

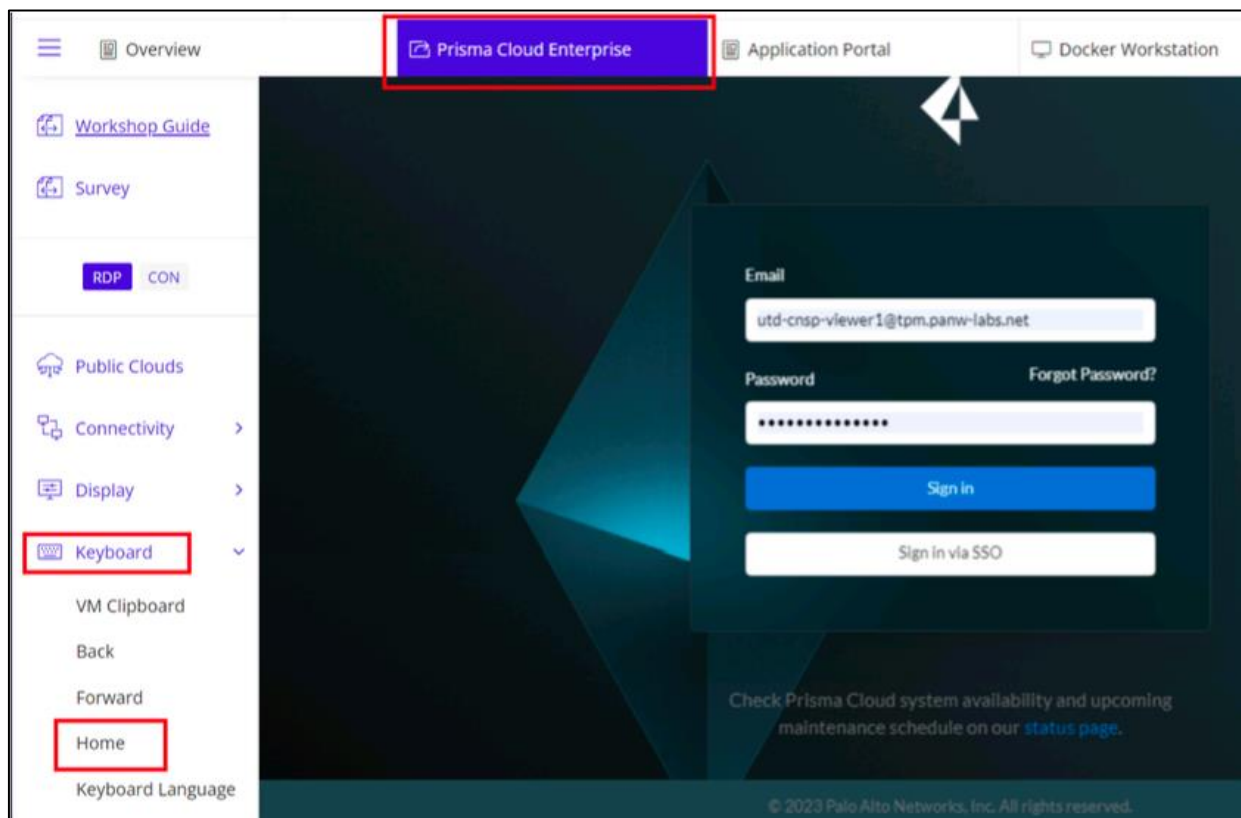
Prisma Cloud is a comprehensive cloud-native security platform with the industry's broadest security and compliance coverage. It protects cloud-native applications, data, networks, computing, storage, users, and higher-level PaaS services across cloud platforms. Prisma Cloud enables Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for comprehensive visibility and threat detection across your organization's hybrid, multi-cloud infrastructure. It dynamically discovers resources as they are deployed and correlates cloud-service-provided data to enable security and compliance insights into your cloud applications and workloads.

In this activity, you will:

- Log in to the Prisma Cloud Lab account
- Learn about the Prisma Cloud console and help center
- Review how to onboard an AWS account on Prisma Cloud tenant
- Review out-of-the-box policies, queries, compliance standards, and remediations

Note: This is a standalone activity and is not dependent on other activities.

