



## Cortex Cloud Posture Management Documentation

Confidential - Copyright © Palo Alto Networks



## 1. Get started with Cortex Cloud

- 1.1. What is Cortex Cloud?
  - 1.1.1. Key features
- 1.2. What is Cortex Cloud Posture Management?
- 1.3. Agentic AI in Cortex Cloud
  - 1.3.1. Cortex Agentic Assistant
    - 1.3.1.1. Agentic Assistant use cases
    - 1.3.1.2. Agentic Assistant security
- 1.4. Use the interface
- 1.5. In-product support case creation
- 1.6. Understand your user persona
- 1.7. Fair Usage policy for Cortex Cloud
- 1.8. Understand license plans
  - 1.8.1. Data retention

## 2. Onboard and configure Cortex Cloud

- 2.1. Plan and prepare
- 2.2. Deployment steps and checklist
  - 2.2.1. Activate Cortex Cloud
    - 2.2.1.1. Cortex Cloud supported regions
    - 2.2.1.2. Enable access to required PANW resources
  - 2.2.2. Upgrade from Prisma Cloud to Cortex Cloud
    - 2.2.2.1. About the Upgrade Helper
    - 2.2.2.2. Link Cortex Cloud to Prisma Cloud
    - 2.2.2.3. Copy content
      - 2.2.2.3.1. Copy Global configurations
      - 2.2.2.3.2. Copy CSM configurations
      - 2.2.2.3.3. Copy CWP configurations
      - 2.2.2.3.4. Copy Cortex Cloud Application Security configurations
    - 2.2.2.4. Migrate Cortex CLI
  - 2.2.3. Set up users and roles
    - 2.2.3.1. User group management
    - 2.2.3.2. Assign user roles and groups
  - 2.2.4. Manage API keys
  - 2.2.5. Set up authentication
    - 2.2.5.1. Authenticate users through the Customer Support Portal
    - 2.2.5.2. Authenticate users using SSO
    - 2.2.5.3. Set up Okta as the Identity Provider Using SAML 2.0
    - 2.2.5.4. Set up Azure AD as the Identity Provider Using SAML 2.0
  - 2.2.6. Cloud service provider (CSP) onboarding
    - 2.2.6.1. Ingest cloud assets
    - 2.2.6.2. Onboard Amazon Web Services
      - 2.2.6.2.1. Manually upload template to AWS
      - 2.2.6.2.2. Configure AWS integration instances and monitor integration instance health
    - 2.2.6.3. Onboard Google Cloud Platform
      - 2.2.6.3.1. Manually upload template to GCP
      - 2.2.6.3.2. Connect Google Workspace with your GCP cloud instance
      - 2.2.6.3.3. Configure GCP integration instances and monitor integration instance health
      - 2.2.6.3.4. Monitor GCP resources inside service perimeters
    - 2.2.6.4. Onboard Microsoft Azure
      - 2.2.6.4.1. Finalize Microsoft Azure onboarding by executing the authentication template
      - 2.2.6.4.2. Configure Azure integration instances and monitor integration instance health
    - 2.2.6.5. Onboard Oracle Cloud Infrastructure
      - 2.2.6.5.1. Manually upload template to OCI
      - 2.2.6.5.2. Configure the OCI connector for log collection
    - 2.2.6.6. Manually connect a cloud instance
    - 2.2.6.7. Edit your onboarded CSP configuration
    - 2.2.6.8. Outposts
      - 2.2.6.8.1. Outpost fundamentals and planning
      - 2.2.6.8.2. Create an outpost
    - 2.2.6.9. Introduction to Terraform for Cloud service provider (CSP) onboarding
    - 2.2.6.10. Container Registry Scanning
      - 2.2.6.10.1. Overview of container registry scanning
        - 2.2.6.10.1.1. Registry Components
        - 2.2.6.10.1.2. How Container Registry Scanning Works
        - 2.2.6.10.1.3. Modify the container registry scanning scope
        - 2.2.6.10.1.4. Scan re-evaluation process
        - 2.2.6.10.1.5. Connect Docker Hub registry
          - 2.2.6.10.1.5.1. Manage a Docker Hub connector
        - 2.2.6.10.1.6. Connect Docker V2 compliant container registry
          - 2.2.6.10.1.6.1. Manage a Docker V2 connector
        - 2.2.6.10.1.7. Connect GitLab container registry
          - 2.2.6.10.1.7.1. Manage a GitLab Container Registry connector
        - 2.2.6.10.1.8. Connect Harbor registry
          - 2.2.6.10.1.8.1. Manage a Harbor connector
        - 2.2.6.10.1.9. Connect JFrog container registry
          - 2.2.6.10.1.9.1. Manage a JFrog connector
        - 2.2.6.10.1.10. Connect Sonatype Nexus registry
          - 2.2.6.10.1.10.1. Manage a Sonatype connector
      - 2.2.6.11. Cloud service provider permissions
        - 2.2.6.11.1. Amazon Web Services provider permissions
        - 2.2.6.11.2. Google Cloud Platform provider permissions



