides a consolidated view of your security and compliance status in AWS. Automate compliance checks, manage security findings, and identify the highest priority compliance and security issues across your AWS environment.

Get started with Security Hub

- Run automated compliance checks across your AWS environment
- Prioritize and remediate security and compliance issues
- Consolidate security findings from AWS and partner products in a standard format across all of your accounts

30-day free trial

2. Navigate to **Integrations** and enter **Prisma Cloud Enterprise** as the search term.
3. Find **Palo Alto Networks: Prisma Cloud Enterprise** and **Accept findings.**



[redacted]

Not viewing data from all linked regions
To view data from all linked regions, go to your aggregation Region console: US East (Ohio) - us-east-2

Integrations

Accept findings from other AWS services or from third-party integrations. You can also send findings from Security Hub to some integrations.

Prisma Cloud Enterprise

Palo Alto Networks: Prisma Cloud Enterprise

Description
Integrate Prisma™ Cloud Enterprise with AWS Security Hub for centralized visibility into security and compliance risks associated with your cloud assets on the AWS Security Hub console.

Type of integration
Sends findings to Security Hub

Categories
Cloud Compliance and Best Practices Checks, User and Entity Behavior Analytics (UEBA), Network Intrusion Detection Systems (IDS)

How to receive findings from this integration
1. Purchase a subscription to this product: Purchase
2. Follow the integration's configuration instructions: Configure

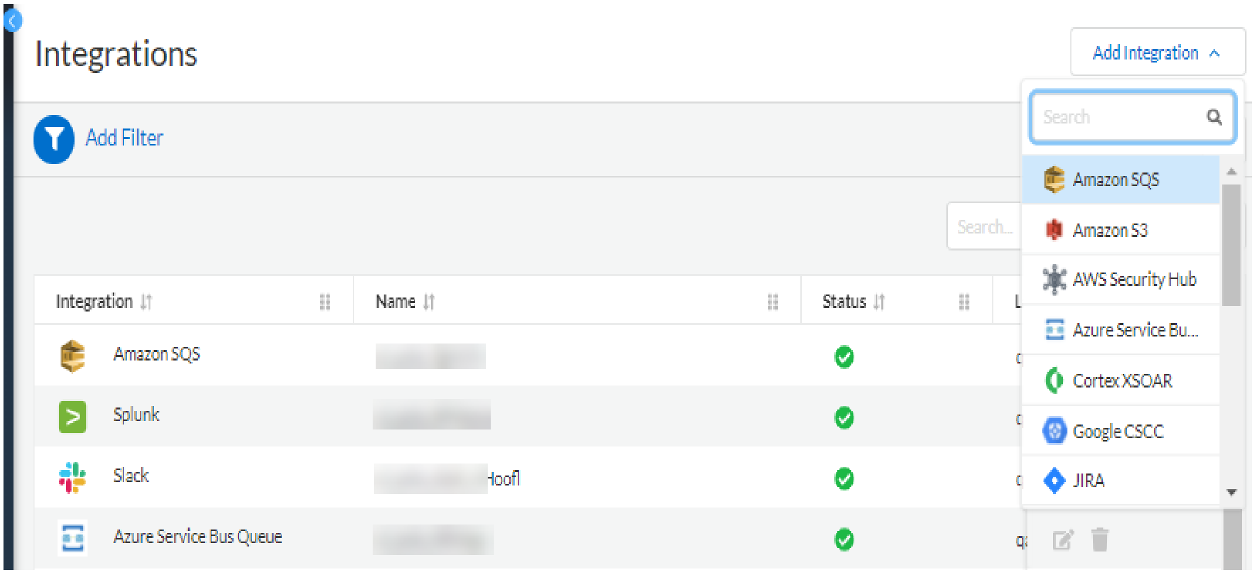
Status
⊖ Not accepting findings

Step 3 - Set up the AWS Security Hub Integration on Prisma Cloud.

1. 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 from the AWS console.

2. Log in to Prisma Cloud.
   Select **Settings Integrations**

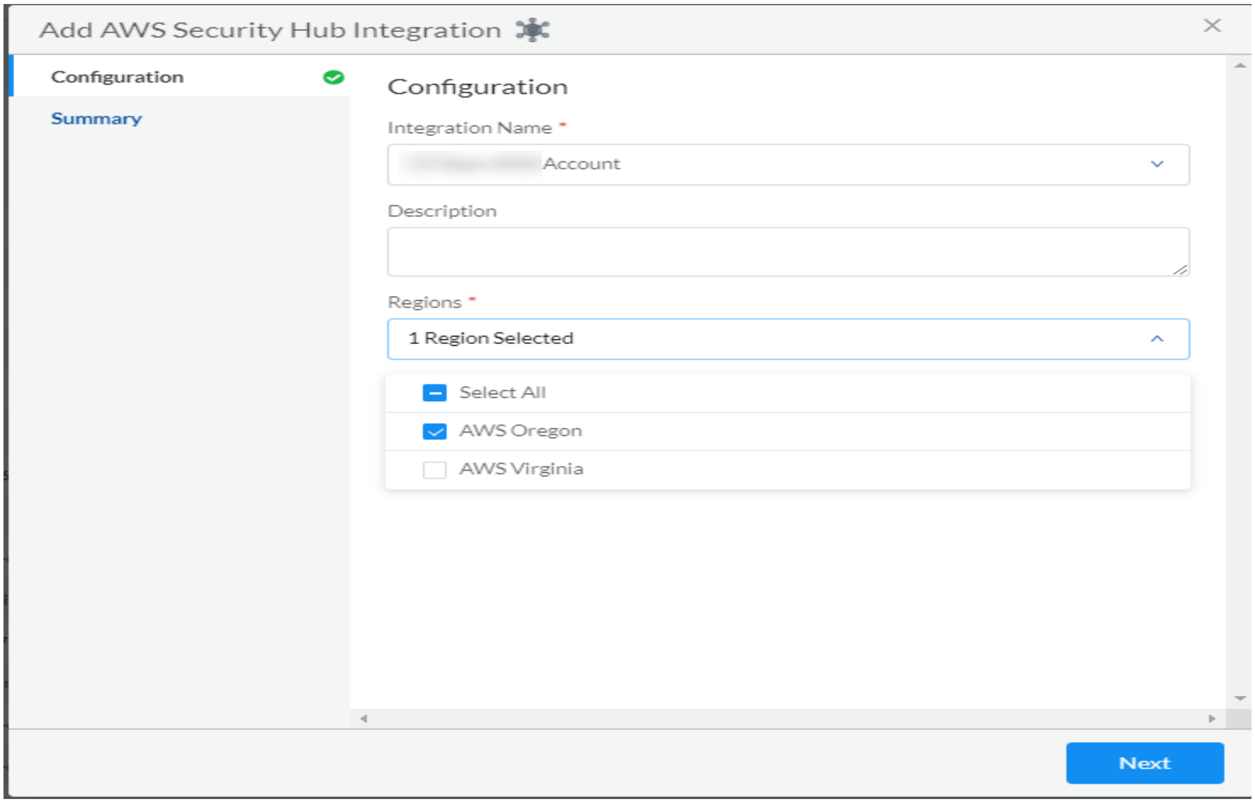
3. Add **Integration AWS Security Hub.** A modal wizard opens where you can add the AWS Security Hub integration



Integration	Name	Status	L
Amazon SQS	[redacted]	✓	c
Splunk	[redacted]	✓	c
Slack	[redacted] Hoofl	✓	c
Azure Service Bus Queue	[redacted]	✓	q

4. Set the **Integration Name** to the AWS account to which you assigned AWS Security Hub read-only access.

5. Enter a **Description** and select a **Region.** You select regions only if you enabled Prisma Cloud on AWS Security Hub.



Configuration

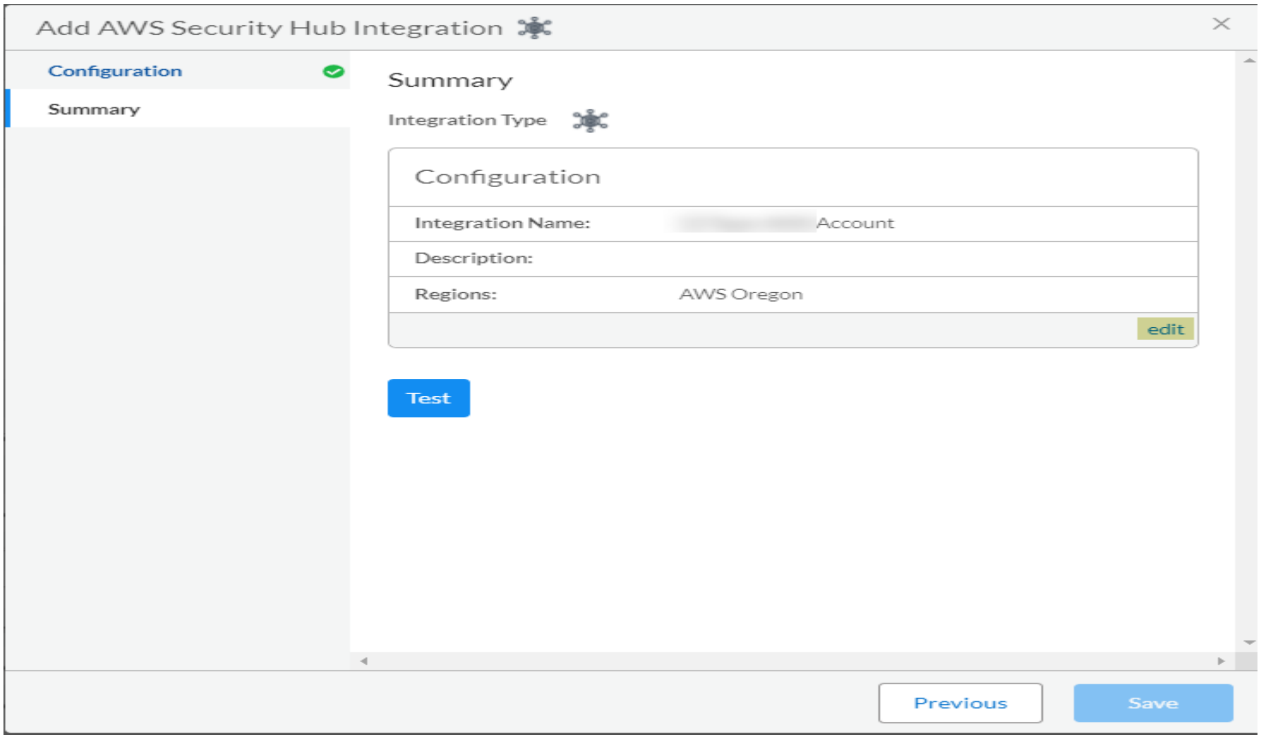
Integration Name *: [redacted] Account

Description:

Regions *: 1 Region Selected

- ▬ Select All
- ☑ AWS Oregon
- □ AWS Virginia

Next. Review the **Summary** and either **edit** to make changes or **Test**.



Summary

Integration Type

Configuration

Integration Name: [redacted] Account

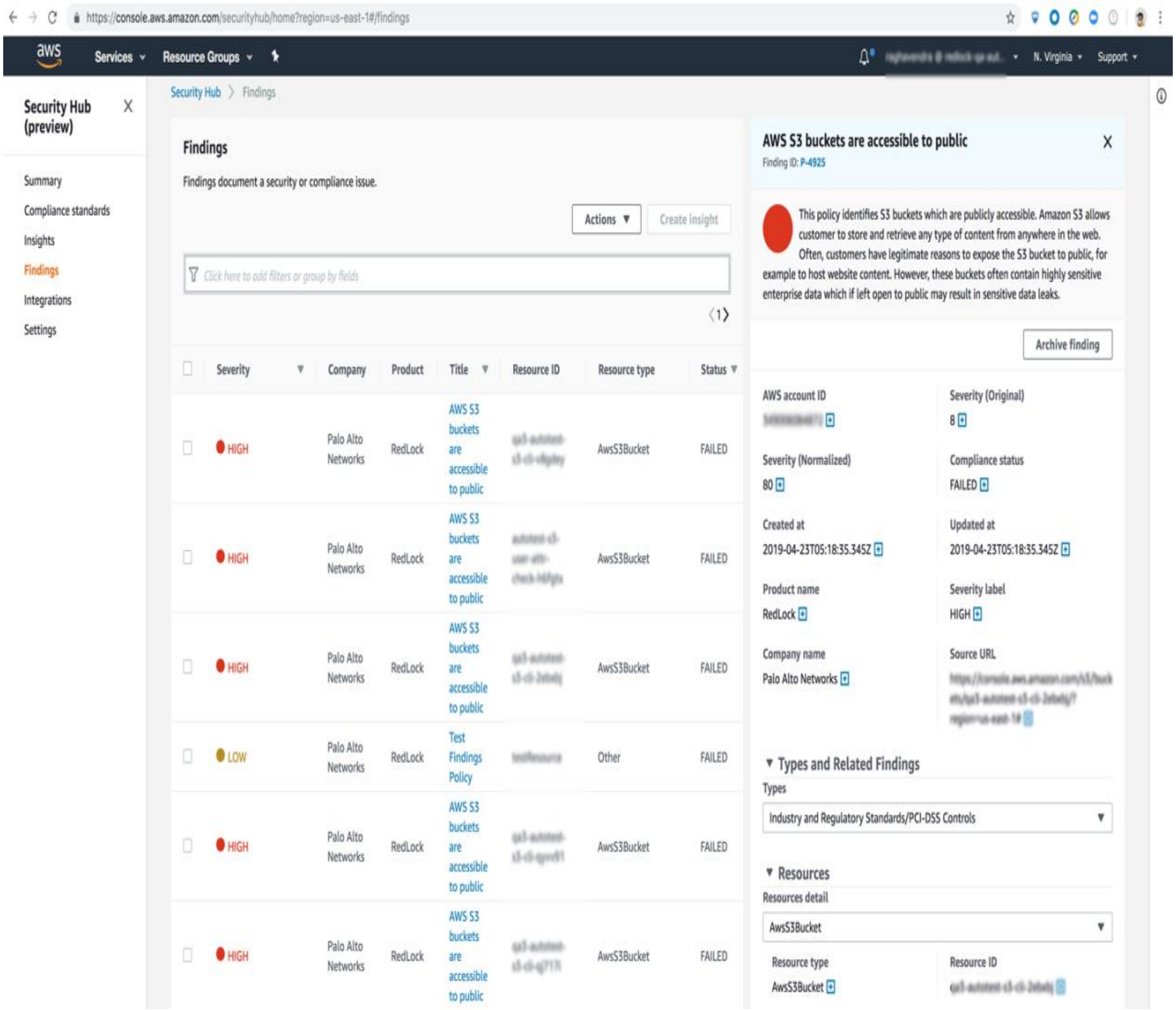
Description:

Regions: AWS Oregon

Save the integration. After you set up the integration successfully, you can use the Get Status link in **Settings Integrations** to periodically check the integration status.

Step 4 - Modify an existing alert rule or create a new alert rule to specify when to send alert notifications. View Prisma Cloud alerts on AWS Security Hub.

Step 5 - Log in to the AWS console and select Security Hub. Click Findings to view the alerts. Select the Title to view details the alert description**.**



https://console.aws.amazon.com/securityhub/home?region=us-east-1#/findings

Findings

Findings document a security or compliance issue.

□	Severity	Company	Product	Title	Resource ID	Resource type	Status
□	● HIGH	Palo Alto Networks	RedLock	AWS S3 buckets are accessible to public	[redacted]	AwsS3Bucket	FAILED
□	● HIGH	Palo Alto Networks	RedLock	AWS S3 buckets are accessible to public	[redacted]	AwsS3Bucket	FAILED
□	● HIGH	Palo Alto Networks	RedLock	AWS S3 buckets are accessible to public	[redacted]	AwsS3Bucket	FAILED
□	● LOW	Palo Alto Networks	RedLock	Test Findings Policy	[redacted]	Other	FAILED
□	● HIGH	Palo Alto Networks	RedLock	AWS S3 buckets are accessible to public	[redacted]	AwsS3Bucket	FAILED
□	● HIGH	Palo Alto Networks	RedLock	AWS S3 buckets are accessible to public	[redacted]	AwsS3Bucket	FAILED

AWS S3 buckets are accessible to public

Finding ID: P-4925

This policy identifies S3 buckets which are publicly accessible. Amazon S3 allows customer to store and retrieve any type of content from anywhere in the web. Often, customers have legitimate reasons to expose the S3 bucket to public, for example to host website content. However, these buckets often contain highly sensitive enterprise data which if left open to public may result in sensitive data leaks.

AWS account ID [redacted]	Severity (Original) 8
Severity (Normalized) 80	Compliance status FAILED
Created at 2019-04-23T05:18:35.345Z	Updated at 2019-04-23T05:18:35.345Z
Product name RedLock	Severity label HIGH
Company name Palo Alto Networks	Source URL [redacted]

▼ Types and Related Findings

Types: Industry and Regulatory Standards/PCI-DSS Controls ▼

▼ Resources

Resources detail: AwsS3Bucket ▼

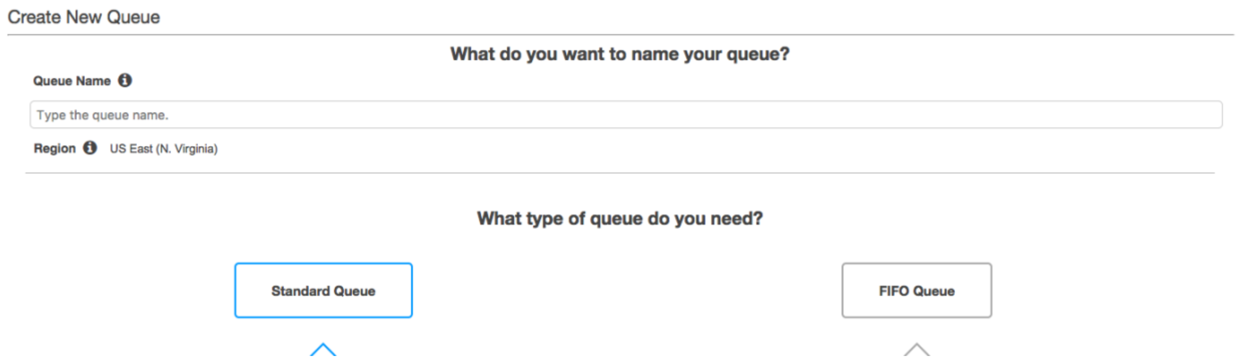
Resource type AwsS3Bucket	Resource ID [redacted]

INTEGRATION WITH AMAZON SQS

If you use Amazon Simple Queue Service (SQS) to enable custom workflows for alerts, Prisma™ Cloud integrates with Amazon SQS. When you set up the integration, as soon as an alert is generated, the alert payload is sent to Amazon SQS.
The integration gives you the flexibility to send alerts to a queue in the same AWS account that you may have onboarded to Prisma Cloud or to a queue in a different AWS account. If you want to send alerts to an SQS in a different AWS account, you must provide the relevant IAM credentials—Access Key or IAM Role.

Step 1- Configure Amazon SQS to receive Prisma Cloud alerts.

1. Log in to the Amazon console with the necessary credentials to create and configure the SQS.
2. Click **Simple Queue Services** (under **Application Integration**).
3. Create a **New Queue** or use an existing queue.



Create New Queue

What do you want to name your queue?