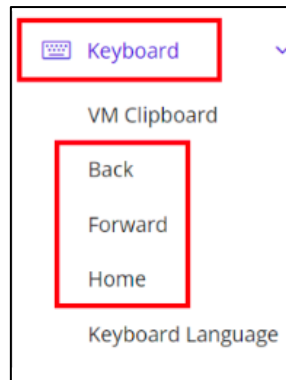
Step 1. Click on the **Prisma Cloud Enterprise** tab to open the demo tenant login.



Step 2. Follow the screen to log in and click the Prisma Cloud icon.

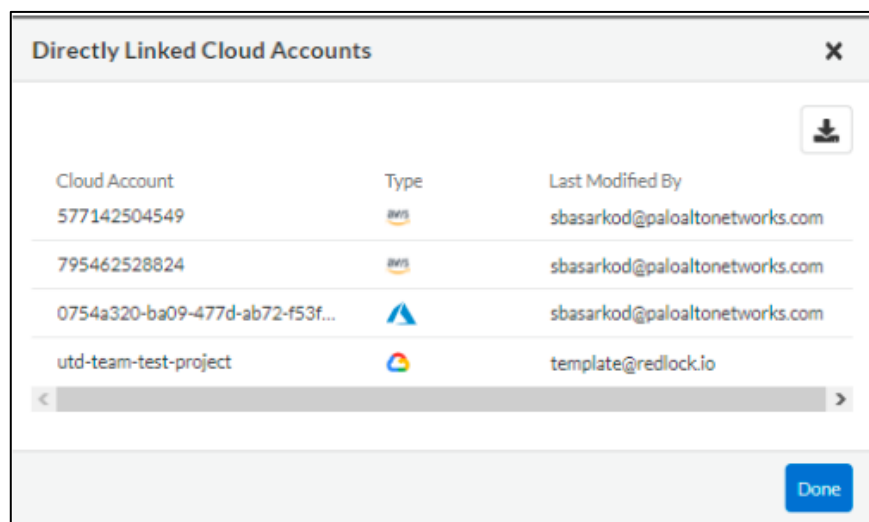
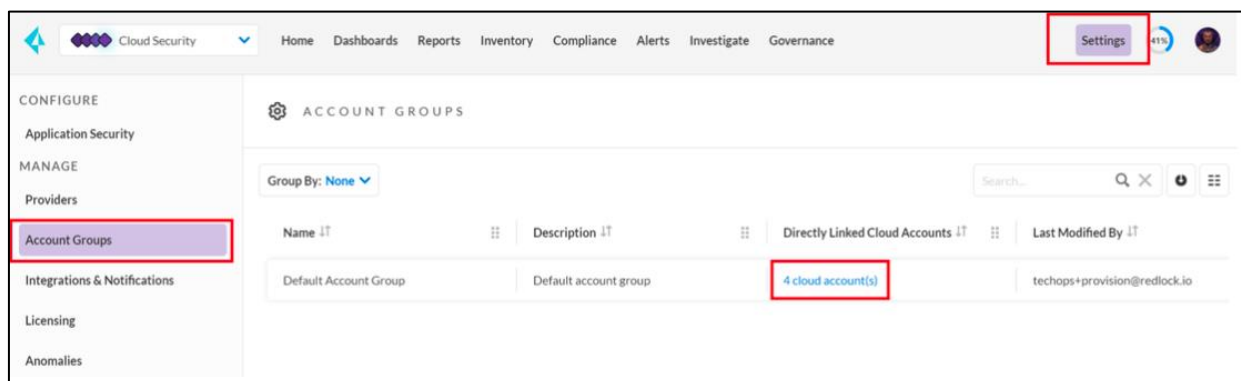
NOTE: If you see a page expired message then **refresh** the web page by clicking on the **Home button** as highlighted in the screen capture.

Step 3. While using the Prisma Cloud console, you can use **CloudShare > Keyboard > Home | Back | Forward** to navigate back and forth.