- 2.2.6.11.3. Microsoft Azure provider permissions
- 2.2.6.11.4. Oracle Cloud Infrastructure provider permissions
- 2.2.7. Onboard the Kubernetes Connector
  - 2.2.7.1. What's new in Kubernetes Connector?
  - 2.2.7.2. Supported Kubernetes distributions

### 2.3. Post-deployment steps

- 2.3.1. Set up your environment
  - 2.3.1.1. Configure server settings
  - 2.3.1.2. Configure security settings
  - 2.3.1.3. Log forwarding
    - 2.3.1.3.1. Forward logs from Cortex Cloud to external services
      - 2.3.1.3.1.1. Integrate a syslog receiver
      - 2.3.1.3.1.2. Integrate Slack for outbound notifications
      - 2.3.1.3.1.3. Configure notification forwarding
      - 2.3.1.3.1.4. Monitor administrative activity
    - 2.3.1.3.2. Data and log notification formats
      - 2.3.1.3.2.1. Management audit log messages
      - 2.3.1.3.2.2. Issue notification format
      - 2.3.1.3.2.3. Management Audit log notification format
      - 2.3.1.3.2.4. Log format for IOC and BIOC issues
      - 2.3.1.3.2.5. Analytics log format
  - 2.3.2. Cortex MCP server
    - 2.3.2.1. Cortex MCP server overview
      - 2.3.2.1.1. Install the Cortex MCP server
      - 2.3.2.1.2. Configure the MCP client
      - 2.3.2.1.3. Use the Cortex MCP server
      - 2.3.2.1.4. Create custom Cortex MCP server tools
  - 2.3.3. Manage user roles and access management
    - 2.3.3.1. Manage user roles
    - 2.3.3.2. Manage user access
      - 2.3.3.2.1. User access reference information
    - 2.3.3.3. Manage user scope
    - 2.3.3.4. Manage access to objects
      - 2.3.3.4.1. Manage access to custom dashboards
      - 2.3.3.4.2. Manage access to saved queries
  - 2.3.4. Configure the Cortex Agentic Assistant
    - 2.3.4.1. Agentic Assistant components and concepts
    - 2.3.4.2. Agents Hub
      - 2.3.4.2.1. Manage actions
      - 2.3.4.2.2. Register actions
      - 2.3.4.2.3. Manage agents
      - 2.3.4.2.4. Build agents
      - 2.3.4.2.5. Expand agent capabilities with MCP integrations
    - 2.3.4.3. Agentic Assistant role-based access control
  - 2.3.5. XQL query management
  - 2.3.6. Customize cases and issues
    - 2.3.6.1. Customize cases and issues
      - 2.3.6.1.1. Set up case scoring
      - 2.3.6.1.2. Create a starring configuration
      - 2.3.6.1.3. Create custom case statuses and resolution reasons
      - 2.3.6.1.4. Create a sync profile
  - 2.3.7. Dashboards and reports

## 3. Review inventory and explore your cloud environment

### 3.1. Inventory management

- 3.1.1. Asset management
  - 3.1.1.1. All Assets
    - 3.1.1.1.1. Container Images
    - 3.1.1.1.2. Kubernetes Cluster
    - 3.1.1.1.3. External Surface assets
  - 3.1.1.2. Serverless function assets
    - 3.1.1.2.1. Overview
    - 3.1.1.2.2. Explore the serverless functions inventory
    - 3.1.1.2.3. Expanded serverless function asset information
  - 3.1.1.3. Network configuration
    - 3.1.1.3.1. Configure your network parameters
  - 3.1.1.4. Asset Groups
  - 3.1.1.5. Vulnerability Assessment