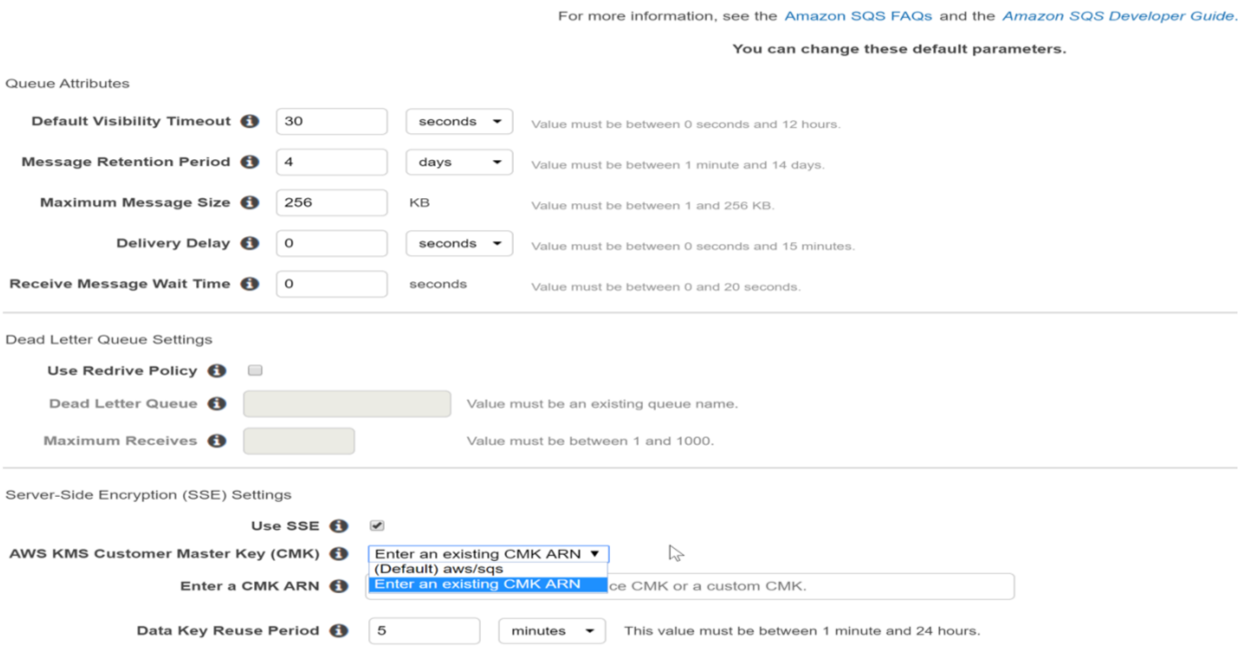
Queue Name: Type the queue name.

Region: US East (N. Virginia)

What type of queue do you need?

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 the AWS default selection or set them per your company policies. **Use SSE** to keep all messages in the Queue encrypted, and select the default AWS KMS Customer Master Key (CMK) or enter your CMK ARN.



For more information, see the Amazon SQS FAQs and the *Amazon SQS Developer Guide*.

You can change these default parameters.

Queue Attributes

Default Visibility Timeout: 30 seconds — Value must be between 0 seconds and 12 hours.

Message Retention Period: 4 days — Value must be between 1 minute and 14 days.

Maximum Message Size: 256 KB — Value must be between 1 and 256 KB.

Delivery Delay: 0 seconds — Value must be between 0 seconds and 15 minutes.

Receive Message Wait Time: 0 seconds — Value must be between 0 and 20 seconds.

Dead Letter Queue Settings

Use Redrive Policy □

Dead Letter Queue — Value must be an existing queue name.

Maximum Receives — Value must be between 1 and 1000.

Server-Side Encryption (SSE) Settings

Use SSE ☑

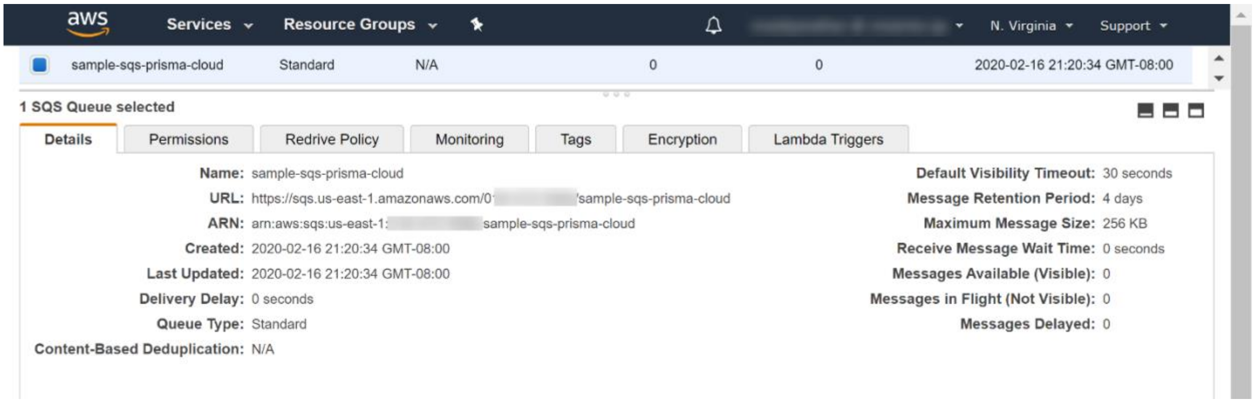
AWS KMS Customer Master Key (CMK): Enter an existing CMK ARN

Enter a CMK ARN — ce CMK or a custom CMK.

Data Key Reuse Period: 5 minutes — This value must be between 1 minute and 24 hours.

Create Queue:

This creates and displays your SQS Queue.
Click the Queue that you created and view the **Details** and copy the **URL** for this queue. You provide this value in Prisma Cloud to integrate Prisma Cloud notifications into this Queue.



sample-sqs-prisma-cloud | Standard | N/A | 0 | 0 | 2020-02-16 21:20:34 GMT-08:00

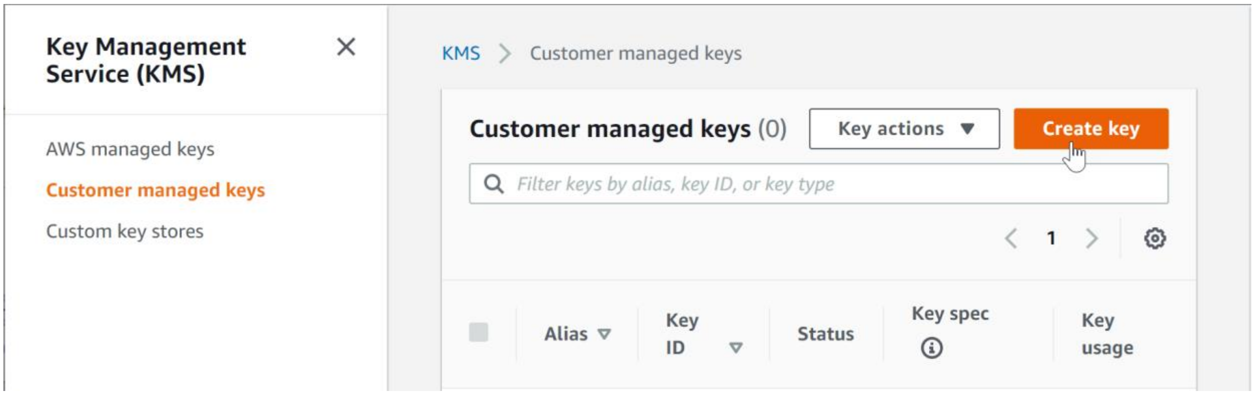
1 SQS Queue selected

Name: sample-sqs-prisma-cloud
URL: https://sqs.us-east-1.amazonaws.com/0[redacted]/sample-sqs-prisma-cloud
ARN: arn:aws:sqs:us-east-1:[redacted]sample-sqs-prisma-cloud
Created: 2020-02-16 21:20:34 GMT-08:00
Last Updated: 2020-02-16 21:20:34 GMT-08:00
Delivery Delay: 0 seconds
Queue Type: Standard
Content-Based Deduplication: N/A

Default Visibility Timeout: 30 seconds
Message Retention Period: 4 days
Maximum Message Size: 256 KB
Receive Message Wait Time: 0 seconds
Messages Available (Visible): 0
Messages in Flight (Not Visible): 0
Messages Delayed: 0

Step 2 - If you are using a Customer Managed Key to encrypt queues in Amazon SQS, you must configure the Prisma Cloud Role with explicit permission to read the key.

1. On the Amazon console, select **KMS** > **Customer Managed Keys** and **Create Key.**



Key Management Service (KMS)

2. Enter an Alias and Description, and add any required **Tags** and click **Next**.
3. Select the IAM users and roles who can use this key through the **KMS**API and click **Next**
4. Select the IAM users and roles who can use this key to encrypt and decrypt the data.
5. 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 use to onboard your AWS setup needs these permissions:

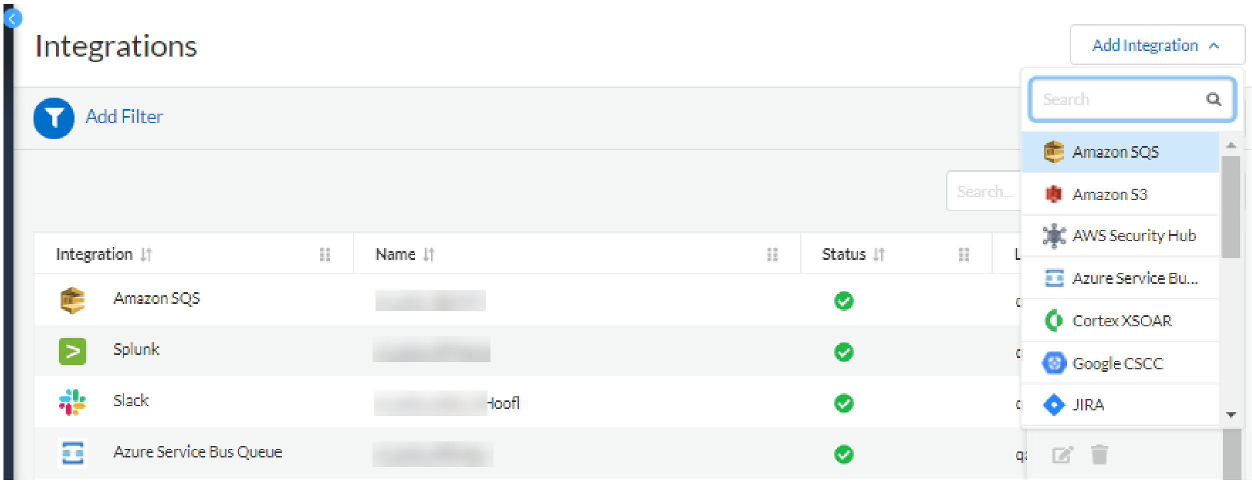
```
"sqs:GetQueueAttributes", "sqs:ListQueues","sqs:SendMessage",
"sqs:SendMessageBatch", "tag:GetResources","iam:GetRole”
```

When you add the above permissions to the CFT Templates and the account you run the template on is the same account to which the SQS Queue belongs, the Prisma Cloud IAM role will have the permissions required to write to the queue. If you do not want to add the permissions to the role or if the SQS Queue belongs to a different account, then proceed to Integrate Prisma Cloud with Amazon SQS.

Step 4 - Set up Amazon SQS integration in Prisma Cloud.

1. Add **Integration Amazon SQS**. A modal wizard opens where you can add the SQS integration.

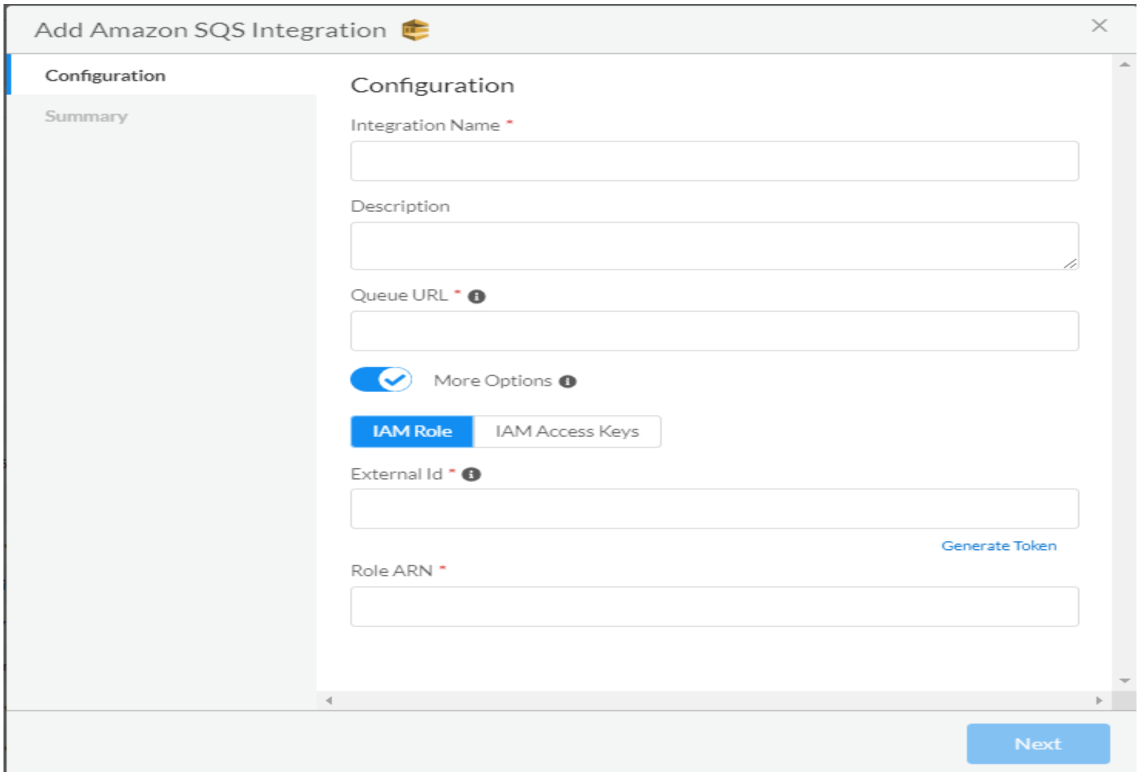
2. Enter a **Name** and **Description** for the integration.



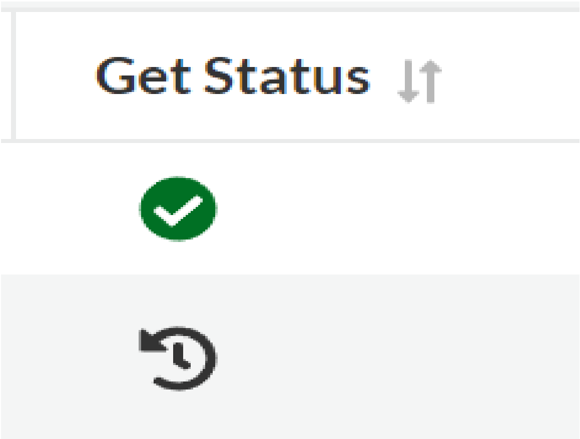
Integration	Name	Status
Amazon SQS	[redacted]	✓
Splunk	[redacted]	✓
Slack	[redacted]	✓
Azure Service Bus Queue	[redacted]	✓

3. Enter the Queue **URL** that you copied when you configured Prisma Cloud in Amazon SQS.

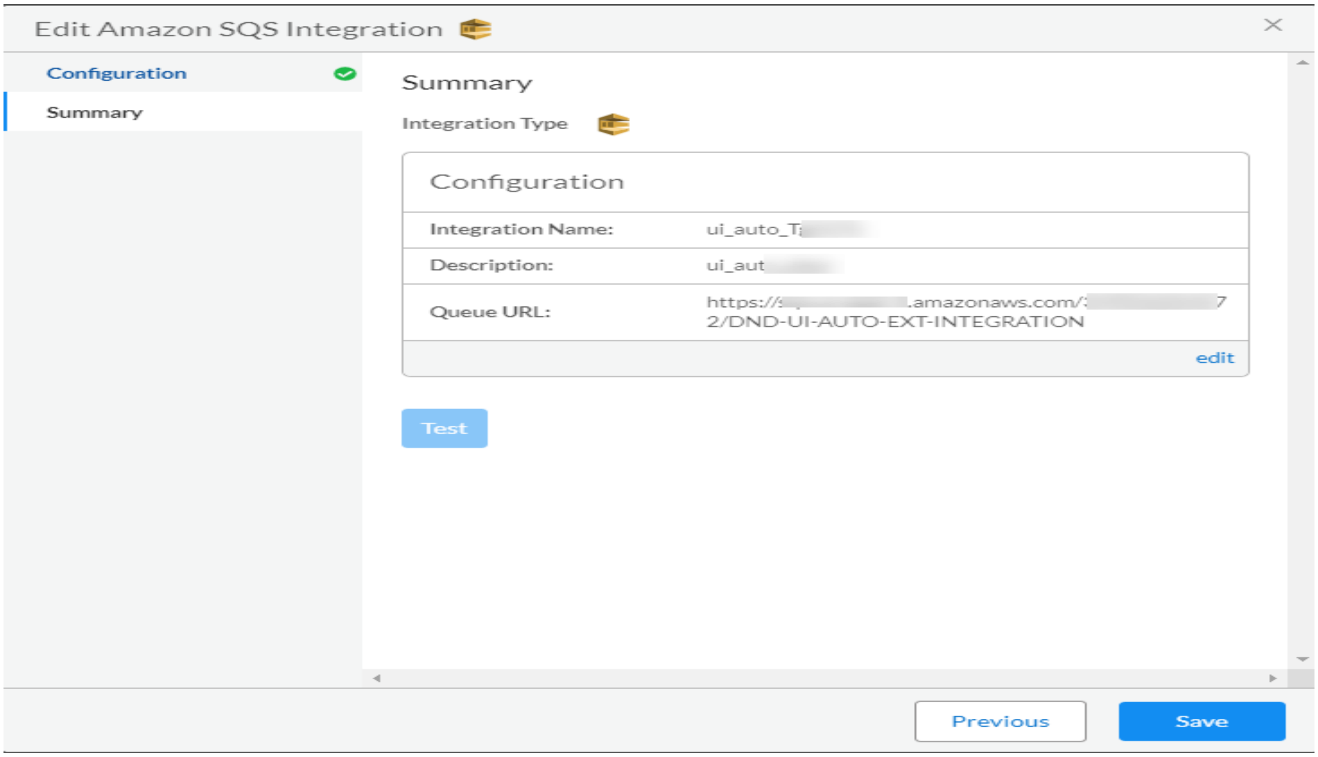
4. The queue URL format on AWS China should be **https://sqs.<China region api identifier>.amazonaws.com.cn/<account id>/<queue name>**.



5. Next to review the **Summary**.
6. Test and **save** the integration. After you set up the integration successfully, you can use the Get Status link in **Settings Integrations** to periodically check the integration status.



7. To edit the integration, on **Settings Integrations**, click the corresponding **edit** icon. The integration **Summary** page opens.



Integration Name:	ui_auto_T[redacted]
Description:	ui_aut[redacted]
Queue URL:	https://[redacted].amazonaws.com/[redacted]7 2/DND-UI-AUTO-EXT-INTEGRATION

8. Edit to update the integration as required.

9. Next to review your edits.

10. Test and **save** the integration.

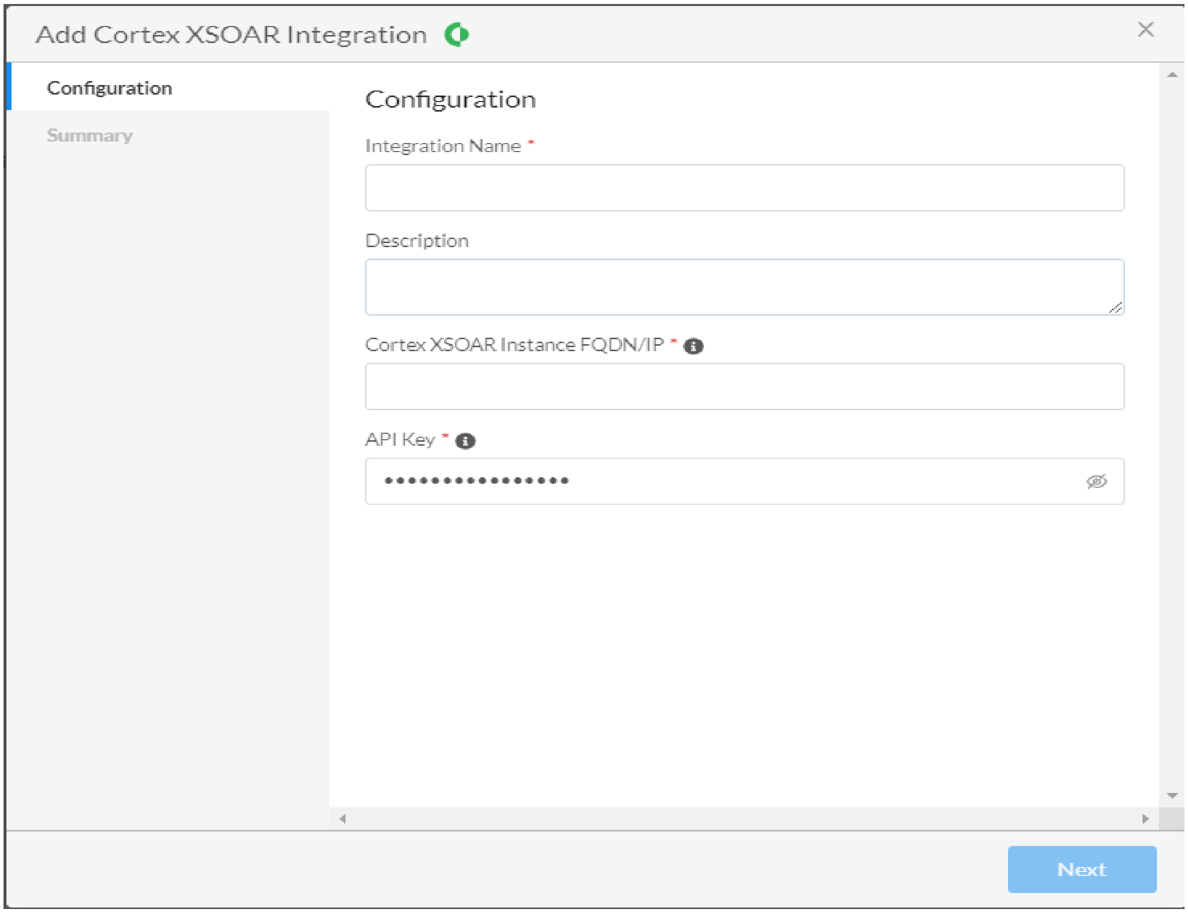
Step 5- Create an Alert Rule for Run-Time Checks or modify an existing rule to enable Amazon.