Step 4. To check the on-boarded public cloud accounts click on the **Settings** the and select **Account Groups**. Click on the **4 Cloud Account(s)** under **Default Account Group**. You can see the public cloud accounts connected to this Prisma Cloud demo account.

NOTE: The screenshots captured in this workshop guide might vary slightly from the actual lab account.



We have already connected AWS, Azure, and GCP accounts to this Prisma Cloud service, and this lab account can be used for testing across all three public cloud providers.

NOTE: The Prisma Cloud Enterprise Edition account used in this lab is read-only, it does not have full access to the Prisma Cloud Service, and access to some functions is denied. This account cannot change the configuration of the associated Prisma Cloud Services.

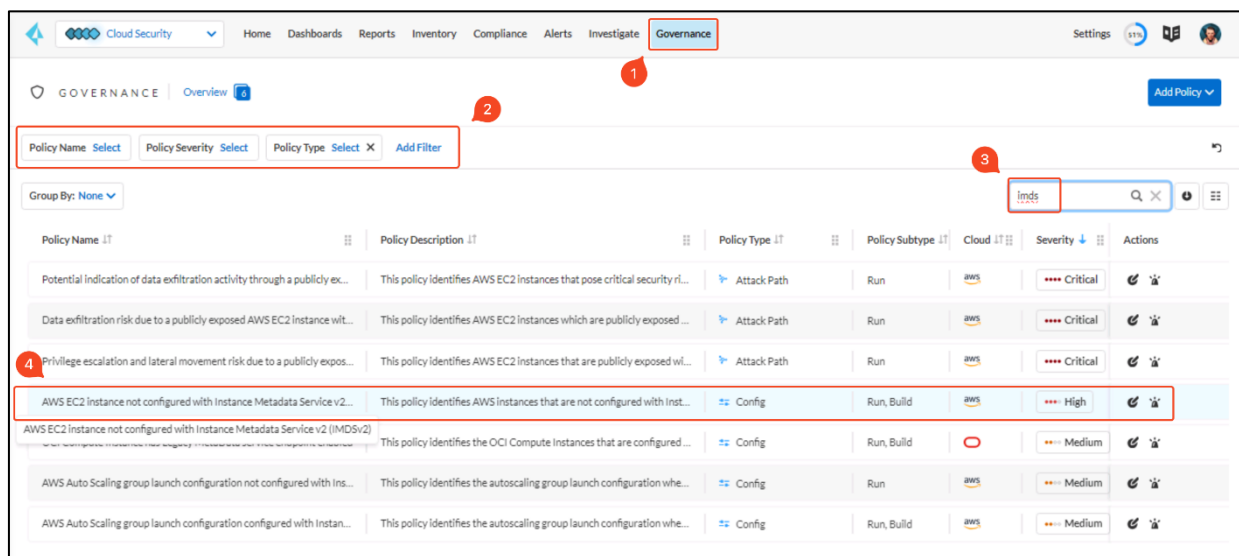
Looking into Prisma Cloud Governance & Policy

In Prisma Cloud, a policy is a set of one or more constraints or conditions that must be adhered to. Prisma Cloud provides predefined policies for configurations and access controls that adhere to established security best practices such as Otoritas Jasa Keuangan (OJK) 38 POJK.03 206, PCI, GDPR, ISO 27001:2013, NIST, and a larger set of policies that enable you to validate security best practices with an impact beyond regulatory compliance. These Prisma Cloud default policies cannot be modified.

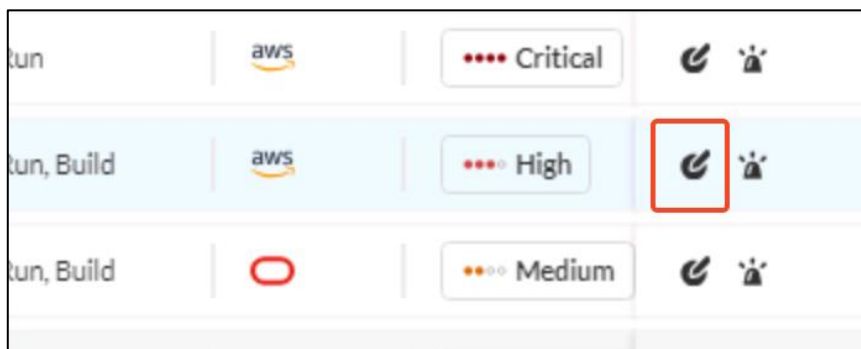
In addition to these predefined policies, you can create custom policies to monitor for violations and enforce your organizational standards. You can use the Default policies as templates to create custom policies. After you set up the policies, any new or existing resources that violate these policies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

Prisma Cloud includes out-of-the-box (OOTB) policies that are part of the Prisma Cloud Recommended Policies Pack.