## 4. Review and prioritize posture issues

### 4.1. Cases and issues

- 4.1.1. Overview of cases
  - 4.1.1.1. What are cases?
  - 4.1.1.2. Resolving cases with AI
  - 4.1.1.3. Case lifecycle
  - 4.1.1.4. Case thresholds
  - 4.1.1.5. Case scope and impact
  - 4.1.1.6. Case and issue domains
- 4.1.2. Case concepts
  - 4.1.2.1. Issues, findings, and events
    - 4.1.2.1.1. Issues
    - 4.1.2.1.2. Findings and events
  - 4.1.2.2. Case grouping
  - 4.1.2.3. Case scoring
  - 4.1.2.4. Case starring
  - 4.1.2.5. What is Causality?
- 4.1.3. Analyze and resolve cases
  - 4.1.3.1. Review all cases
  - 4.1.3.2. Start case analysis



- 4.1.3.2.1. Agentic Assistant- Case Investigation agent
- 4.1.3.3. Establish case context
  - 4.1.3.3.1. AI-generated case summaries
  - 4.1.3.3.2. Assess case severity and score
  - 4.1.3.3.3. Update case attributes
- 4.1.3.4. Analyze case details
  - 4.1.3.4.1. Grouping graph
  - 4.1.3.4.2. Evidence
  - 4.1.3.4.3. Issue feed
  - 4.1.3.4.4. Associated assets and artifacts
  - 4.1.3.4.5. MITRE ATT&CK tactics and techniques
  - 4.1.3.4.6. Detailed View
  - 4.1.3.4.7. Issue card
- 4.1.3.5. Resolve the case
  - 4.1.3.5.1. Resolution Center
  - 4.1.3.5.2. Collaborative notes and comments
  - 4.1.3.5.3. Resolve a case
  - 4.1.3.5.4. Resolution reasons for cases and issues
- 4.1.3.6. Additional case actions
  - 4.1.3.6.1. Create a case
  - 4.1.3.6.2. Merge a case