Integration With CORTEX XSOAR

Set up Cortex XSOAR as an external integration on Prisma Cloud. If you have a firewall or cloud Network Security Group between the internet and Cortex XSOAR, you must ensure network reachability and Enable Access to the Prisma Cloud Console.
For the push-based integration, you must use Cortex XSOAR version 5.0.0 and the latest Prisma Cloud content pack.

Step 1 - Log in to Prisma Cloud and select Settings **Integrations**.

Step 2 - Add Integration Cortex XSOAR. A modal wizard opens where you can add the Cortex integration.


Add Cortex XSOAR Integration

Configuration

Integration Name *

Description

Cortex XSOAR Instance FQDN/IP *

API Key *

•••••••••••••••••

Step 3- Enter **Integration Name** and **Description**.

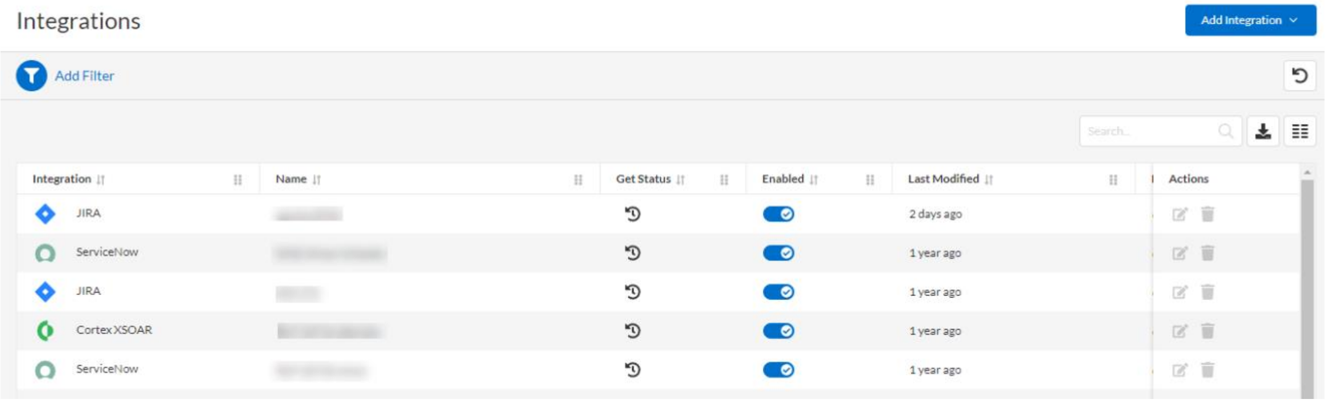
Step 4- Enter your **Cortex XSOAR Instance FQDN/IP** address.
If you are adding a Cortex XSOAR instance that is part of a multi-tenant deployment, enter the tenant URL without the protocol (http or https).

Step 5- Enter the **API Key** associated with the Cortex XSOAR administrative user account.

The API key you provide must belong to a Cortex XSOAR administrative user who has read-write permissions, which are required to enable this push-based integration. Within Cortex XSOAR, navigate to **Settings > Integrations > API Keys** and **Get Your Key.**

Step 6- Click **Next** and then **Test**.

Step 7- Save the integration. After you set up the integration successfully, you can use the Get Status link in **Settings Integrations** to periodically check the integration status.



Integration	Name	Get Status	Enabled	Last Modified	Actions
JIRA	[redacted]	⟲	✓	2 days ago	✎ 🗑
ServiceNow	[redacted]	⟲	✓	1 year ago	✎ 🗑
JIRA	[redacted]	⟲	✓	1 year ago	✎ 🗑
Cortex XSOAR	[redacted]	⟲	✓	1 year ago	✎ 🗑
ServiceNow	[redacted]	⟲	✓	1 year ago	✎ 🗑

Step 8 - Modify an existing Alert Rule or create a new Alert Rule to send alert notifications to Cortex XSOAR. (See Send Prisma Cloud Alert Notifications to Third-Party Tools.)

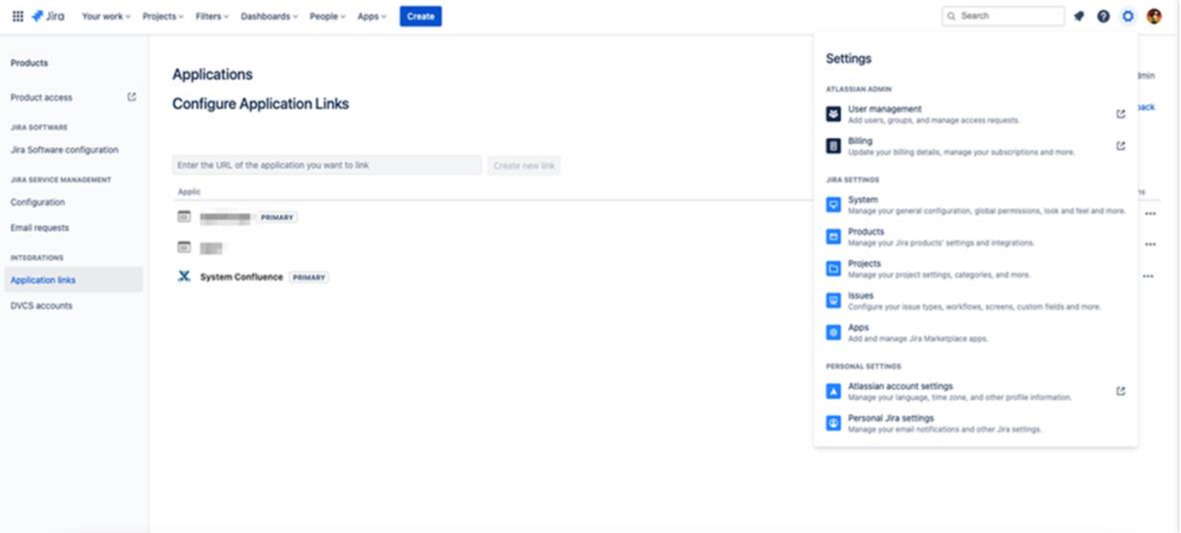
Step 9 - Get your Prisma Cloud Access Key.
If you do not have an access key, see Create and Manage Access Keys. You need the Access Key ID and Secret Key ID to complete the integration on Cortex XSOAR.

Step 10- Set up the Integration on Cortex XSOAR

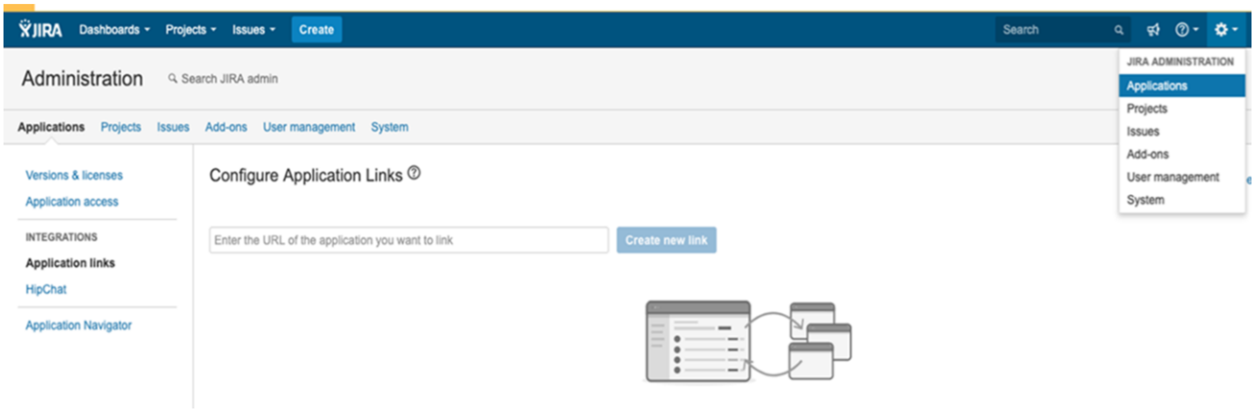
INTEGRATION WITH JIRA

Step 1- Login to Jira as a Jira Administrator.

Step 2 - Locate **Application Links**.
For Jira Cloud, select **Jira Settings >Products >Application Links**.

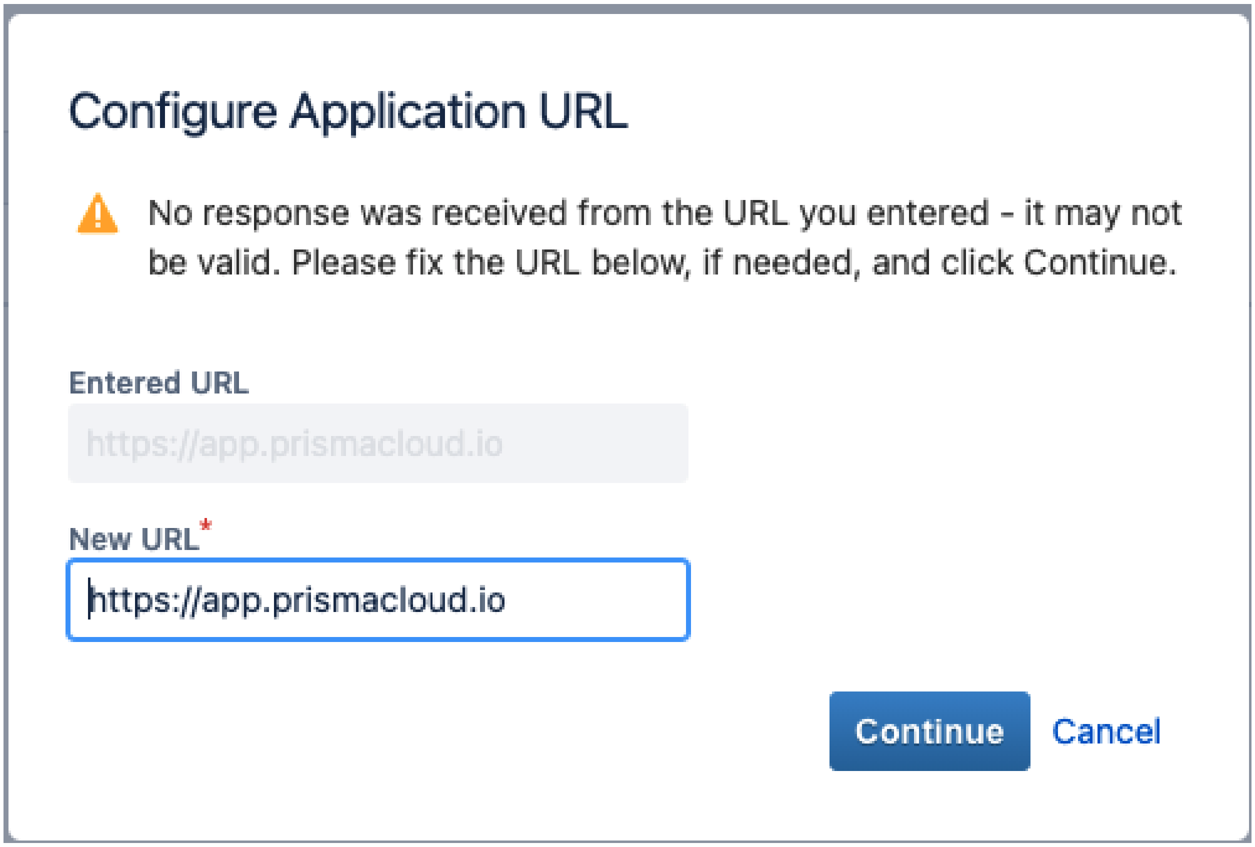

Jira
Your work
Projects
Filters
Dashboards
People
Apps
Create
Search
Products
Product access
JIRA SOFTWARE
Jira Software configuration
JIRA SERVICE MANAGEMENT
Configuration
Email requests
INTEGRATIONS
Application links
DVCS accounts
Applications
Configure Application Links
Enter the URL of the application you want to link
Create new link
Applic
PRIMARY
System Confluence
PRIMARY
Settings
ATLASSIAN ADMIN
User management
Add users, groups, and manage access requests.
Billing
Update your billing details, manage your subscriptions and more.
JIRA SETTINGS
System
Manage your general configuration, global permissions, look and feel and more.
Products
Manage your Jira products' settings and integrations.
Projects
Manage your project settings, categories, and more.
Issues
Configure your issue types, workflows, screens, custom fields and more.
Apps
Add and manage Jira Marketplace apps.
PERSONAL SETTINGS
Atlassian account settings
Manage your language, time zone, and other profile information.
Personal Jira settings
Manage your email notifications and other Jira settings.

For Jira On-Premises, select **Settings** >**Applications >Application Links**.



Step 3- Enter the URL for your instance of Prisma Cloud in **Configure Application Links** and Create **a new link**..

Step 4- Disregard a message in



Configure Application URL

⚠ No response was received from the URL you entered - it may not be valid. Please fix the URL below, if needed, and click Continue.

Entered URL: https://app.prismacloud.io

New URL*: https://app.prismacloud.io

Configure Application URL and **Continue**.

Step 5 - Enter the **Application Name** and set the **Application Type** to **Generic Application**.

Step 6 - Create **incoming Link** and **Continue**.

Step 7 - On **Link Applications**, specify a **Consumer Key** and a **Consumer Name**. Save the **Consumer Key** because you will need this value when you enter the information in Prisma Cloud.

Step - 8 Copy the **Public Key** shown below and **continue**.

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnYoXB+BZ555jUIFyN+0b3g7haTch
syeWwDcUrTcebbDN1jy5zjZ/vp31//L9HzA0WCFtmgj5hhaFcMl1bCFY93oiobsiWsJmMLgDyYB
ghpManIQ73TEHDIAsV49r2TLtX01iRWSW65CefBHD6b/1rvrhxVDDKjfxgCMLojHBPb7nLqXMx
OKrY8s1yCLXyzoFGTN6ankFgyJ0BQh+SMj/hyB59LPVin0bf415ME1FpCJ3yow258sOT7TAJ00
```