Step 6. In Prisma Cloud Enterprise Edition, click on Governance.



Step 7. Make sure the filters are cleared, type in "imds" into the search bar, and click on the Edit icon for the policy "AWS EC2 instance not configured with Instance Metadata Service v2 (IMDSv2)".



Step 8. On the popped-out window, run through the policy description, then click Next.

Step 9. On the query section, notice that the query has been configured as this is an OOTB policy. Then, click Next.

Edit Config Policy

Add Details

Create query

Compliance Standards

Remediation

Compliance Standards

Compliance Standards

Standard	Requirement	Section	
ISO/IEC 27001:2022	Organisational Controls	A5.10	—
Secure Controls Framework (SCF) - ...	Network Security	NET-04.10	—
MITRE ATT&CK v14.0 Cloud IaaS fo...	TA0007	T1580 - Cloud Infrastructure Disco...	—
RBI Baseline Cyber Security and Re...	Data Leak prevention strategy	15.3	—
ISO 27002:2022	Organizational controls	5.10	—
New Zealand Information Security ...	19	19.1	—
MITRE ATT&CK v10.0	TA0007	T1580 - Cloud Infrastructure Disco...	—
ISO/IEC 27001:2022	Technological Controls	A8.3	—
ISO 27002:2022	Technological controls	8.3	—

Previous

Next

Step 9. In the remediation section, the recommendation for Remediation has been provided as a manual procedure to remediate if there is a policy violation. CLI command has also been configured, where a CLI command will be provided to remediate the misconfiguration if there is a violation. Click "X" to close the window.

Prisma Cloud Compliance Overview

The Compliance Overview is a dashboard that provides a snapshot of your overall compliance posture across various compliance standards.

Use the Compliance Dashboard as a tool for risk oversight across all the supported cloud platforms and gauge the effectiveness of the security processes and controls you have implemented to keep your enterprise secure. You can also create compliance reports and run them immediately, or schedule them regularly to measure your compliance over time.

The Compliance Dashboard supports you whether you've spent a lot of time designing and establishing internal regulations and devising the right policies, or you use the built-in regulatory compliance standards available on Prisma Cloud.

You can also find the list of compliance standards that Prisma Cloud supports [here](#)













In this activity, you will:

- Review Compliance Overview in Prisma Cloud Enterprise Edition
- Schedule and generate compliance reports for internal consumption

Note: This is a standalone activity and is not dependent on other activities.

Step 10. Go to **Prisma Cloud Enterprise > Cloud Security > Compliance**

Step 11. Here you can see a list of compliance standards supported by Prisma Cloud out of the box:

 Cloud Security ▼ Home Dashboards Reports Inventory Compliance Alerts Investigate Governance			
COMPLIANCE Standards ⌵ Add View Manage Views			
Date Most Recent Add Filter			
Data As Of: 47 minutes ago			
Name ⌵	Description ⌵	Clouds ⌵	Policies Assigned ⌵
CIS v1.0.0 (Alibaba Cloud)	CIS Alibaba Cloud Foundation Benchmark v.1.0.0		19
CIS v1.0.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.0.0		24
CIS v1.1.0 (GKE)	CIS Google Kubernetes Engine Foundation Benchmark v.1.1.0		23
CIS v1.1.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.1.0		23
CIS v1.2.0 (GKE)	CIS Google Kubernetes Engine (GKE) v1.2.0		23
CIS v1.2.0 (OCI)	CIS Oracle Cloud Infrastructure Foundations Benchmark v.1.2.0		28
CIS v1.3.0 (GKE) - Level 1	CIS Google Kubernetes Engine (GKE) v1.3.0 - Level 1		17
CIS v1.3.0 (GKE) - Level 2	CIS Google Kubernetes Engine (GKE) v1.3.0 - Level 2		5
CIS v1.4.0 (GKE) - Level 1	CIS Google Kubernetes Engine (GKE) v1.4.0 - Level 1		17
CIS v1.4.0 (GKE) - Level 2	CIS Google Kubernetes Engine (GKE) v1.4.0 - Level 2		5
CIS v2.0.0 (GCP) Level 1	CIS Google Cloud Platform Foundation Benchmark v2.0.0 (Level 1)		37

Step 12. Type "NIST" in the search bar in the top right corner to filter the compliance standards. Click on "NIST SP 800-171 Revision 2".

The screenshot shows the Prisma Cloud Compliance page. A search bar in the top right corner contains the text "NIST". Below the search bar, a table lists compliance standards. The row for "NIST SP 800-171 Revision 2" is highlighted with a red box.

Name	Description	Clouds	Policies Assigned	Total	Passed	Failed
NIST 800-171 Rev1	NIST 800-171 Rev1 Compliance Standard	aws	63	389	119	270
NIST 800-53 Rev 5	NIST Special Publication 800-53 Revision 5	aws, azure, gcp	312	752	284	468
NIST 800-53 Rev4	NIST 800-53 Rev4 Compliance Standard	aws, azure, gcp	374	765	283	482
NIST SP 800-171 Revision 2	NIST Special Publication 800-171 Revision 2	aws, azure, gcp, oracle	537	1,562	585	977
NIST SP 800-172	NIST Special Publication 800-172	aws, azure, gcp, oracle	537	1,562	585	977
NIST CSF	NIST Cybersecurity Framework (CSF) version 1.1	aws, azure, gcp, oracle	524	1,515	529	986

Step 13. On the next page, you can see how the compliance standard is being structured. This is based on the actual compliance requirement, and Prisma Cloud maps the policies according to each section of the compliance requirement. Click on "CONFIGURATION MANAGEMENT".

The screenshot shows the Prisma Cloud Compliance page with the breadcrumb "Compliance Standards > NIST SP 800-171 Revision 2". A table lists the sections of the standard. The row for "CONFIGURATION MANAGEMENT" is highlighted with a red box.

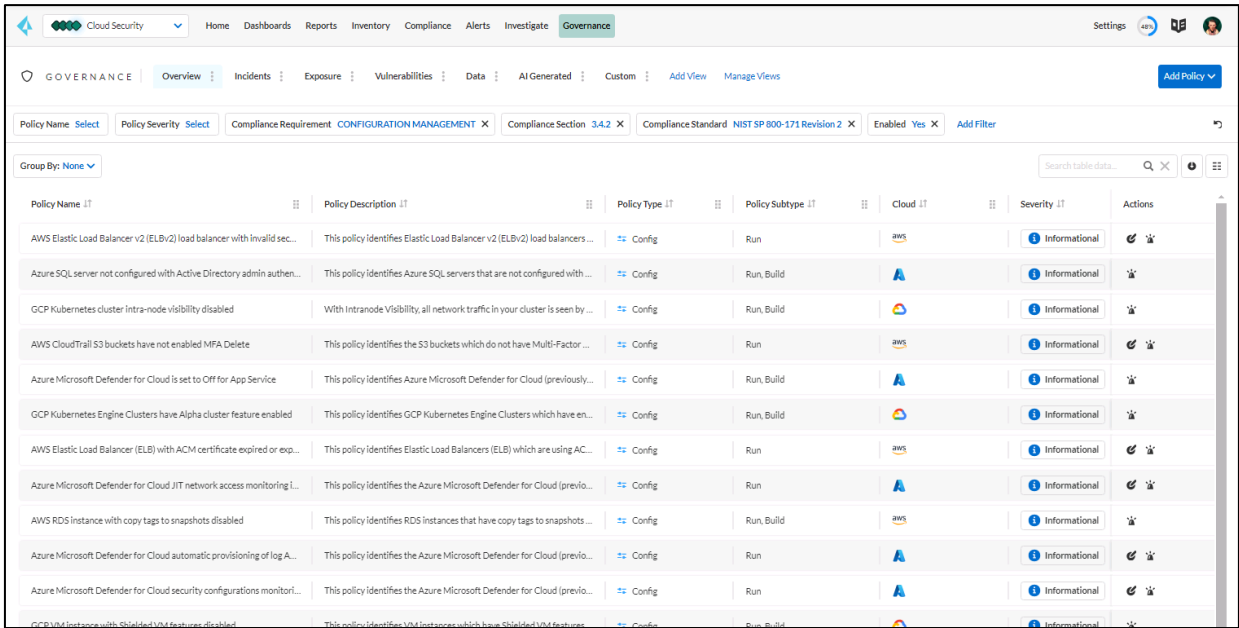
Name	Requirement ID	Description	Policies Assigned	Total
CONFIGURATION MANAGEMENT	3.4	CONFIGURATION MANAGEMENT	113	652
SYSTEM AND COMMUNICATIONS PROTECTION	3.13	SYSTEM AND COMMUNICATIONS PROTECTION	189	537
AUDIT AND ACCOUNTABILITY	3.3	AUDIT AND ACCOUNTABILITY	67	234
SYSTEM AND INFORMATION INTEGRITY	3.14	SYSTEM AND INFORMATION INTEGRITY	127	214
ACCESS CONTROL	3.1	ACCESS CONTROL	82	556
MAINTENANCE	3.7	MAINTENANCE	14	3