```
ejyyhC3igh+nVQXP+1V0ztpnpfoXUypA7UKvdI0Qf1ZsviyHNwiNg7xgYc+H64cBmAgfcfDNzXyP
mJZkM7cGC2y4ukQIDAQAB
```

Prisma Cloud is listed in your Jira account after successful creation.

Setup **Jira Integration** on Prisma Cloud

Step 1 - Login to Prisma Cloud.

Step 2 - Select **Settings Integrations**.

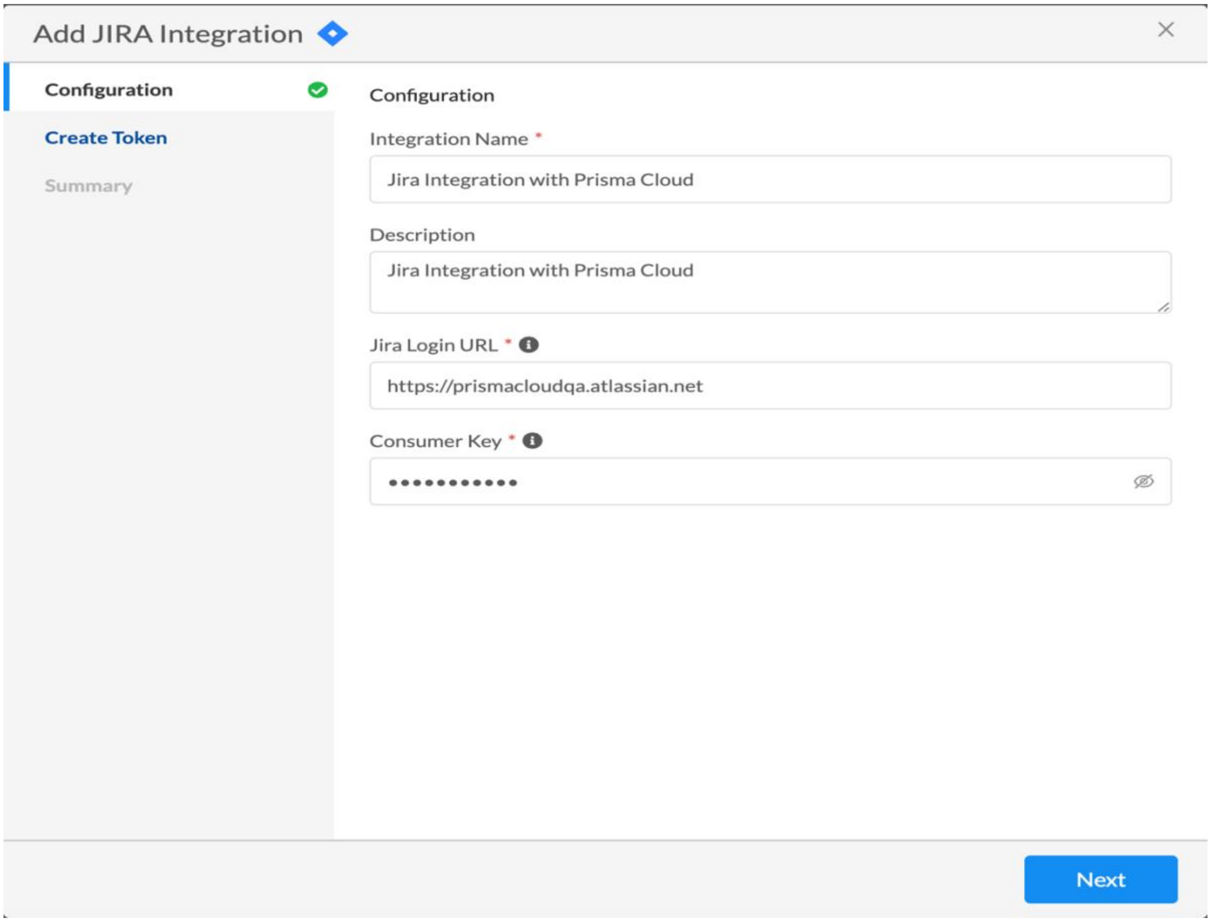
Step 3 - Click **Add Integration**

Step 4 - Set **Integration** to **JIRA**.

Step 5 - Specify a meaningful **Integration Name** and, optionally, add a **Description**.

Step 6 - Enter the **JIRA Login URL**. Make sure the URL starts with https and does **not** have a trailing slash (‘/’) at the end.

Step 7 - Enter the Consumer Key that you created when you created the Prisma Cloud application in Jira and click **Next**.



Add JIRA Integration

Configuration

Integration Name *

Jira Integration with Prisma Cloud

Description

Jira Integration with Prisma Cloud

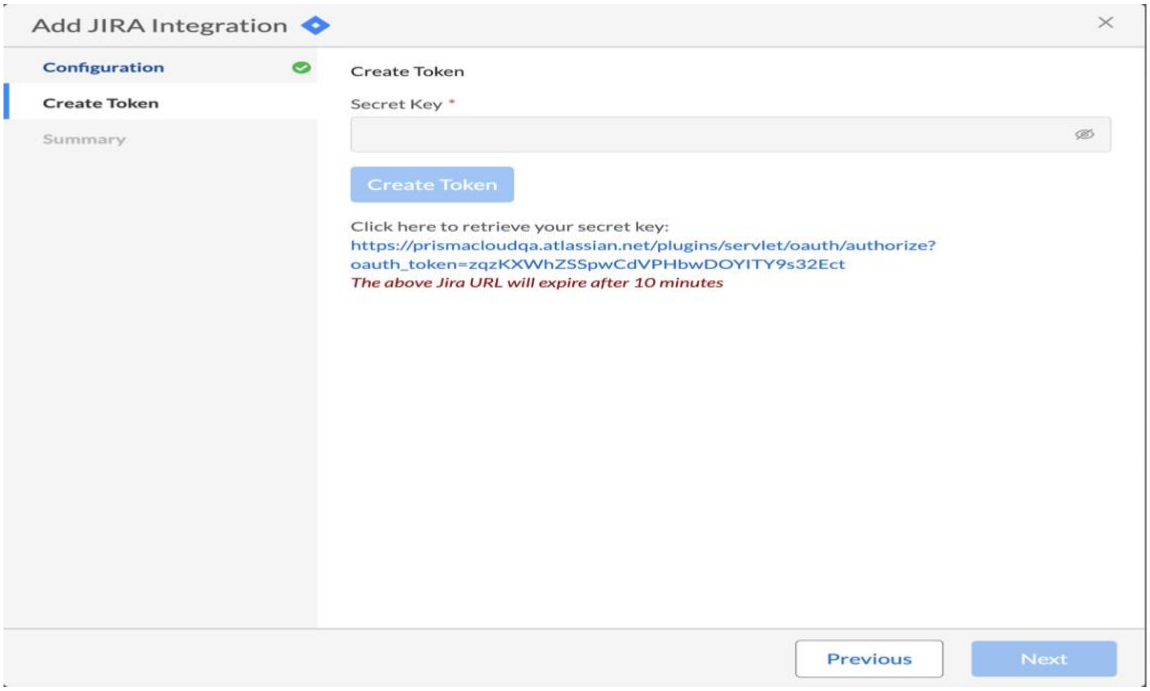
Jira Login URL *

https://prismacloudqa.atlassian.net

Consumer Key *

••••••••••••

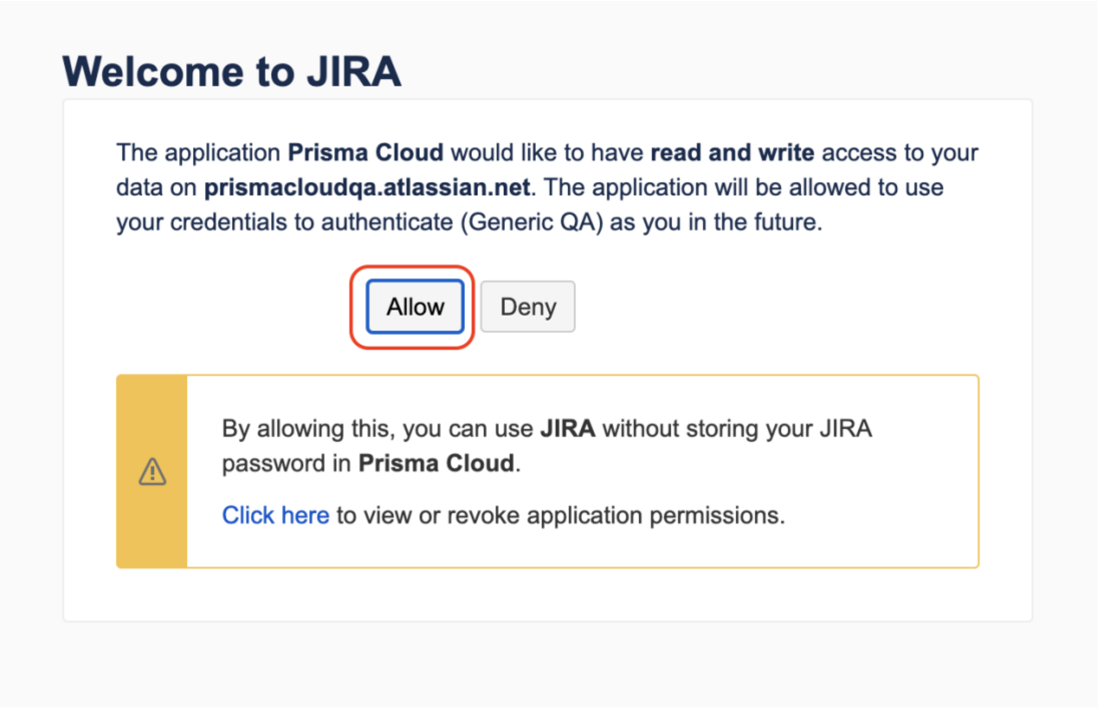
Step 8 - Click the secret key URL link to retrieve your secret key. The URL with the verification code is valid for only 10 minutes.



Secret Key *

Click here to retrieve your secret key:
https://prismacloudqa.atlassian.net/plugins/servlet/oauth/authorize?oauth_token=zqzKXWhZSSpwCdVPHbwDOYITY9s32Ect
The above Jira URL will expire after 10 minutes

Step 9 - When redirected to the **Welcome to JIRA** page, allow Prisma Cloud “**read and write”** access to data in your Jira account.



The application **Prisma Cloud** would like to have **read and write** access to your data on **prismacloudqa.atlassian.net**. The application will be allowed to use your credentials to authenticate (Generic QA) as you in the future.

By allowing this, you can use **JIRA** without storing your JIRA password in **Prisma Cloud**.

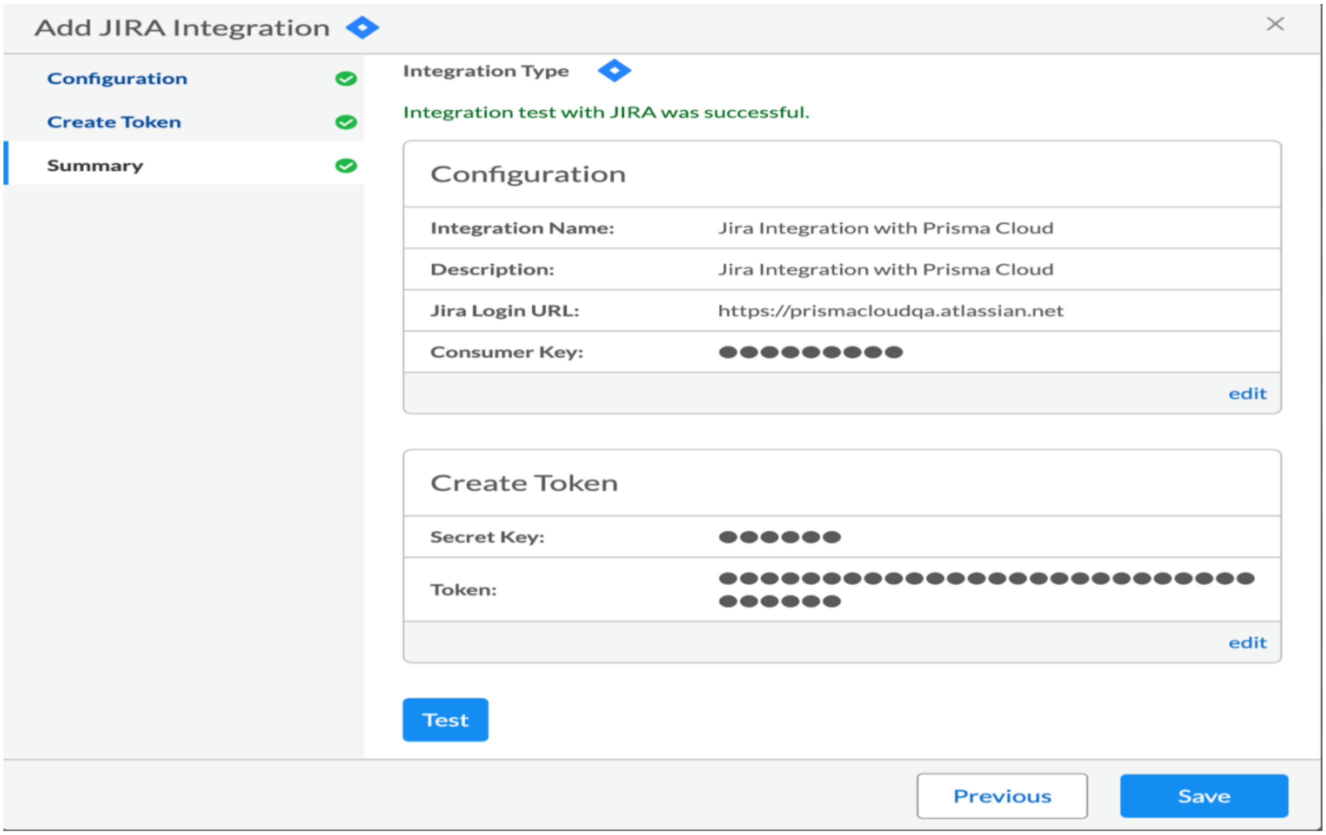
Click here to view or revoke application permissions.

Step 10 - Copy the verification code displayed on the page, paste it as the **Secret Key**, and click **Create Token**.

Step 11- After you see the Token generated! message, click **Next.**

Step 12 - Check the **Summary** and click **Test**.

Step 13 - After you see the Integration test with JIRA was successful. message, click **Save**. The integration will be listed on the Integrations page.



Integration test with JIRA was successful.

Configuration

Integration Name:	Jira Integration with Prisma Cloud
Description:	Jira Integration with Prisma Cloud
Jira Login URL:	https://prismacloudqa.atlassian.net
Consumer Key:	●●●●●●●●●●

Create Token

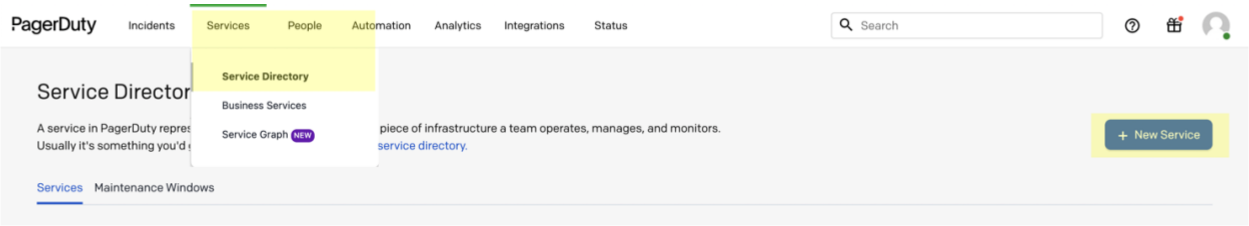
Secret Key:	●●●●●●
Token:	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Integration With PagerDuty

Step 1. Create a new service in PagerDuty and get the integration key.

1. Log in to PagerDuty.

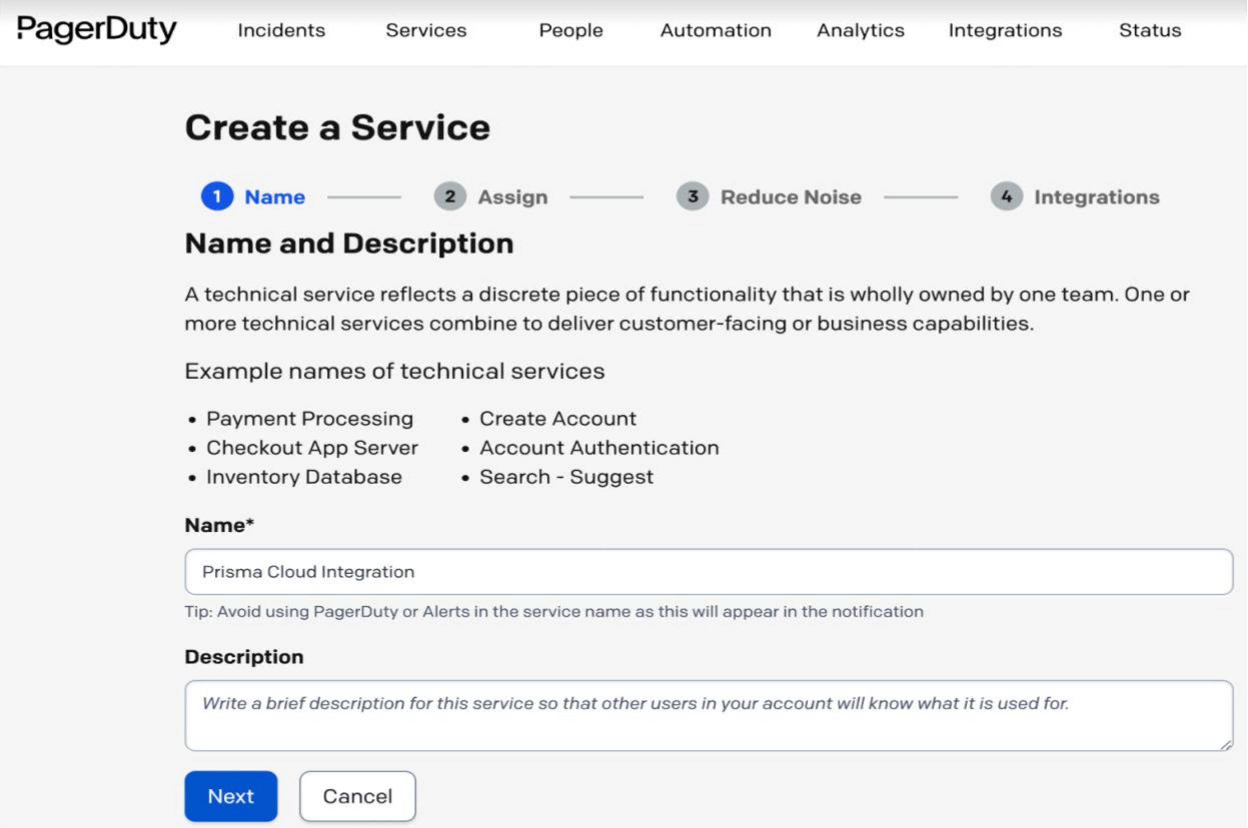
2. Click **Services, Service Directory** and create a **+ New Service**



Service Director

A service in PagerDuty repres piece of infrastructure a team operates, manages, and monitors.
Usually it's something you'd service directory.

3. Complete the **Create a Service** form.
- Enter a **Name**, **Description**, and click **Next**



Create a Service

Name and Description

A technical service reflects a discrete piece of functionality that is wholly owned by one team. One or more technical services combine to deliver customer-facing or business capabilities.

Example names of technical services

- Payment Processing
- Checkout App Server
- Inventory Database
- Create Account
- Account Authentication
- Search - Suggest

Name*

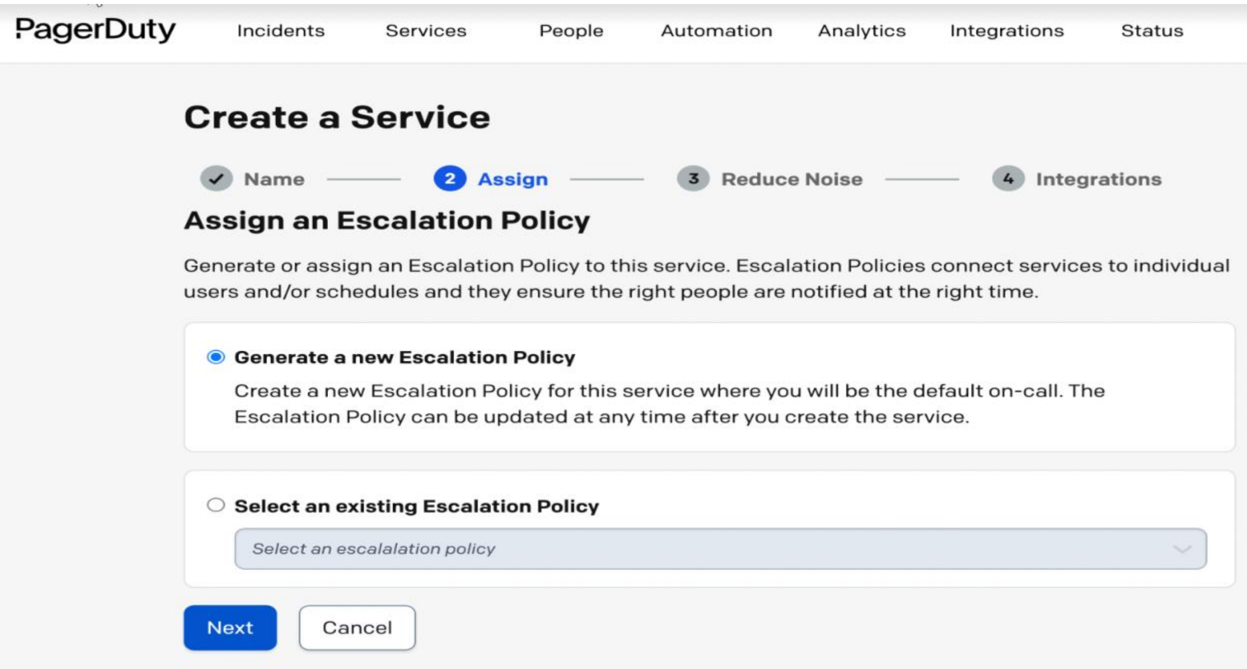
Prisma Cloud Integration

Tip: Avoid using PagerDuty or Alerts in the service name as this will appear in the notification

Description

Write a brief description for this service so that other users in your account will know what it is used for.

-Generate a new escalation policy or select an existing policy to the service and click **Next.**



Create a Service

✓ Name — 2 Assign — 3 Reduce Noise — 4 Integrations

Assign an Escalation Policy

Generate or assign an Escalation Policy to this service. Escalation Policies connect services to individual users and/or schedules and they ensure the right people are notified at the right time.

● **Generate a new Escalation Policy**

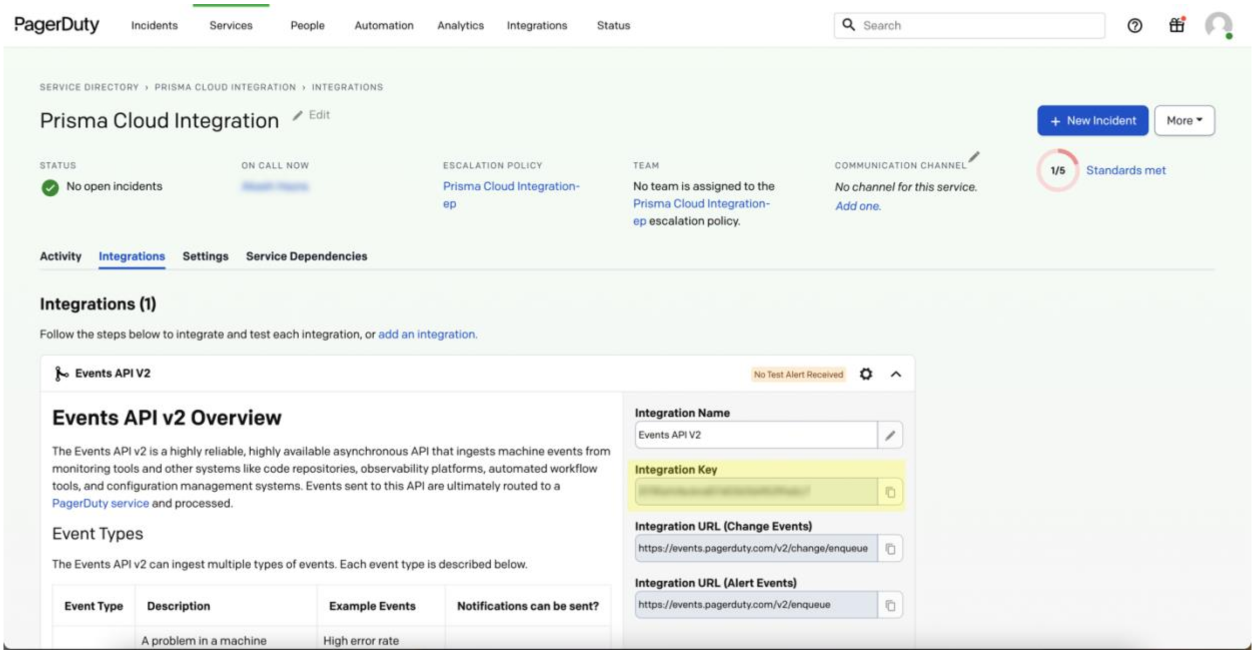
Create a new Escalation Policy for this service where you will be the default on-call. The Escalation Policy can be updated at any time after you create the service.

○ **Select an existing Escalation Policy**

Select an escalalation policy

-Set the Alert Grouping options as you need and click **Next**.

-Select the **Events API V2** integration.



SERVICE DIRECTORY › PRISMA CLOUD INTEGRATION › INTEGRATIONS

Prisma Cloud Integration ✎ Edit

STATUS: No open incidents

ON CALL NOW: [redacted]

ESCALATION POLICY: Prisma Cloud Integration-ep

TEAM: No team is assigned to the Prisma Cloud Integration-ep escalation policy.

COMMUNICATION CHANNEL: *No channel for this service. Add one.*

1/5 Standards met

Integrations (1)

Follow the steps below to integrate and test each integration, or add an integration.

Events API V2 — No Test Alert Received

Events API v2 Overview

The Events API v2 is a highly reliable, highly available asynchronous API that ingests machine events from monitoring tools and other systems like code repositories, observability platforms, automated workflow tools, and configuration management systems. Events sent to this API are ultimately routed to a PagerDuty service and processed.

Event Types

The Events API v2 can ingest multiple types of events. Each event type is described below.

Event Type	Description	Example Events	Notifications can be sent?
	A problem in a machine	High error rate	

Integration Name: Events API V2

Integration Key: [redacted]

Integration URL (Change Events): https://events.pagerduty.com/v2/change/enqueue

Integration URL (Alert Events): https://events.pagerduty.com/v2/enqueue

-Click **Create Service**.