Step 14. On the next page, you can also see how policies are mapped to each sub-section of the compliance standard. Click on the numbers under **Policies Assigned**, the same row as section 3.4.2.

The screenshot shows the Prisma Cloud Compliance page with the breadcrumb "Compliance Standards > NIST SP 800-171 Revision 2 > CONFIGURATION MANAGEMENT". A table lists the sub-sections of the standard. The row for "3.4.2 Establish and enforce security configuration settings for information technology products" is highlighted with a red box.

Section ID	Description	Policies Assigned	Total	Passed	Failed	Critical	High
3.4.2	Establish and enforce security configuration settings for information technology products...	109	652	98	554		
3.4.9	Control and monitor user-installed software.	4					
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software...	0					
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols...	0					
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide...	0					
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated...	0					
3.4.4	Analyze the security impact of changes prior to implementation.	0					

Step 15. On the next page, you will be able to see all the policies that are mapped to this particular sub-section. This allows you to understand how all the policies are built into the compliance requirement and how Prisma Cloud can assist organizations with their compliance with certain standards or regulatory requirements.



The screenshot shows the Prisma Cloud Governance page. The top navigation bar includes Home, Dashboards, Reports, Inventory, Compliance, Alerts, Investigate, and Governance. The main header has tabs for GOVERNANCE, Overview, Incidents, Exposure, Vulnerabilities, Data, AI Generated, Custom, Add View, and Manage Views. Below the header, there are filters for Policy Name, Policy Severity, Compliance Requirement (CONFIGURATION MANAGEMENT), Compliance Section (3.4.2), Compliance Standard (NIST SP 800-171 Revision 2), and Enabled (Yes). A search bar is also present. The main content area displays a table of policies with columns for Policy Name, Policy Description, Policy Type, Policy Subtype, Cloud, Severity, and Actions. The table lists various AWS and Azure policies related to Elastic Load Balancing, SQL servers, Kubernetes clusters, CloudTrail, Microsoft Defender, and RDS instances.

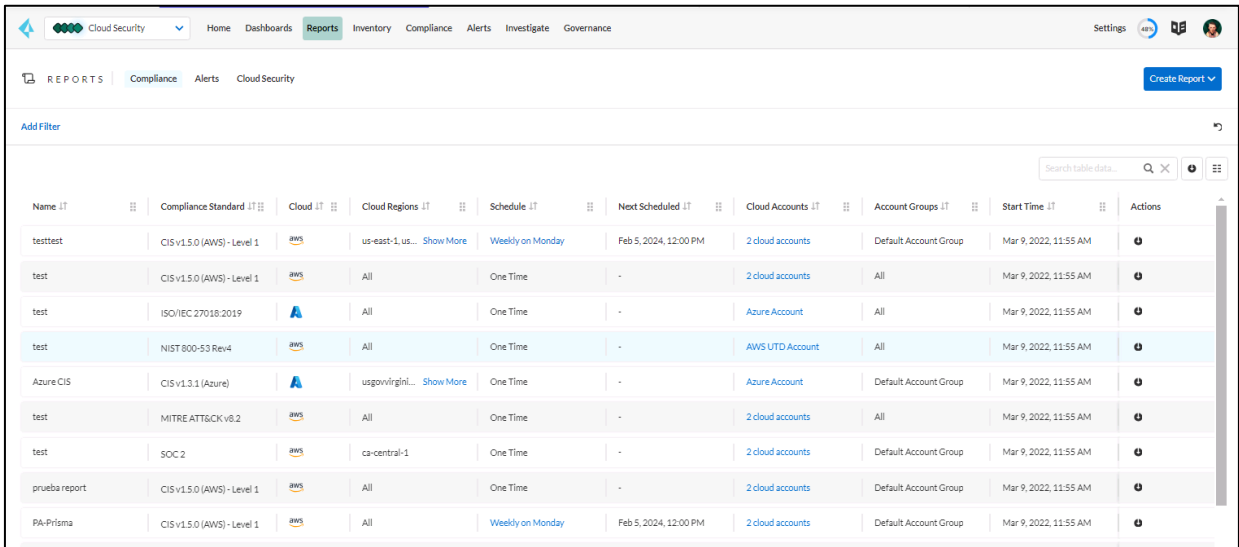
Policy Name	Policy Description	Policy Type	Policy Subtype	Cloud	Severity	Actions
AWS Elastic Load Balancer v2 (ELBv2) load balancer with invalid sec...	This policy identifies Elastic Load Balancer v2 (ELBv2) load balancers ...	Config	Run	AWS	Informational	
Azure SQL server not configured with Active Directory admin authen...	This policy identifies Azure SQL servers that are not configured with ...	Config	Run, Build	Azure	Informational	
GCP Kubernetes cluster intra-node visibility disabled	With Intranode Visibility, all network traffic in your cluster is seen by ...	Config	Run, Build	GCP	Informational	
AWS CloudTrail S3 buckets have not enabled MFA Delete	This policy identifies the S3 buckets which do not have Multi-Factor ...	Config	Run	AWS	Informational	
Azure Microsoft Defender for Cloud is set to Off for App Service	This policy identifies Azure Microsoft Defender for Cloud (previously...	Config	Run, Build	Azure	Informational	
GCP Kubernetes Engine Clusters have Alpha cluster feature enabled	This policy identifies GCP Kubernetes Engine Clusters which have en...	Config	Run, Build	GCP	Informational	
AWS Elastic Load Balancer (ELB) with ACM certificate expired or exp...	This policy identifies Elastic Load Balancers (ELB) which are using AC...	Config	Run	AWS	Informational	
Azure Microsoft Defender for Cloud JIT network access monitoring L...	This policy identifies the Azure Microsoft Defender for Cloud (previo...	Config	Run	Azure	Informational	
AWS RDS instance with copy tags to snapshots disabled	This policy identifies RDS instances that have copy tags to snapshots ...	Config	Run, Build	AWS	Informational	
Azure Microsoft Defender for Cloud automatic provisioning of log A...	This policy identifies the Azure Microsoft Defender for Cloud (previo...	Config	Run	Azure	Informational	
Azure Microsoft Defender for Cloud security configurations monitori...	This policy identifies the Azure Microsoft Defender for Cloud (previo...	Config	Run	Azure	Informational	
GCP VM4 instance with Shield VM4 features disabled	This policy identifies VM4 instances which have Shield VM4 features...	Config	Run, Build	GCP	Informational	

Download Compliance Report

Note: The lab uses a read-only user, which doesn't have access to generate a compliance report. Therefore, we'll only run through the steps to download a compliance report.