4. After creating a new service, you will be directed to its **Integrations** page.

5. Copy and save the **Integration Key.**

Step -2 After creating a new service, you will be directed to its Integrations page.

1. Copy and save the **Integration Key**. You will need to enter this integration key while setting up PagerDuty integration on Prisma Cloud.

2. Set up PagerDuty as an integration channel on Prisma Cloud.

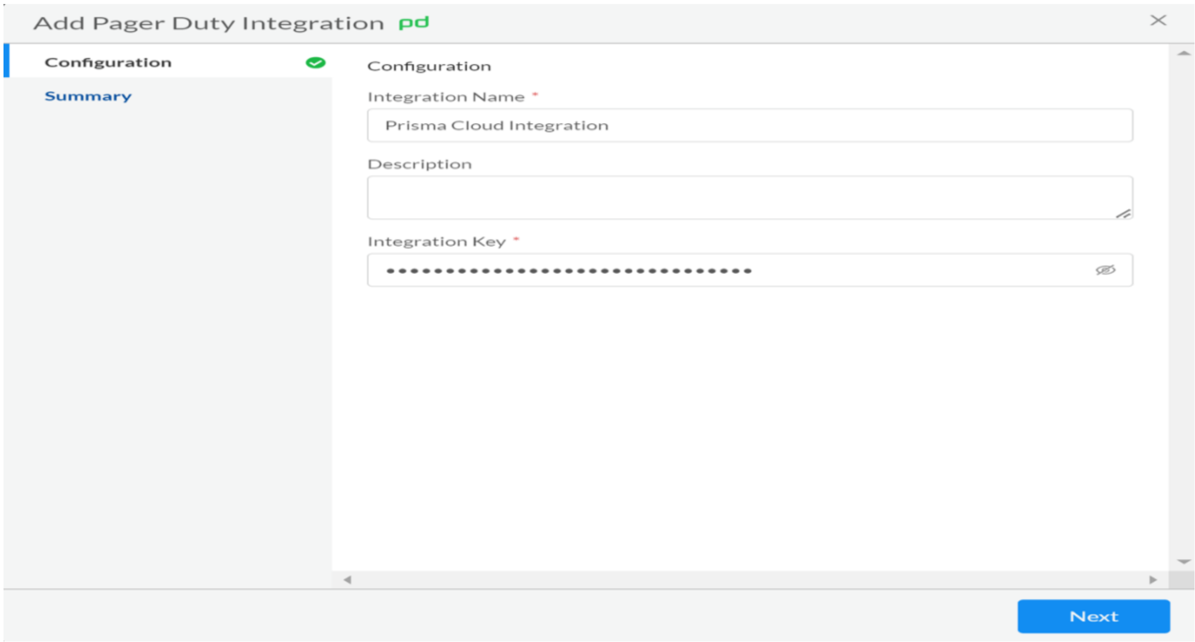
3. Log in to Prisma Cloud and select **Settings Integrations**.

4. Click **Add Integration**.

5. Set the **Integration** to **Pager Duty.**

6. Enter the **Integration Name** and **Description.**

7. Enter the **Integration Key** that you had saved while creating your PagerDuty service.



Add Pager Duty Integration

Configuration

Integration Name *

Prisma Cloud Integration

Description

Integration Key *

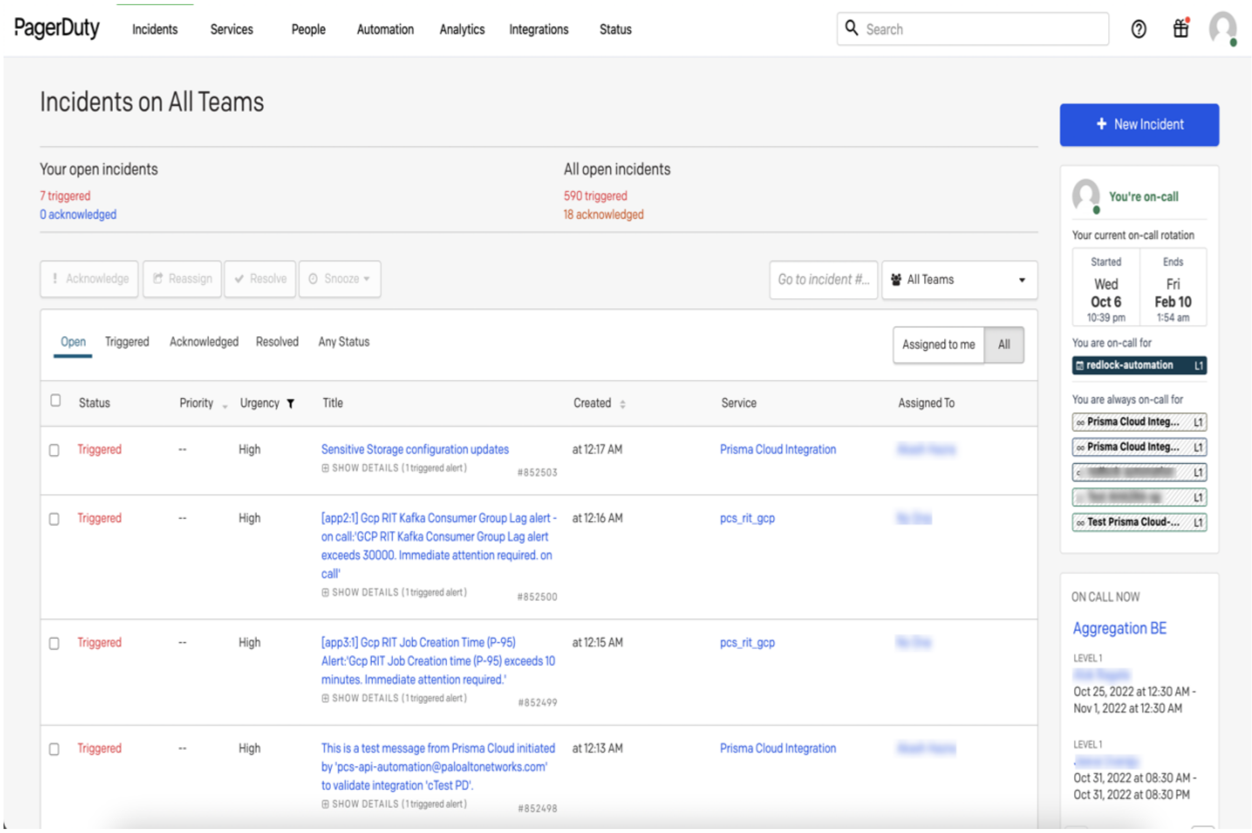
••••••••••••••••••••••••••••••••

8. Click **Next** and then **Test**.

Step 3 - Save the integration. Prisma Cloud creates a test incident and sends it to your service in PagerDuty. To ensure that integration is successful, look for test integration in your PagerDuty Service.

Step 4- Modify an existing alert rule or create a new alert rule to send alert notifications to PagerDuty.

Step 5 -View Prisma Cloud in PagerDuty. In PagerDuty, all the open alerts display the Incident State as Triggered and all the resolved alerts display the Incident State as Resolved.



Incidents on All Teams

Your open incidents
7 triggered
0 acknowledged

All open incidents
590 triggered
18 acknowledged

□	Status	Priority	Urgency	Title	Created	Service	Assigned To
□	Triggered	--	High	Sensitive Storage configuration updates ⊞ SHOW DETAILS (1 triggered alert) #852503	at 12:17 AM	Prisma Cloud Integration	[redacted]
□	Triggered	--	High	[app2:1] Gcp RIT Kafka Consumer Group Lag alert - on call:'GCP RIT Kafka Consumer Group Lag alert exceeds 30000. Immediate attention required. on call' ⊞ SHOW DETAILS (1 triggered alert) #852500	at 12:16 AM	pcs_rit_gcp	[redacted]
□	Triggered	--	High	[app3:1] Gcp RIT Job Creation Time (P-95) Alert:'Gcp RIT Job Creation time (P-95) exceeds 10 minutes. Immediate attention required.' ⊞ SHOW DETAILS (1 triggered alert) #852499	at 12:15 AM	pcs_rit_gcp	[redacted]
□	Triggered	--	High	This is a test message from Prisma Cloud initiated by 'pcs-api-automation@paloaltonetworks.com' to validate integration 'cTest PD'. ⊞ SHOW DETAILS (1 triggered alert) #852498	at 12:13 AM	Prisma Cloud Integration	[redacted]

You're on-call

Your current on-call rotation

Started	Ends
Wed Oct 6 10:39 pm	Fri Feb 10 1:54 am

You are on-call for
redlock-automation L1

You are always on-call for
Prisma Cloud Integ... L1
Prisma Cloud Integ... L1
[redacted] L1
[redacted] L1
Test Prisma Cloud-... L1

ON CALL NOW

Aggregation BE

LEVEL 1
[redacted]
Oct 25, 2022 at 12:30 AM - Nov 1, 2022 at 12:30 AM

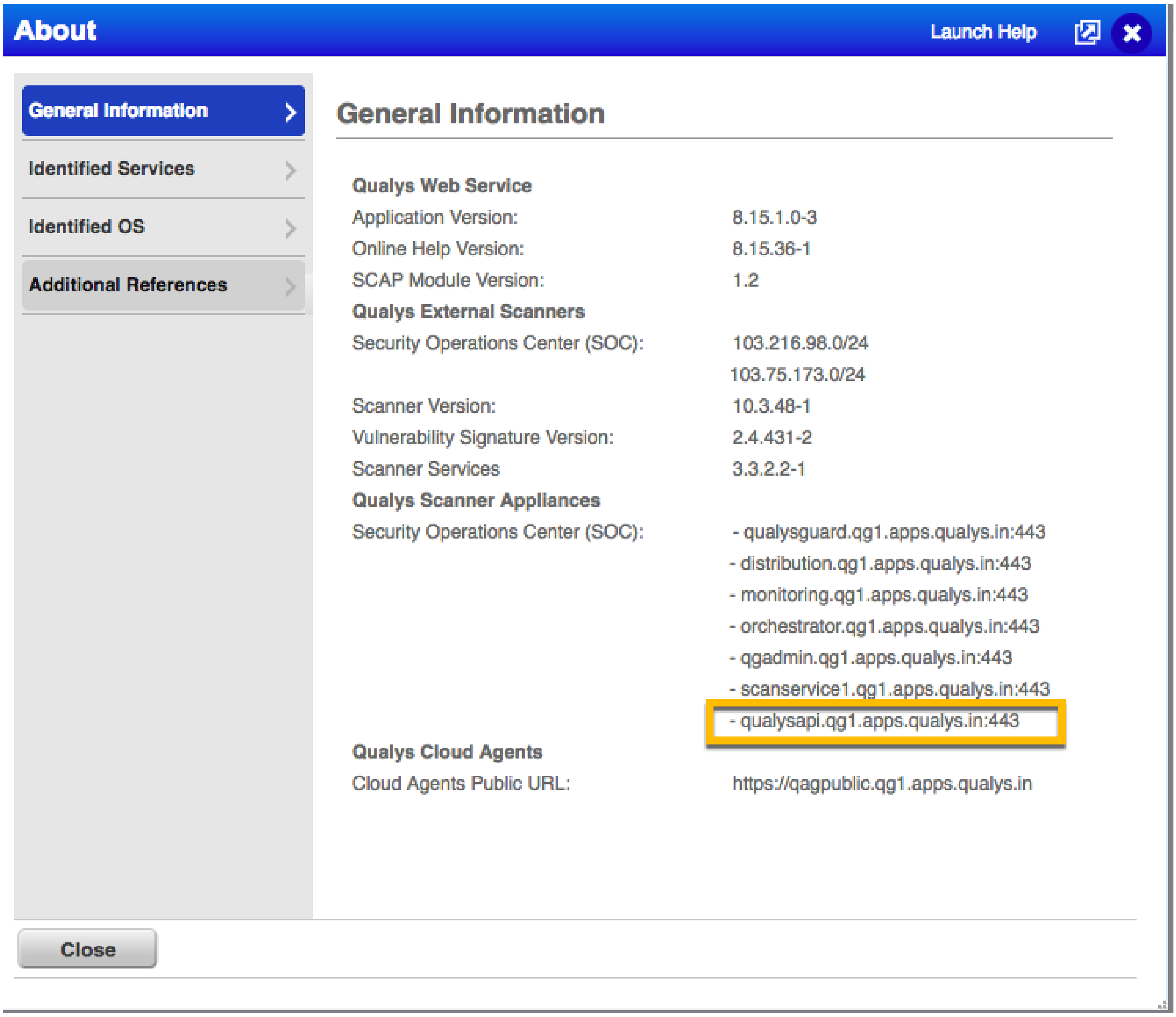
LEVEL 1
[redacted]
Oct 31, 2022 at 08:30 AM - Oct 31, 2022 at 08:30 PM

INTEGRATION WTH QUALYS

1. Gather the information that you need to set up the Qualys integration on Prisma Cloud.

○ You must obtain the Qualys Security Operations Center (SOC) server API URL (also known as or associated with a POD—the point of delivery to which you are assigned and connected for access to Qualys).

Get the API URL from your Qualys account. The Qualys API URL is listed under **Qualys Scanner Appliances**. When you enter this URL in as the **Qualys API Server URL**, do not include :443.



General Information

Qualys Web Service

Application Version:	8.15.1.0-3
Online Help Version:	8.15.36-1
SCAP Module Version:	1.2

Qualys External Scanners

Security Operations Center (SOC):	103.216.98.0/24 103.75.173.0/24
Scanner Version:	10.3.48-1
Vulnerability Signature Version:	2.4.431-2
Scanner Services	3.3.2.2-1

Qualys Scanner Appliances

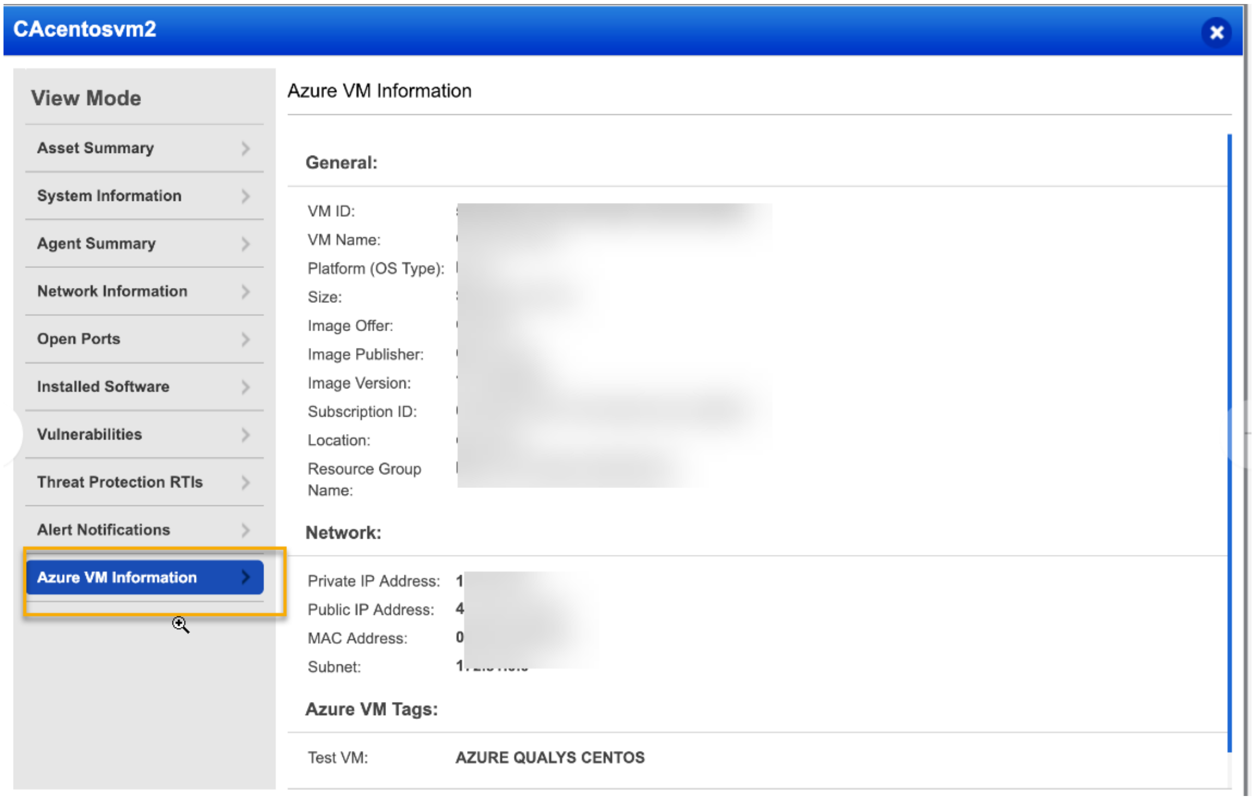
Security Operations Center (SOC):	- qualysguard.qg1.apps.qualys.in:443 - distribution.qg1.apps.qualys.in:443 - monitoring.qg1.apps.qualys.in:443 - orchestrator.qg1.apps.qualys.in:443 - qgadmin.qg1.apps.qualys.in:443 - scanservice1.qg1.apps.qualys.in:443 - qualysapi.qg1.apps.qualys.in:443

Qualys Cloud Agents

Cloud Agents Public URL:	https://qagpublic.qg1.apps.qualys.in

- You must provide Qualys users with the privileges required to enable the integration using the Manager role, the Unit Manager role, or both. You can modify the Manager role to enable read-only access permission if needed. (Refer to the Qualys documentation for details about User Roles Comparison (Vulnerability Management).)
- You must enable Vulnerability Management (VM), Cloud Agent (CA), and Asset View (AV) for Qualys users.
- You must enable Qualys API and Qualys EC2 API access for Qualys users.

Make sure that **Azure VM Information** is visible in Qualys.



Azure VM Information

General:

VM ID:
VM Name:
Platform (OS Type):
Size:
Image Offer:
Image Publisher:
Image Version:
Subscription ID:
Location:
Resource Group Name:
[redacted]

Network:

Private IP Address:
Public IP Address:
MAC Address:
Subnet:
[redacted]

Azure VM Tags:

Test VM: AZURE QUALYS CENTOS

2. Set up Qualys Integration on Prisma Cloud.

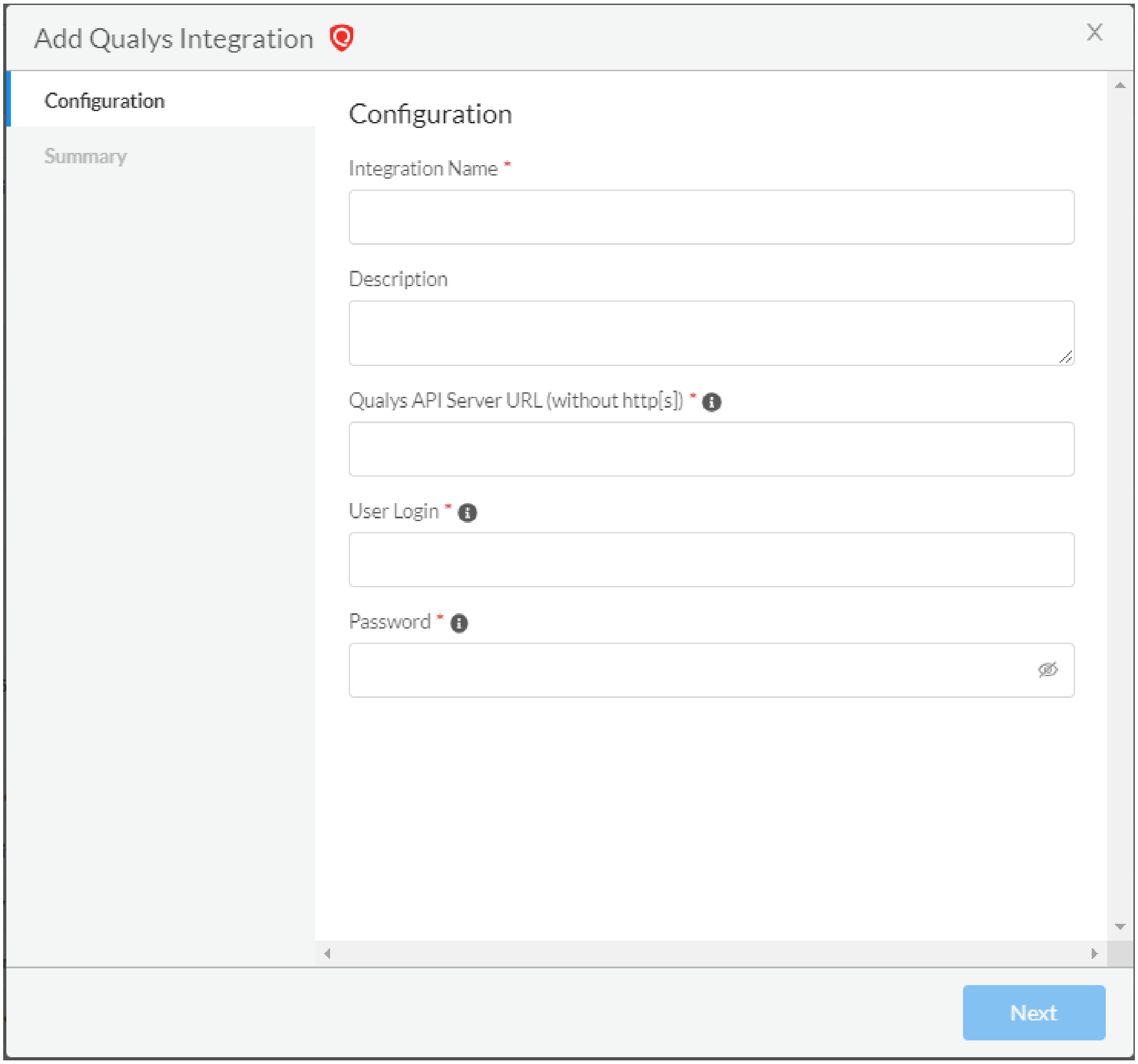
    1. Select **Settings Integrations**. **Add Integration Qualys**. A modal wizard opens where you can add the Qualys integration.

    2. Enter an **Integration Name** and **Description.**

    3. Enter the **Qualys API Server URL (without http[s])**.

        This is the **API URL** for your Qualys account. When you enter this URL, (http(s)) or the port (:443).

    4. Enter your Qualys **User Login** and **Password**.



5. **Test** and **save** the integration.

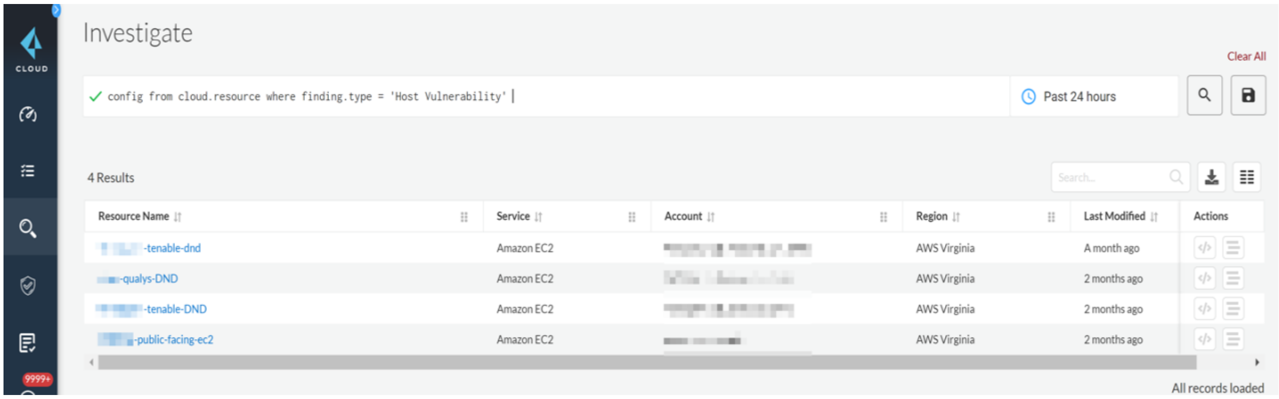
   The integration will be listed on the Integrations page, where you can enable, disable, or delete integrations as needed.

View Qualys host vulnerability data in Prisma Cloud.

After you configure Prisma Cloud with access to the Qualys findings, you can use RQL queries for visibility into the host vulnerability information collected by Qualys.

Use **Config Query** for visibility for host vulnerabilities.

```
config from cloud.resource where finding.type = 'Host Vulnerability'
```



Investigate

Clear All

```
config from cloud.resource where finding.type = 'Host Vulnerability'
```

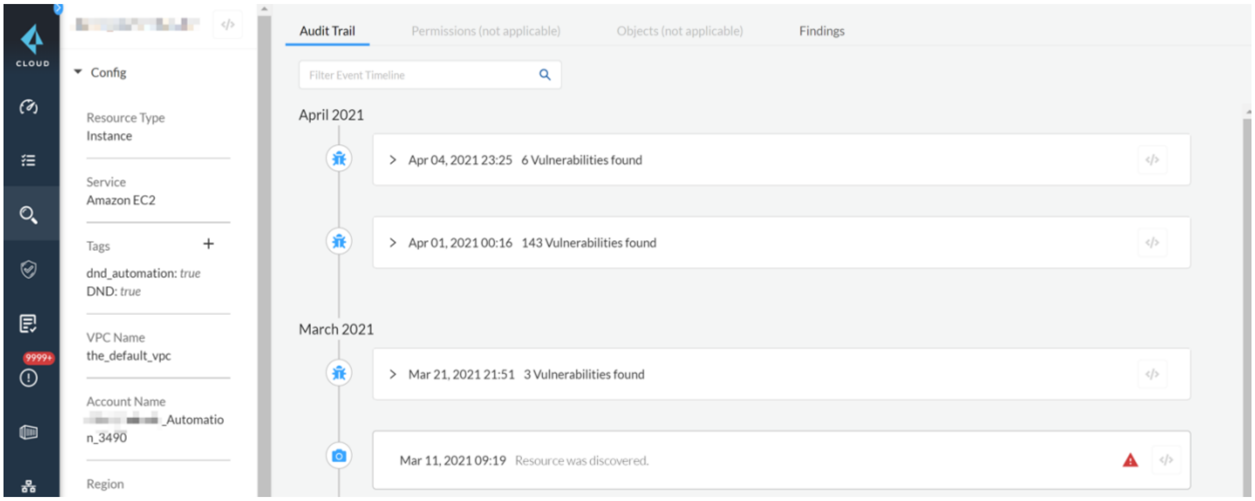
Past 24 hours

4 Results

Resource Name	Service	Account	Region	Last Modified	Actions
[redacted]-tenable-dnd	Amazon EC2	[redacted]	AWS Virginia	A month ago	
[redacted]-qualys-DND	Amazon EC2	[redacted]	AWS Virginia	2 months ago	
[redacted]-tenable-DND	Amazon EC2	[redacted]	AWS Virginia	2 months ago	
[redacted]-public-facing-ec2	Amazon EC2	[redacted]	AWS Virginia	2 months ago	

All records loaded

Click View the **Audit Trail** see the CVE numbers.



[redacted]

Config

Resource Type
Instance

Service
Amazon EC2

Tags
dnd_automation: *true*
DND: *true*

VPC Name
the_default_vpc

Account Name
[redacted]_Automation_3490

Region

April 2021

Apr 04, 2021 23:25 6 Vulnerabilities found

Apr 01, 2021 00:16 143 Vulnerabilities found

March 2021

Mar 21, 2021 21:51 3 Vulnerabilities found

Mar 11, 2021 09:19 Resource was discovered.

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.

Network Query

```
network from vpc.flow_record where dest.resource IN ( resource where finding.type = 'Host Vulnerability' )
```

3. 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 username, password, and the URL for the Qualys service in the following Curl examples:

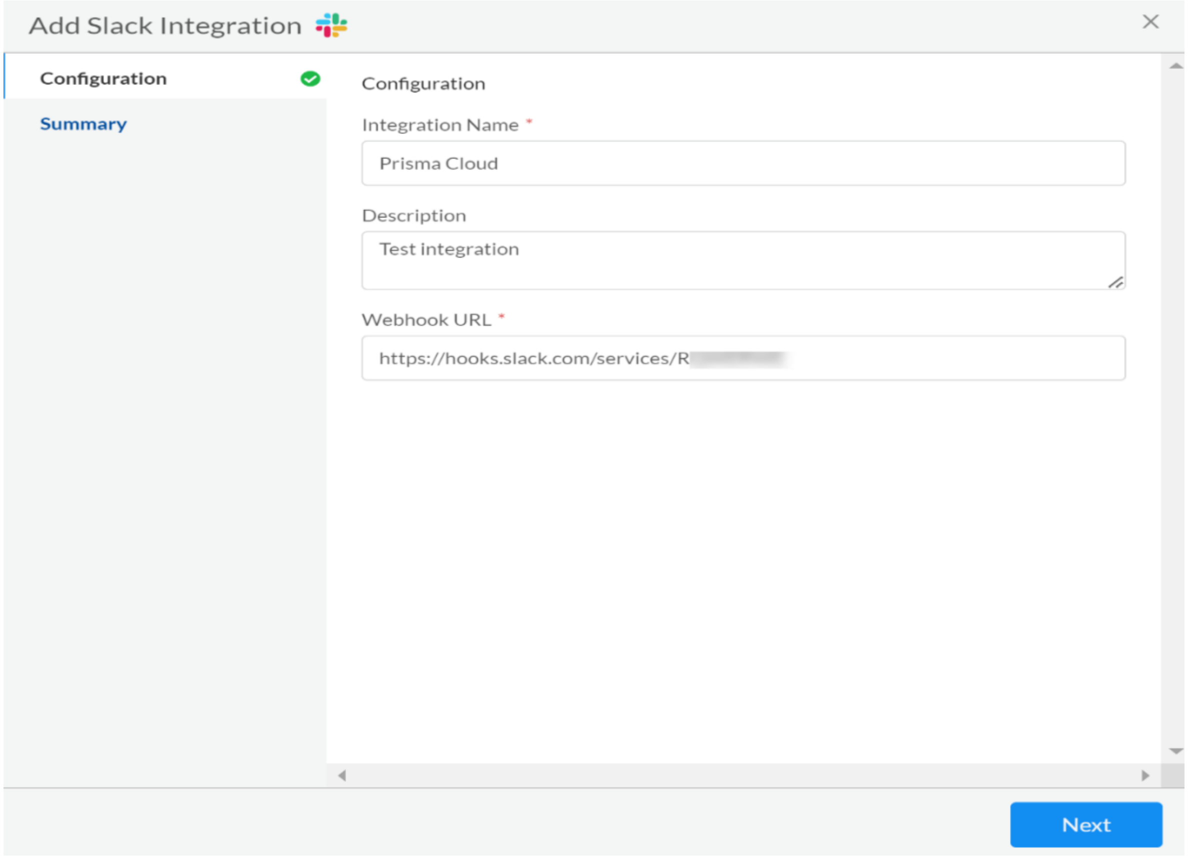
```
curl -H “X-Requested-With: Curl Sample” -u “Username:Password” “https://qualysapi.qg1.apps.qualys.in/api/2.0/fo/scan/?action=list&echo_request=1”


curl -k “https://qualysapi.qg1.apps.qualys.in/msp/asset_group_list.php” -u “Username:Password”