Step 15. Go to **Prisma Cloud Enterprise > Cloud Security > Reports**

Step 16. On this page, you will see all the different reports created by existing users or yourself, either for one-time usage or a regular schedule.



The screenshot shows the Prisma Cloud Reports page. The top navigation bar includes Home, Dashboards, Reports, Inventory, Compliance, Alerts, Investigate, and Governance. The main header has tabs for REPORTS, Compliance, Alerts, and Cloud Security. Below the header, there are filters for Add Filter and a search bar. The main content area displays a table of reports with columns for Name, Compliance Standard, Cloud, Cloud Regions, Schedule, Next Scheduled, Cloud Accounts, Account Groups, Start Time, and Actions. The table lists various reports for CIS v1.5.0 (AWS), ISO/IEC 27018:2019, NIST 800-53 Rev4, Azure CIS, MITRE ATT&CK v8.2, SOC 2, and Prisma.

Name	Compliance Standard	Cloud	Cloud Regions	Schedule	Next Scheduled	Cloud Accounts	Account Groups	Start Time	Actions
testtest	CIS v1.5.0 (AWS) - Level 1	AWS	us-east-1, us... Show More	Weekly on Monday	Feb 5, 2024, 12:00 PM	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
test	CIS v1.5.0 (AWS) - Level 1	AWS	All	One Time	-	2 cloud accounts	All	Mar 9, 2022, 11:55 AM	
test	ISO/IEC 27018:2019	Azure	All	One Time	-	Azure Account	All	Mar 9, 2022, 11:55 AM	
test	NIST 800-53 Rev4	AWS	All	One Time	-	AWS UTD Account	All	Mar 9, 2022, 11:55 AM	
Azure CIS	CIS v1.3.1 (Azure)	Azure	usgovvirginia... Show More	One Time	-	Azure Account	Default Account Group	Mar 9, 2022, 11:55 AM	
test	MITRE ATT&CK v8.2	AWS	All	One Time	-	2 cloud accounts	All	Mar 9, 2022, 11:55 AM	
test	SOC 2	AWS	ca-central-1	One Time	-	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
prueba report	CIS v1.5.0 (AWS) - Level 1	AWS	All	One Time	-	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	
PA-Prisma	CIS v1.5.0 (AWS) - Level 1	AWS	All	Weekly on Monday	Feb 5, 2024, 12:00 PM	2 cloud accounts	Default Account Group	Mar 9, 2022, 11:55 AM	

Step 17. On the search bar, type "NIST". Click on the **Download** icon in the Action column to download the report.

The screenshot shows the Prisma Cloud Reports interface. At the top, there's a navigation bar with 'Cloud Security' selected. Below it, a sub-navigation bar shows 'REPORTS', 'Compliance', 'Alerts', and 'Cloud Security'. A 'Create Report' button is on the right. A search bar at the top right contains the text 'NIST'. Below the search bar is a table with the following columns: Name, Compliance Standard, Cloud, Cloud Regions, Schedule, Next Scheduled, Cloud Accounts, Account Groups, and Actions. The table contains five rows. The second row, 'test report 800-172', is highlighted with a red box. The 'Actions' column for this row also has a red box around the download icon.

Name	Compliance Standard	Cloud	Cloud Regions	Schedule	Next Scheduled	Cloud Accounts	Account Groups	Actions
test	NIST 800-53 Rev4	aws	All	One Time	-	AWS UTD Account	All	
test report 800-172	NIST SP 800-172	aws	All	One Time	-	2 cloud accounts	All	
Alex Test	NIST 800-53 Rev 5	aws	All	One Time	-	AWS UTD Account	All	
nistcsf	NIST CSF	Azure	All	One Time	-	Azure Account	All	
NIST-SP-800-171	NIST SP 800-171 Revisio...	Azure	All	One Time	-	Azure Account	All	

Note: As you're accessing Prisma Cloud via a full-screen remote desktop, you might not be able to view the downloaded document. For a NIST sample report, refer to a sample document [here](#).

Note: You can schedule a compliance report to be sent to specific teams in regular basis (weekly, daily, etc).