curl -k -H “X-Requested-With:curl” “https://qualysapi.qg1.apps.qualys.in/api/2.0/fo/scan/stats/?action=list” -u “Username:Password”
```

Configure the Slack Integration on Prisma Cloud

After you create the webhook, you can now configure the Slack integration on Prisma Cloud.

Log in to Prisma Cloud to enable the integration.

1. Select **Settings Integrations**.
2. Set the **Add Integration** to **Slack**.
3. Enter a name and a description for this integration.
4. Enter the **WebHook URL**.



Configuration

Integration Name *

Prisma Cloud

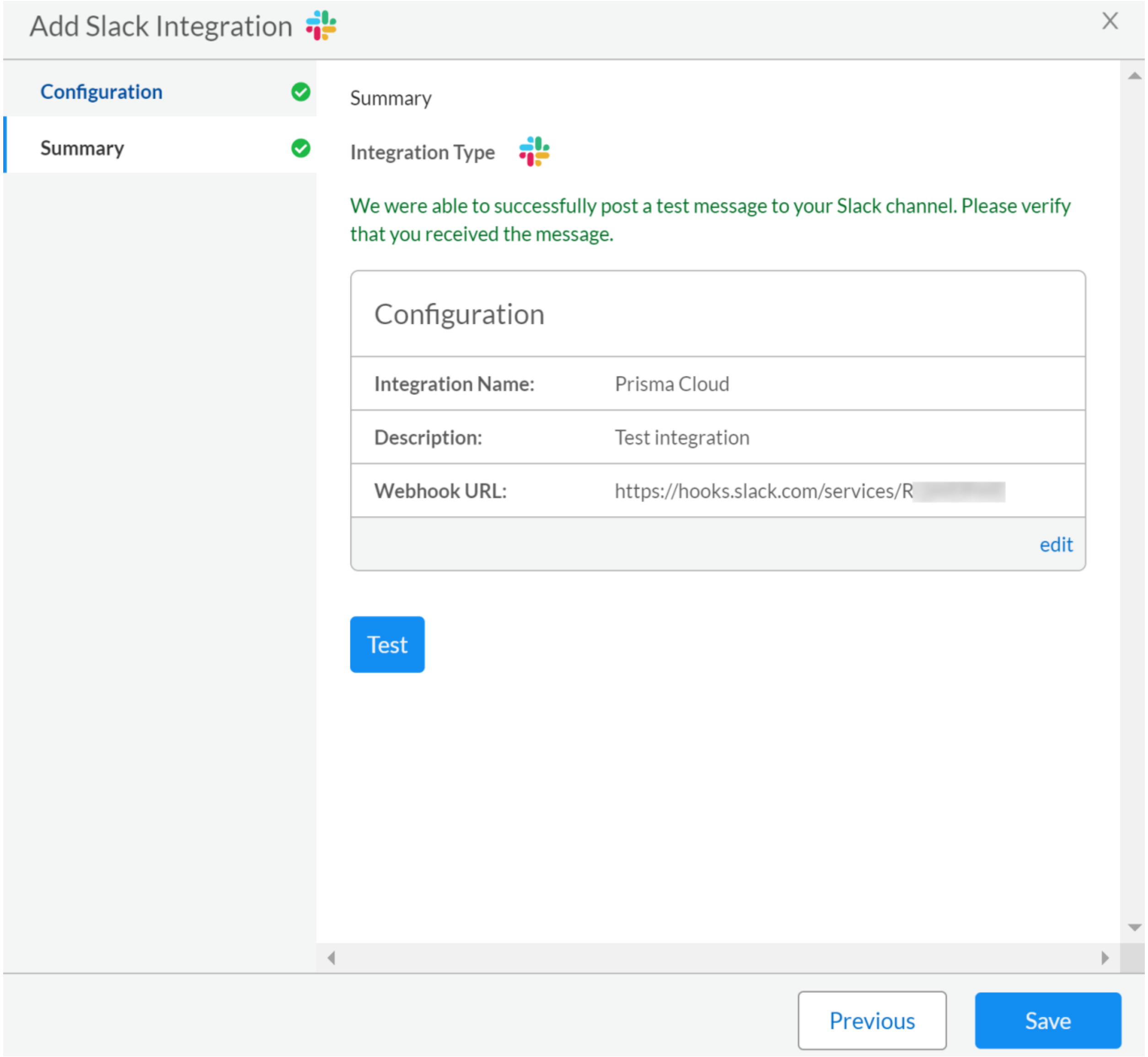
Description

Test integration

Webhook URL *

https://hooks.slack.com/services/R[redacted]

5. Click **Next** and then **Test**.



We were able to successfully post a test message to your Slack channel. Please verify that you received the message.

Configuration

Integration Name:	Prisma Cloud
Description:	Test integration
Webhook URL:	https://hooks.slack.com/services/R[redacted]

6. **Save** the integration. After you set up the integration successfully, you can use the Get Status link in **Settings Integrations** to periodically check the integration status.

SPLUNK INTEGRATION

Step 1 - Set up Splunk HTTP Event Collector (HEC) to view alert notifications from Prisma Cloud in Splunk. Select > **Settings** > **Data inputs** > **HTTP Event Collector** and make sure you see HEC added in the list and that the status shows that it is **Enabled.**

Step 2 - Set up the Splunk integration in Prisma Cloud.

1. Log in to Prisma Cloud.

2. Select **Settings Integrations**.

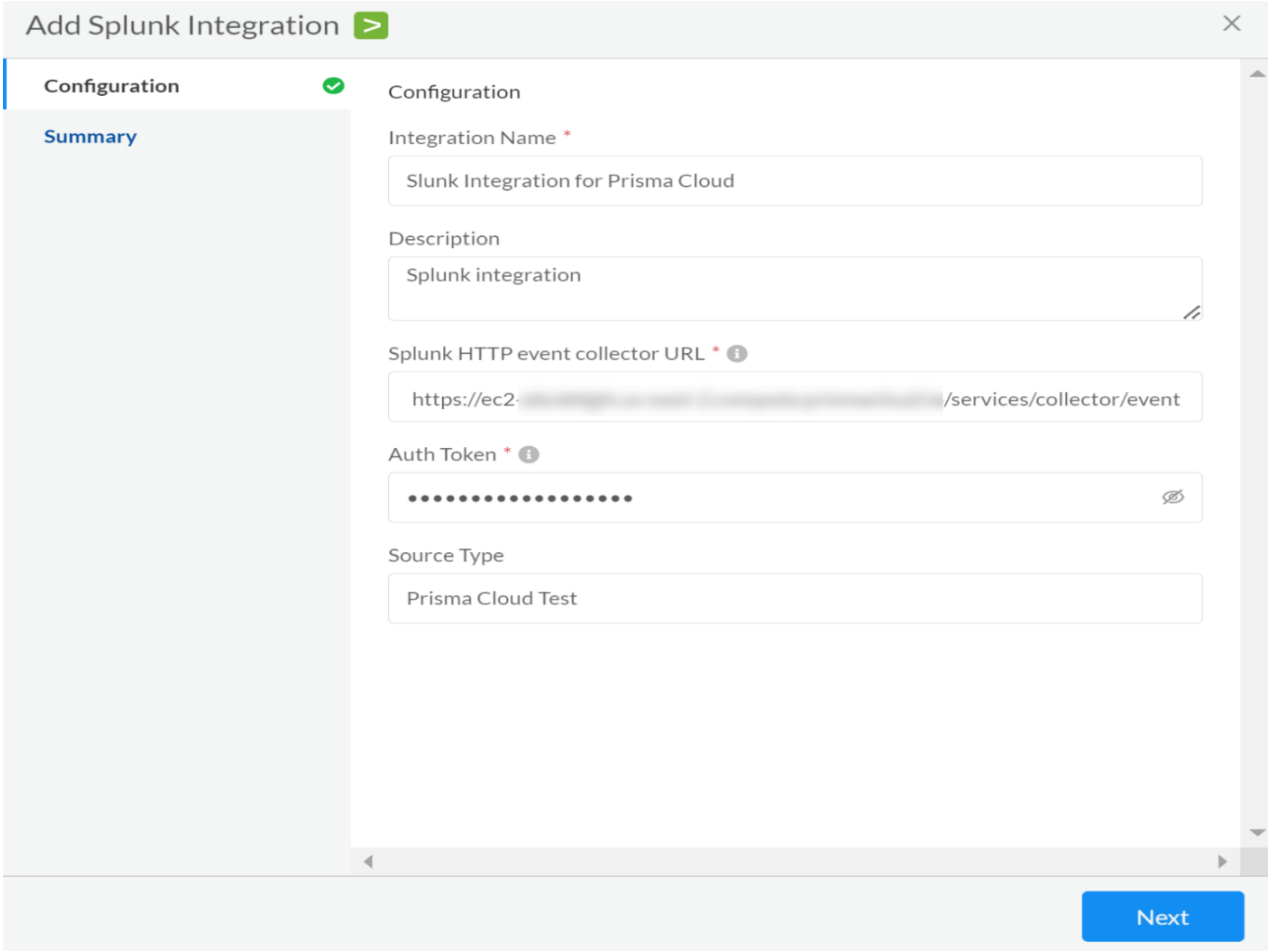
3. Set the **Add Integration** to **Splunk**.

4. Enter an **Integration Name**, optionally, a **Description**.

5. Enter the **Splunk HEC URL** that you set up earlier.

The Splunk HEC URL is a Splunk endpoint for sending event notifications to your Splunk deployment. You can either use HTTP or HTTPS for this purpose. Since Prisma Cloud sends data about an alert or error in JSON format, make sure to include **/services/collector** endpoint as part of the Splunk HEC URL.

6. Enter **Auth Token**.
The integration uses token-based authentication between Prisma Cloud and Splunk to authenticate connections to Splunk HEC. A token is a 32-bit number that is presented in Splunk.



Configuration

Integration Name *
Slunk Integration for Prisma Cloud

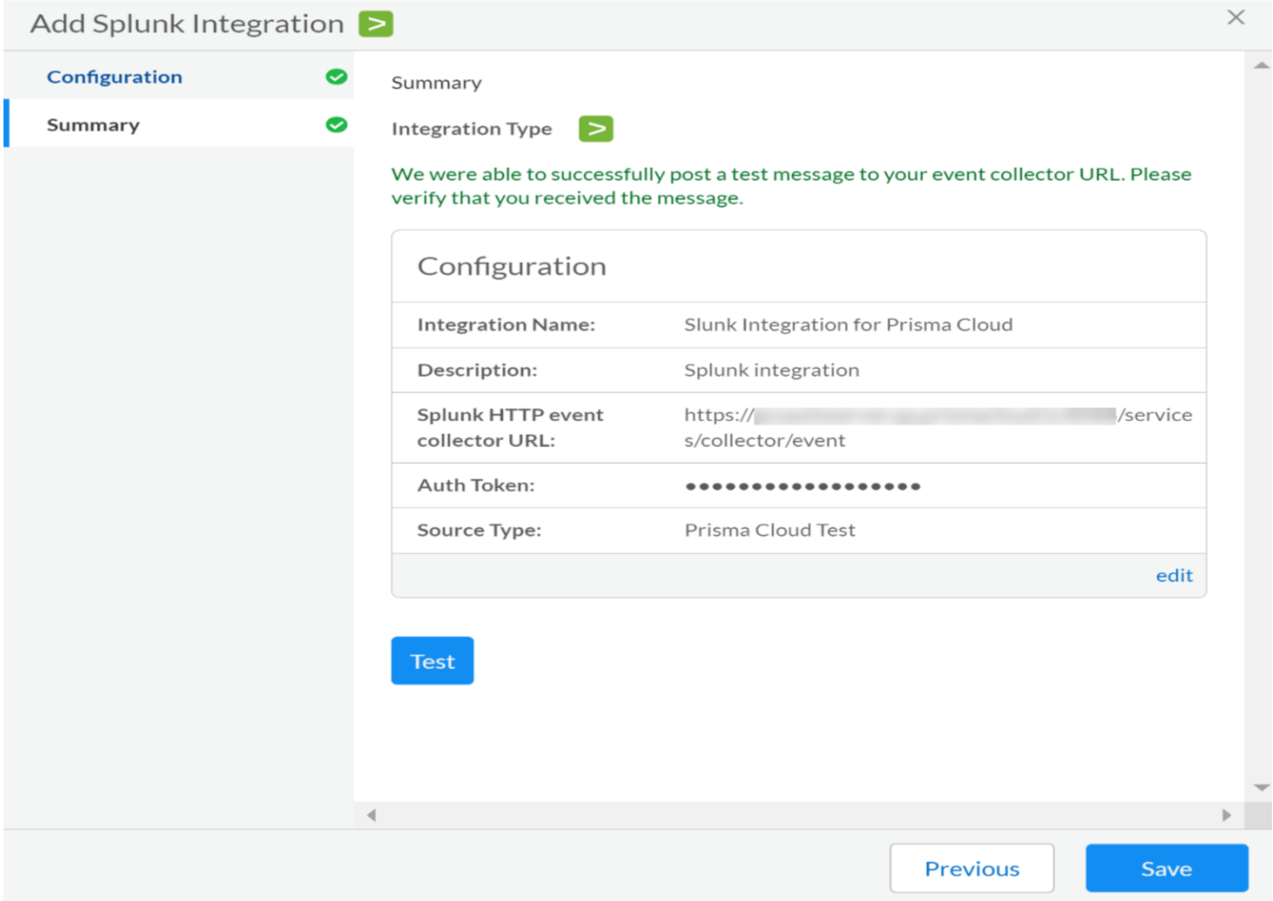
Description
Splunk integration

Splunk HTTP event collector URL *
https://ec2-[redacted]/services/collector/event

Auth Token *
•••••••••••••••••••

Source Type
Prisma Cloud Test

7. Click **Next** and then **Test**.



Add Splunk Integration

Summary

Integration Type

We were able to successfully post a test message to your event collector URL. Please verify that you received the message.

Configuration

Integration Name:	Slunk Integration for Prisma Cloud
Description:	Splunk integration
Splunk HTTP event collector URL:	https://[redacted]/services/collector/event
Auth Token:	••••••••••••••••••
Source Type:	Prisma Cloud Test

8. Save the integration.

TENABLE INTEGRATION

Step 1- Tenable.io provides API access to assets and their vulnerability information. Configure the Tenable account to use the Tenable AWS, Azure, and GCP connectors. You cannot identify the cloud resource without these connectors.

The Tenable API requires an access key and a secret key to be added to the request header. Generate an access key and secret key for each user on the Tenable.io app. Also, ensure that the Tenable role you are using to enable this integration has administrator permissions that include vulns-request-export and assets-request-export API access.

Step 2. Set up Tenable integration on Prisma Cloud.

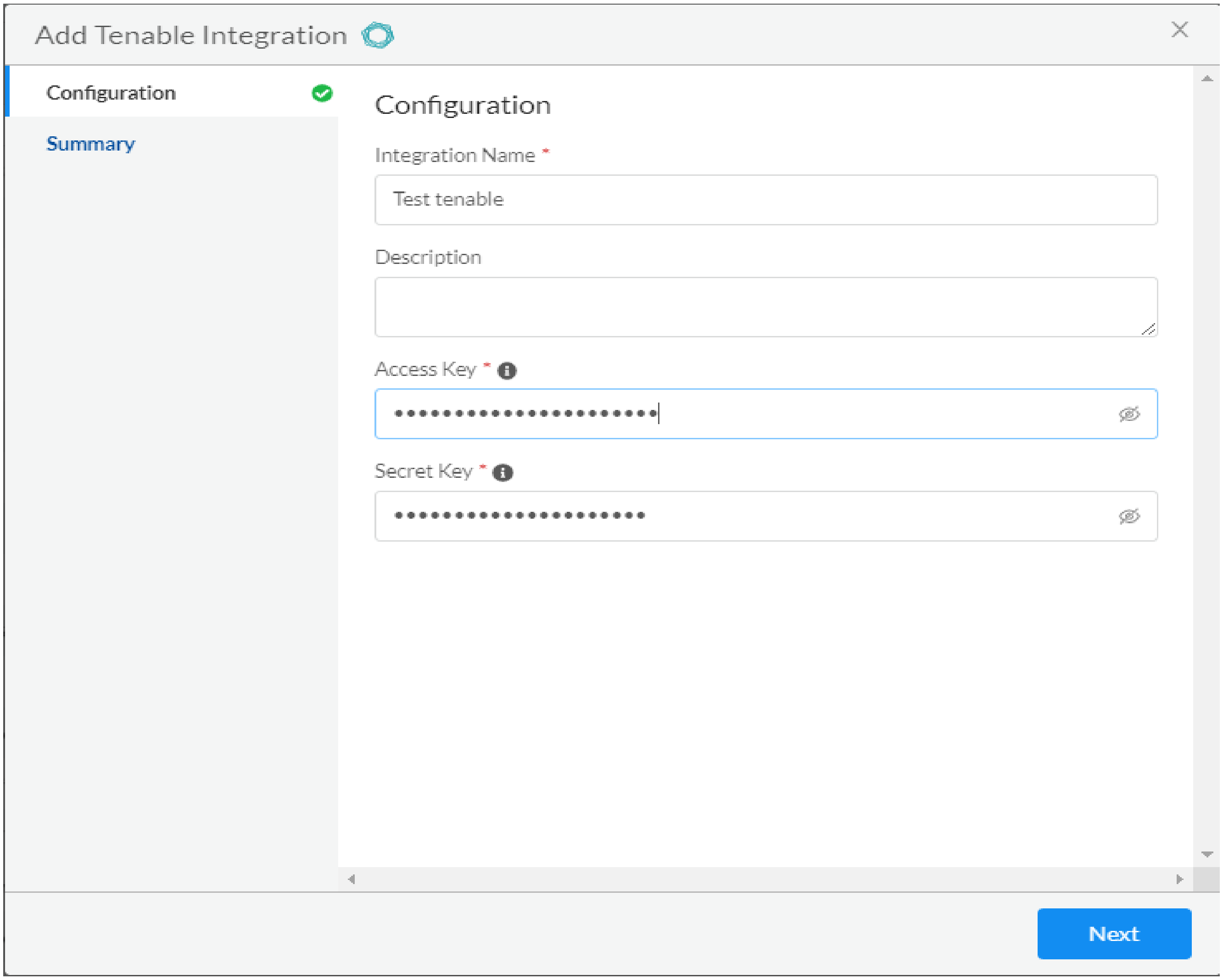
1. Login to Prisma Cloud.

2. Select **Settings** > **Integrations**.

3. Set the **Add Integration** to **Tenable**.

4. Enter **Name** and **Description**.

5. Enter the **Access Key** and the **Secret Key** that are generated in Tenable.io.



Add Tenable Integration

Configuration

Integration Name *

Test tenable

Description

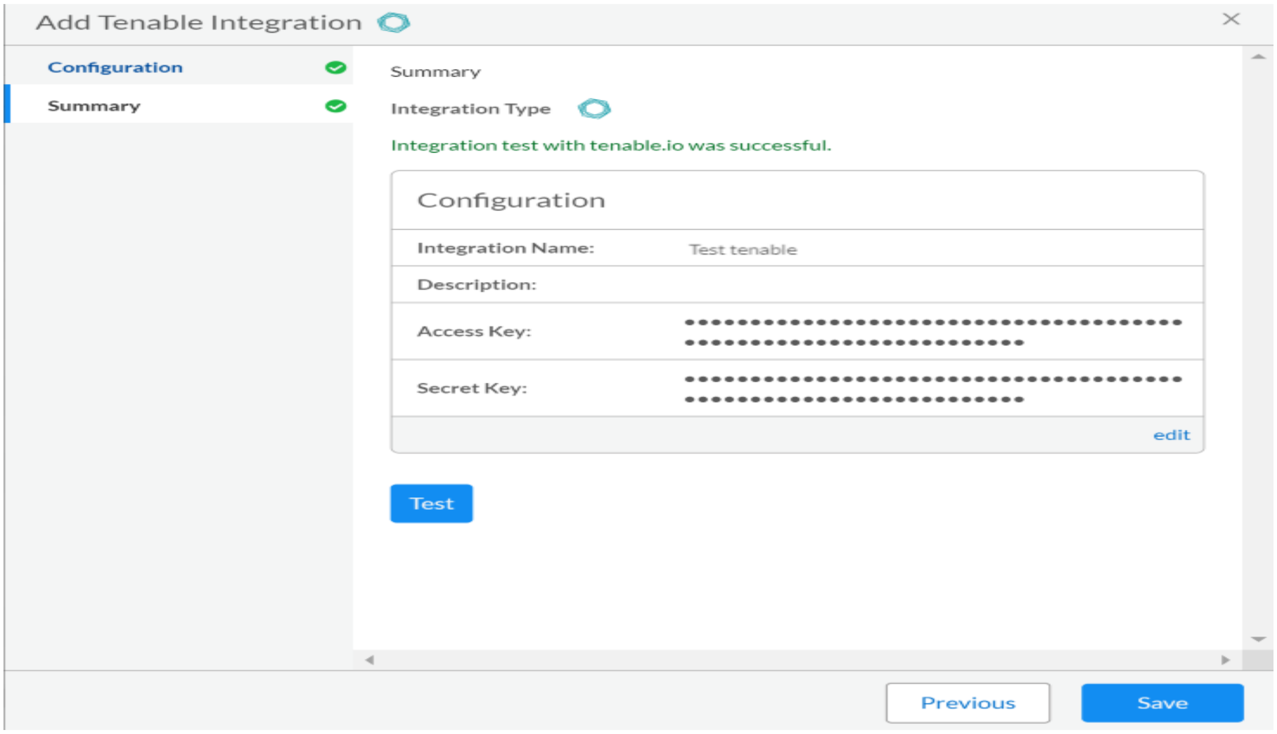
Access Key *

••••••••••••••••••••••

Secret Key *

•••••••••••••••••••••

6. Click **Next** and then **Test t**he integration.



Summary

Integration Type

Integration test with tenable.io was successful.

Configuration

Integration Name:	Test tenable
Description:	
Access Key:	•••
Secret Key:	•••

7. Review the Summary and **Save** the integration.

8. Navigate to **Alert Summary** and choose **Host Vulnerability** to see details.

WEBHOOK INTEGRATION

Step 1 - Obtain your Webhook URL.

If you have additional details that you want to include in the payload to enable additional security or to verify the authenticity of the request, you can include these as key-value pairs in a custom header.

Step 2 - Set up webhooks as an integration channel on Prisma Cloud.

If you have a firewall or cloud Network Security Group between the internet and webhooks, you need to ensure network reachability and Enable Access to the Prisma Cloud Console.

1. Log in to Prisma Cloud and select **Settings >Integrations**.

2. **Add Integration > Webhook**.

3. Enter **Integration Name** and your **Webhook URL**.

   You can also provide a **Description** of the integration for your records.

4. Learn about your customization options.

- Add custom **HTTP Headers** as key-value pairs.

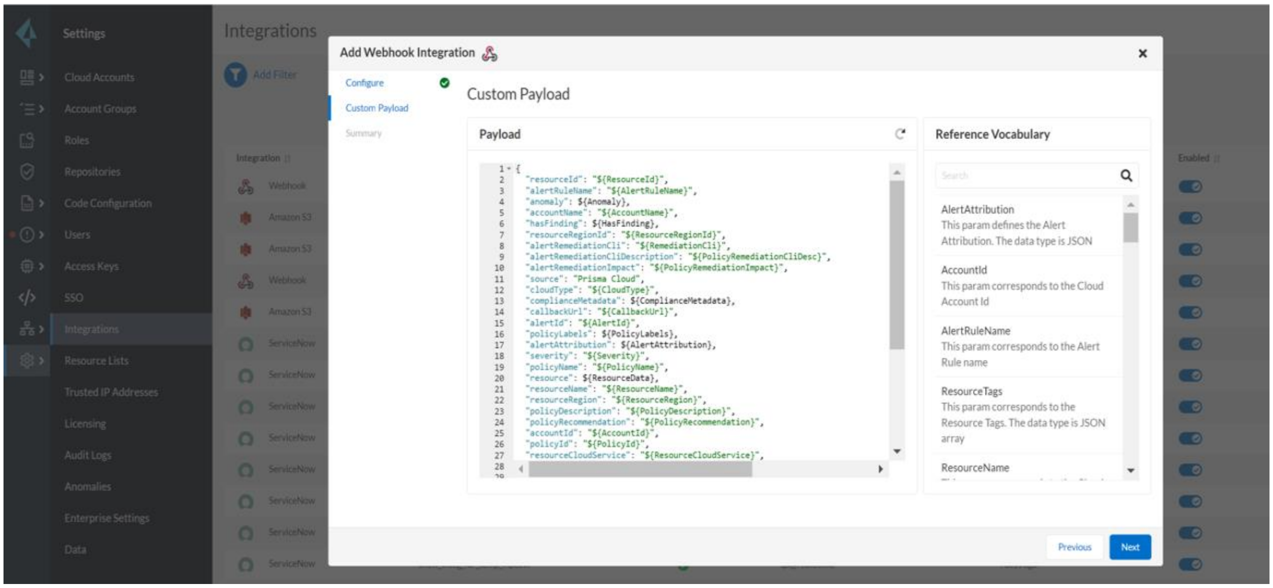
  You can include an authentication token in the custom header. The integration includes Content-Type as a default header, and you cannot edit it.

- Use the JSON editor to modify the JSON data in the alert payload. You can review the existing payload and modify the key and value pairs to suit the implementation needs for the subscribing webhook client. The JSON editor includes the reference vocabulary for a brief description of each key.

  1. Enable **Custom Payload**.

  2. Click **Next** to review the custom payload format.

  The alert payload information including the key and the value is displayed onscreen. You can revise the payload to meet your integration needs.



Custom Payload

Payload

```
{
  "resourceId": "${ResourceId}",
  "alertRuleName": "${AlertRuleName}",
  "anomaly": ${Anomaly},
  "accountName": "${AccountName}",
  "hasFinding": ${HasFinding},
  "resourceRegionId": "${ResourceRegionId}",
  "alertRemediationCli": "${RemediationCli}",
  "alertRemediationCliDescription": "${PolicyRemediationCliDesc}",
  "alertRemediationImpact": "${PolicyRemediationImpact}",
  "source": "Prisma Cloud",
  "cloudType": "${CloudType}",
  "complianceMetadata": ${ComplianceMetadata},
  "callbackUrl": "${CallbackUrl}",
  "alertId": "${AlertId}",
  "policyLabels": ${PolicyLabels},
  "alertAttribution": ${AlertAttribution},
  "severity": "${Severity}",
  "policyName": "${PolicyName}",
  "resource": ${ResourceData},
  "resourceName": "${ResourceName}",
  "resourceRegion": "${ResourceRegion}",
  "policyDescription": "${PolicyDescription}",
  "policyRecommendation": "${PolicyRecommendation}",
  "accountId": "${AccountId}",
  "policyId": "${PolicyId}",
  "resourceCloudService": "${ResourceCloudService}",
```

Reference Vocabulary

AlertAttribution
This param defines the Alert Attribution. The data type is JSON

AccountId
This param corresponds to the Cloud Account Id

AlertRuleName
This param corresponds to the Alert Rule name

ResourceTags
This param corresponds to the Resource Tags. The data type is JSON array

ResourceName

5. Select **Next** to review the integration summary.

6. **Test** and **Save Integration**

INTEGRATION WITH SERVICENOW

Learn how to integrate Prisma™ Cloud with ServiceNow to help you prioritize and respond to Security incidents on ServiceNow.

Integrate Prisma™ Cloud with ServiceNow and get automatically notified about Prisma Cloud alerts through ServiceNow tickets to prioritize incidents and vulnerabilities that impact your business. Prisma Cloud integrates with the ITSM module (incident table), the Security Incident Response module (sn_si_incident table), and the Event Management modules (em_event table) on ServiceNow to generate alerts in the form of ITSM Incident, Security Incident, and Event tickets. After you enable the integration, when Prisma Cloud scans your cloud resources and detects a policy violation, it generates an alert and pushes it to ServiceNow as a ticket. When you dismiss an alert on Prisma Cloud, Prisma Cloud sends a state change notification to update the ticket status on ServiceNow. This integration seamlessly fits in to the existing workflows for incident management (ITSM), security operations management (Security Incident Response) or event management for your organization.

The Prisma Cloud integration with ServiceNow is qualified with the most recent cloud-based GA versions of ServiceNow; the on-premise versions are not supported.

Note: If you are using a ServiceNow developer instance, make sure that it is not hibernating.

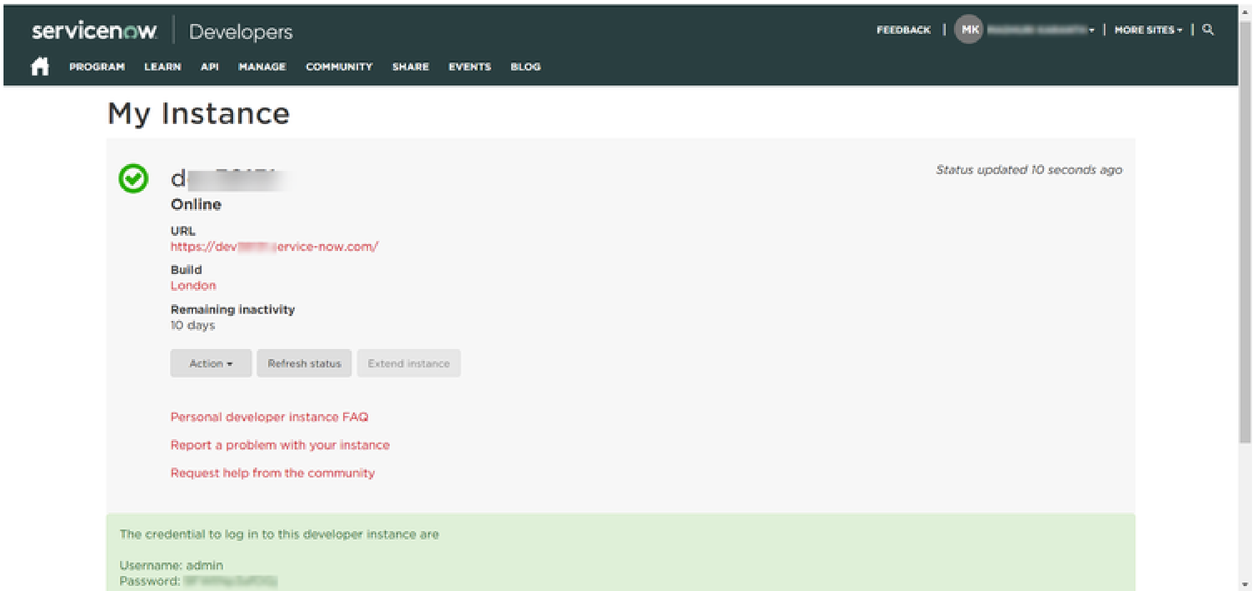
1. Set Up Permissions on ServiceNow
2. Enable the ServiceNow Integration on Prisma Cloud
3. Set up Notification Templates
4. View Alerts

If you see errors, review how to Interpret Error Messages.

Step 1- Prerequisites for the Prisma Cloud and ServiceNow Integration.

1. You must have permissions to create a local user account on ServiceNow.

Create a Username and password that are local on the instance itself. A local user account is a requirement because the ServiceNow web services cannot authenticate against an LDAP or SSO Identity provider and it is unlike the authentication flow that ServiceNow supports for typical administrative users who access the service using a web browser.Refer to the ServiceNow documentation for more information.



My Instance

d[redacted]

Online

Status updated 10 seconds ago

URL
https://dev[redacted]ervice-now.com/

Build
London

Remaining inactivity
10 days

Personal developer instance FAQ
Report a problem with your instance
Request help from the community

The credential to log in to this developer instance are

Username: admin
Password: [redacted]

2. Review the ServiceNow roles required.

Prisma Cloud has verified that the following roles provide the required permissions. If your implementation has different roles and RBAC mechanisms, work with your ServiceNow administrator.

New York, Orlando, and Paris

- (Optional) personalize for accessing tables.
- Personalize role is recommended to support type-ahead fields in notification templates for ServiceNow on Prisma Cloud. With this permission, when you enter a minimum of three characters in a type-ahead field, this role enables you to view the list of available options. If you do not enable personalize permissions, you must give table specific read-access permissions for type-ahead inputs.
- evt_mgmt_integration basic role has create access to the Event [em_event] and Registered Nodes [em_registered_nodes] tables to integrate with external event sources.
- itil role is required for the incident table actions.
- sn_si.basic role is required for the sn_si.incident security incident table actions.

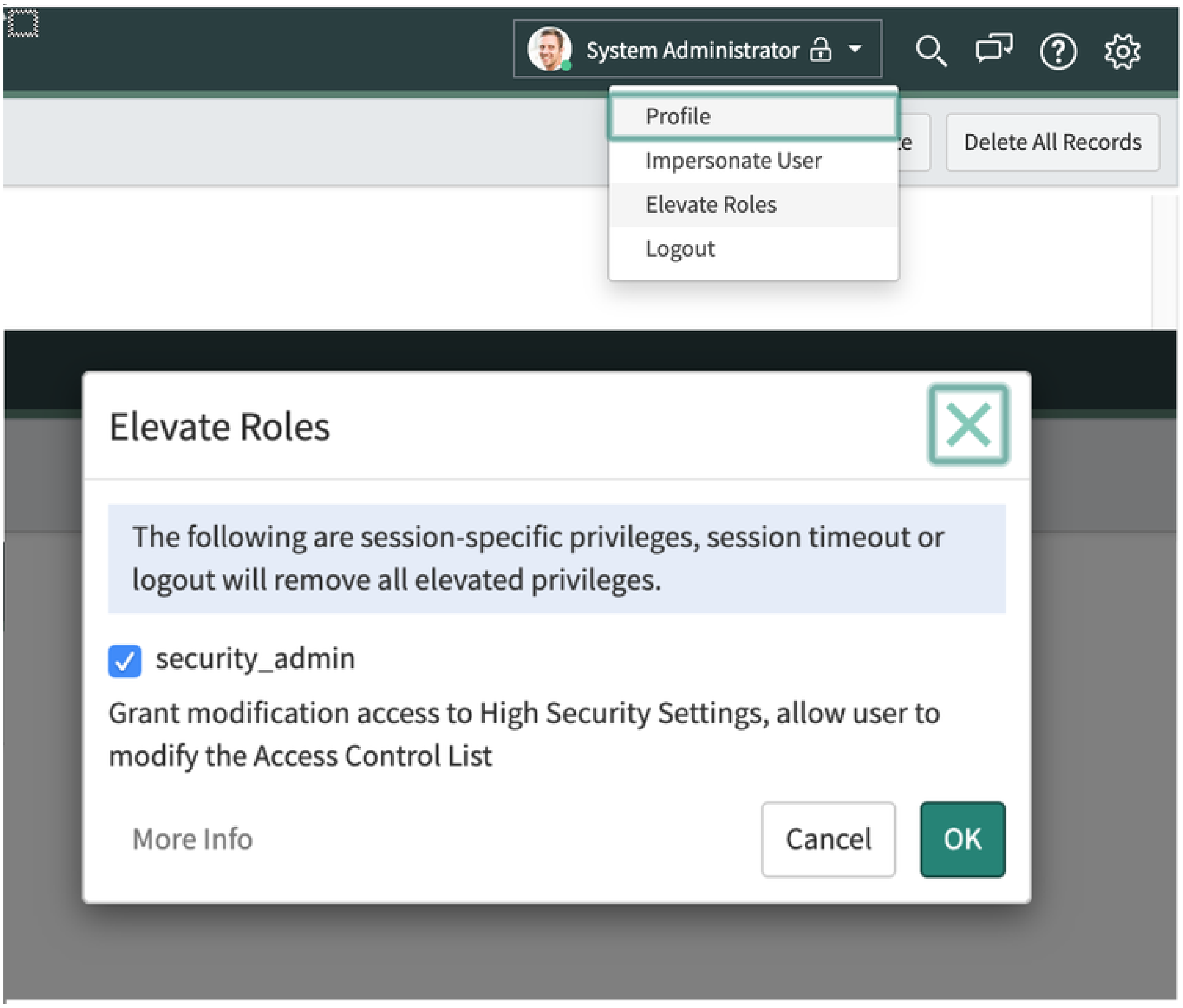
3. For the user you added earlier, create a custom role with the permissions listed above.

These permissions are required to create tickets and access the data in the respective ITSM, Events, and Security Incident Response tables and fields on ServiceNow.

Prisma Cloud needs access to the Plugins (V_plugin), Dictionary (sys_dictionary), and Choice Lists (sys_choices) tables to fetch data from the ServiceNow fields. You can view this information in the ServiceNow notification templates that enable you to customize Prisma Cloud alerts in ServiceNow.

1. Select "User Administration > Roles" to create a new role and assign it to the local administrative user you created earlier.
2. Pick a table, such as the Plugins table, and select the menu (“hamburger”) icon next to a table column header to "Configure > Table".

3. Elevate the role to security_admin to enable modification of the access control list (ACL).



Elevate Roles

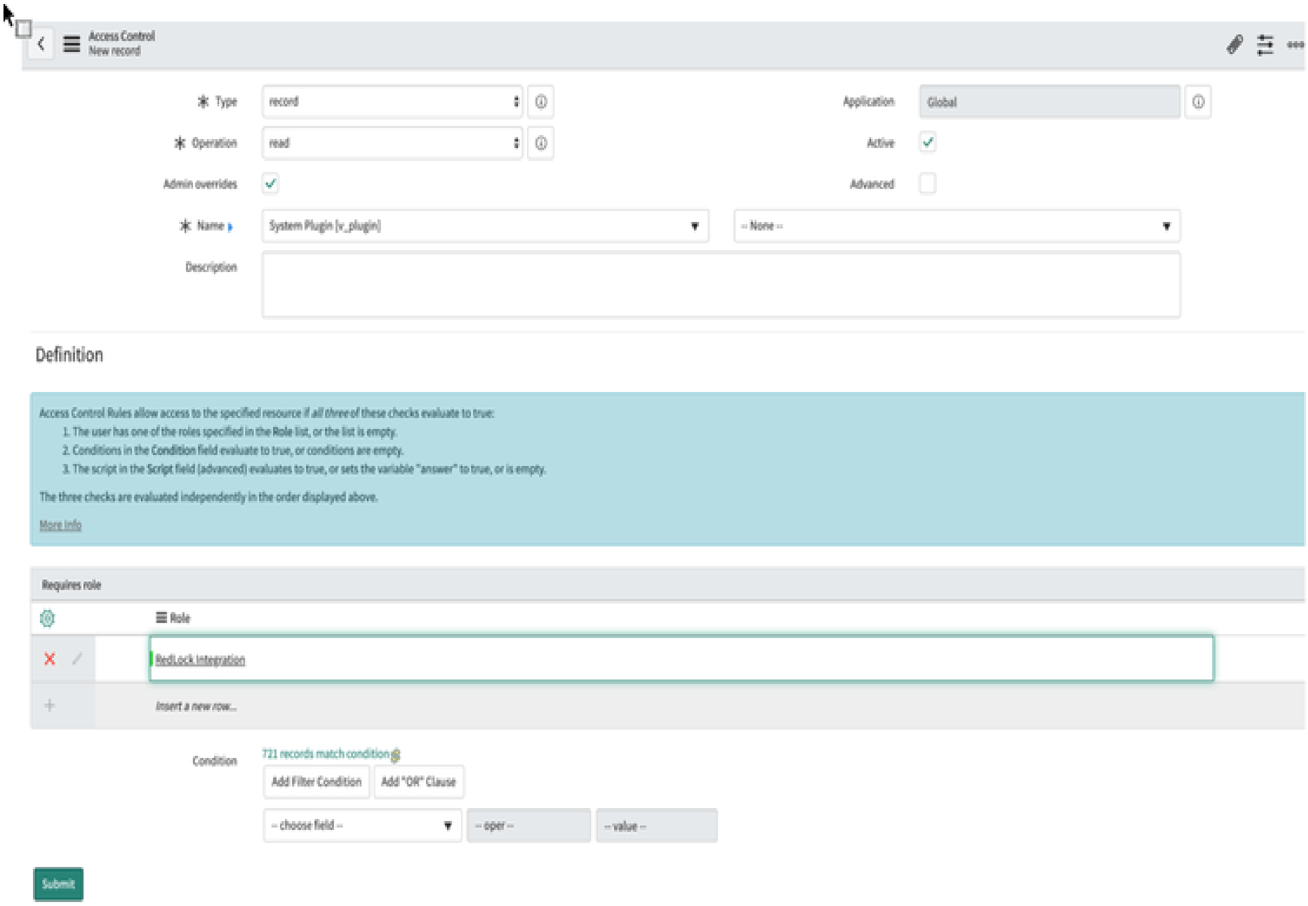
The following are session-specific privileges, session timeout or logout will remove all elevated privileges.

☑ security_admin

Grant modification access to High Security Settings, allow user to modify the Access Control List

4. Select "Access Controls > New".

5. Set Operation to Read and assign this permission to the role.



Access Control
New record

* Type	record	Application	Global
* Operation	read	Active	☑
Admin overrides	☑	Advanced	☐
* Name	System Plugin [v_plugin]	-- None --	
Description			

Definition

Access Control Rules allow access to the specified resource if *all three* of these checks evaluate to true:

1. The user has one of the roles specified in the **Role** list, or the list is empty.
2. Conditions in the **Condition** field evaluate to true, or conditions are empty.
3. The script in the **Script** field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

More info

Requires role

Role
RedLock Integration
Insert a new row...

Condition: 721 records match condition

6. Enable permissions for the remaining tables and assign them to the same role.

Verify that all three tables—Plugins (V_plugin), Dictionary (sys_dictionary), and Choice Lists (sys_choices) have the role and the required permission especially if you have defined field-level ACL rules to restrict access to objects in your ServiceNow implementation.

4. You must be familiar with the fields and field-types in your ServiceNow implementation to set up the Notification templates on Prisma Cloud. Because this knowledge is essential for setting up the mapping of the Prisma Cloud alert payload to the corresponding fields on ServiceNow, you must work with your ServiceNow administrator to successfully enable this integration.

Step 2- Prerequisites for the Security Incident Module

The Security Incident Response plugin is optional but is required if you want to generate Security Incident tickets. To create Security Incident tickets, you must also have the Security Incident Response plugin installed on your ServiceNow instance.

Verify that the Security Incident Response plugin is activated. To activate a plugin you must be ServiceNow administrator; if you do not see the plugin in the list, verify that you have purchased the subscription.

Step 3- Prerequisites for the Event Management Module

The Event Management plugin is optional but is required if you want to generate Event tickets on ServiceNow. To create Event tickets, you must have the Event Management subscription and the plugin installed on your ServiceNow instance.

Verify that the Event Management plugin is activated. To activate a plugin you must be ServiceNow administrator; if you do not see the plugin in the list, verify that you have purchased the subscription.

Enable the ServiceNow Integration on Prisma Cloud

Set up ServiceNow as an external integration on Prisma Cloud.

1. Log in to Prisma Cloud and select "Settings > Integrations > +Add New".
2. Set the Integration Type to ServiceNow.
3. Enter a meaningful Integration Name and a Description.
4. Enter your FQDN for accessing ServiceNow.

   https://www.<yourservicenowinstance>.com

   <yourservicenowinstance>.com/

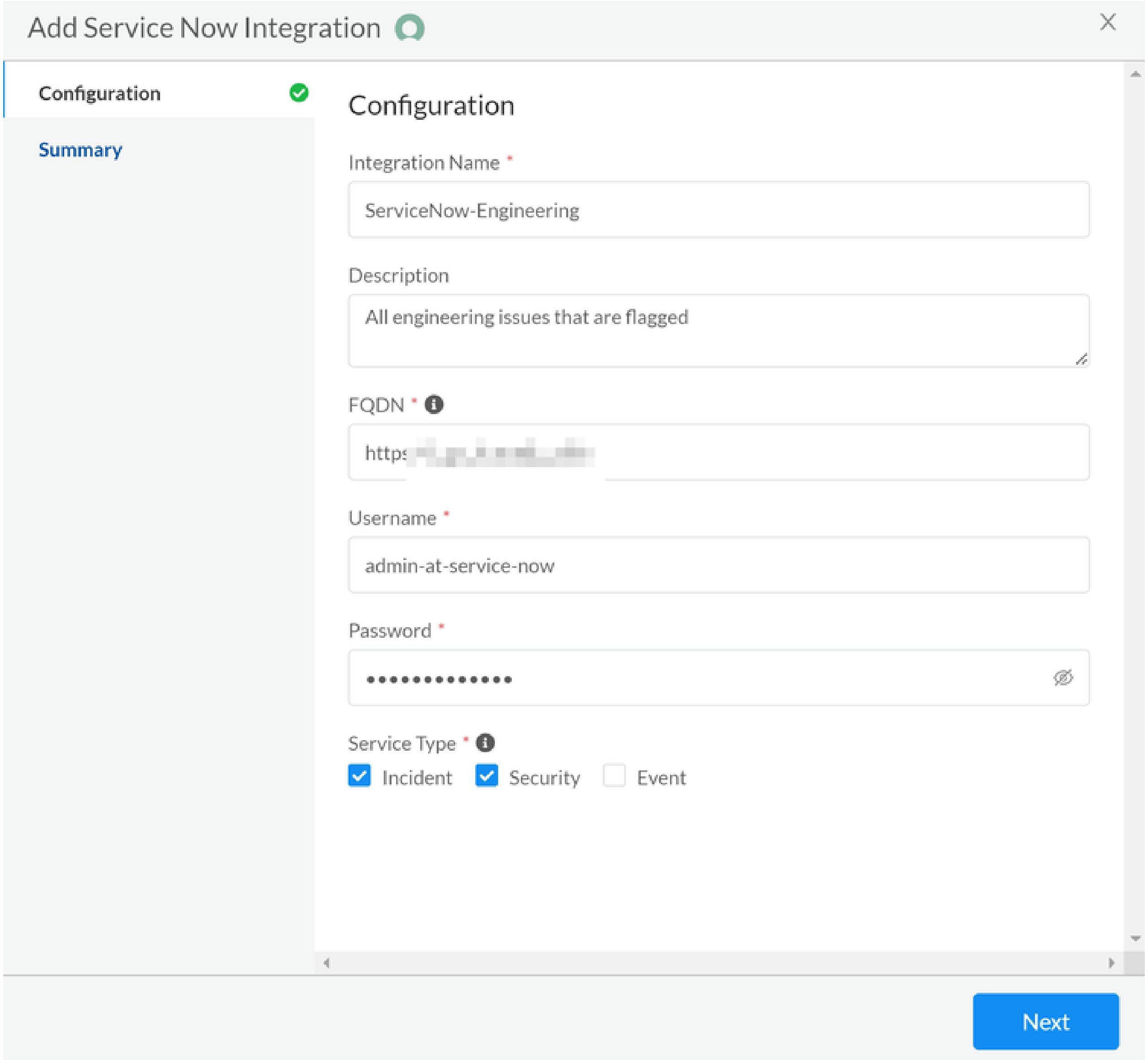
   <yourservicenowinstance>.com/sidedoor.do

   <yourservicenowinstance>.com/login.do

5. Enter the Username and Password for the ServiceNow administrative user account.
   The ServiceNow web services use the SOAP API that supports basic authentication, whereby the administrative credentials are checked against the instance itself and not against any LDAP or SSO Identity provider. Therefore, you must create a local administrative user account and enter the credentials for that local user account here instead of the SSO credentials of the administrator. This method is standard for SOAP APIs that pass a basic authentication header with the SOAP request.

6. Select the Service Type for which you want to generate tickets—Incident, Security, and/or Event.
   You must have the plugin installed to create Security incident tickets or Event tickets; make sure to work with your ServiceNow administrator to install and configure the Security Incident Response module or Event Management module. If you select Security only, Prisma Cloud generates all tickets as Security Incident Response (SIR) on ServiceNow.

7. Click Next and then Test.



Add Service Now Integration

Configuration

Integration Name *
ServiceNow-Engineering

Description
All engineering issues that are flagged

FQDN *
https[redacted]

Username *
admin-at-service-now

Password *
•••••••••••••

Service Type *
☑ Incident ☑ Security ☐ Event

8. Test and save the integration.
   Continue with setting up the notification template, and then verify the status of the integration on "Settings > Integrations".