## 4.2. Investigation and response

- 4.2.1. Investigate issues
  - 4.2.1.1. Overview of the Issues page
  - 4.2.1.2. Link or unlink issues from a case
  - 4.2.1.3. Run an automation on an issue
  - 4.2.1.4. Use the War Room in an investigation
  - 4.2.1.5. Use the Work Plan in an investigation
  - 4.2.1.6. Issue syncing
  - 4.2.1.7. Issue investigation actions
    - 4.2.1.7.1. Copy issues
    - 4.2.1.7.2. Update issue fields
    - 4.2.1.7.3. Export issue details to a file
    - 4.2.1.7.4. Exclude an issue
    - 4.2.1.7.5. Query case and issue data
- 4.2.2. Review findings
  - 4.2.2.1. Findings card
- 4.2.3. Investigate artifacts and assets
  - 4.2.3.1. Investigate an IP address
  - 4.2.3.2. Investigate an asset
  - 4.2.3.3. Investigate a file and process hash
  - 4.2.3.4. Investigate a user
- 4.2.4. Cortex Assistant
  - 4.2.4.1. Cortex Assistant layout
  - 4.2.4.2. Cortex Assistant capabilities
- 4.2.5. Automation
  - 4.2.5.1. Automation in Cortex Cloud
  - 4.2.5.2. Quick Actions
  - 4.2.5.3. Automation Exclusion Center
    - 4.2.5.3.1. Manage automation exclusion policies
  - 4.2.5.4. Playbooks
    - 4.2.5.4.1. Playbooks overview
    - 4.2.5.4.2. Playbook development checklist
    - 4.2.5.4.3. Plan your playbook
    - 4.2.5.4.4. Manage playbooks
    - 4.2.5.4.5. Build your playbook
      - 4.2.5.4.5.1. Task 1. Choose from existing playbooks or create your own
      - 4.2.5.4.5.2. Task 2. Configure playbook settings
      - 4.2.5.4.5.3. Task 3. Add objects from the Task Library
      - 4.2.5.4.5.4. Task 4. Add custom playbook features
      - 4.2.5.4.5.5. Task 5. Test and debug the playbook
      - 4.2.5.4.5.6. Task 6. Manage playbook content
    - 4.2.5.4.6. Customize your playbook
      - 4.2.5.4.6.1. Configure a sub-playbook loop
      - 4.2.5.4.6.2. Filter and transform data
      - 4.2.5.4.6.3. Extend context
      - 4.2.5.4.6.4. Extract indicators
      - 4.2.5.4.6.5. Update issue fields with playbook tasks
    - 4.2.5.4.7. Test your playbook
      - 4.2.5.4.7.1. Troubleshoot playbook performance
    - 4.2.5.4.8. Manage playbook content
    - 4.2.5.4.9. Best practices
  - 4.2.5.5. AI Prompts
    - 4.2.5.5.1. AI prompts role-based access control
    - 4.2.5.5.2. Use existing prompts
    - 4.2.5.5.3. Create a prompt
  - 4.2.5.6. Create an automation rule
  - 4.2.5.7. Scripts
    - 4.2.5.7.1. Use existing scripts
    - 4.2.5.7.2. Create a script
    - 4.2.5.7.3. Use the Automation Engineer agent to accelerate script development and deployment
    - 4.2.5.7.4. Change the Docker image in a script
      - 4.2.5.7.4.1. Connect an engine to an image registry
  - 4.2.5.8. Context data
    - 4.2.5.8.1. Issue context data
    - 4.2.5.8.2. Case context data
    - 4.2.5.8.3. Search context data
    - 4.2.5.8.4. Add context data to an issue
    - 4.2.5.8.5. Add context data to a case
    - 4.2.5.8.6. Delete context data from a case
    - 4.2.5.8.7. Use context data in a playbook
  - 4.2.5.9. Lists
    - 4.2.5.9.1. Create a list
    - 4.2.5.9.2. List commands
    - 4.2.5.9.3. Use cases: JSON lists
    - 4.2.5.9.4. Transform a list into an array
  - 4.2.5.10. Integrations
    - 4.2.5.10.1. Integrations in Cortex Cloud
    - 4.2.5.10.2. Add an integration instance



- 4.2.5.10.3. Use integration commands in the CLI
- 4.2.5.10.4. Troubleshoot Integrations
- 4.2.5.10.5. Manage credentials
- 4.2.5.11. Engines
  - 4.2.5.11.1. What is an engine?
  - 4.2.5.11.2. Engine requirements
  - 4.2.5.11.3. Install an engine
    - 4.2.5.11.3.1. Docker
    - 4.2.5.11.3.2. Podman
  - 4.2.5.11.4. Manage engines
  - 4.2.5.11.5. Upgrade an engine
  - 4.2.5.11.6. Remove an engine
  - 4.2.5.11.7. Configure engines
    - 4.2.5.11.7.1. Configure the engine to use a web proxy
    - 4.2.5.11.7.2. Configure the engine to call the server without using a proxy
    - 4.2.5.11.7.3. Configure an engine to use custom certificates
  - 4.2.5.11.8. Use an engine in an integration
  - 4.2.5.11.9. Run a script using an engine
  - 4.2.5.11.10. Troubleshoot engines
  - 4.2.5.11.11. Troubleshoot integrations running on engines
- 4.2.6. Build XQL queries
  - 4.2.6.1. About the Query Builder
  - 4.2.6.2. How to build XQL queries
    - 4.2.6.2.1. Get started with XQL queries
    - 4.2.6.2.2. Useful XQL user interface features
    - 4.2.6.2.3. XQL Query best practices
    - 4.2.6.2.4. Expected results when querying fields
    - 4.2.6.2.5. Create XQL query
    - 4.2.6.2.6. Review XQL query results
    - 4.2.6.2.7. Translate to XQL
    - 4.2.6.2.8. Graph query results
  - 4.2.6.3. XQL query entities
    - 4.2.6.3.1. Create authentication query
    - 4.2.6.3.2. Create event log query
    - 4.2.6.3.3. Create file query
    - 4.2.6.3.4. Create image load query
    - 4.2.6.3.5. Create network connections query
    - 4.2.6.3.6. Create network query
    - 4.2.6.3.7. Create process query
    - 4.2.6.3.8. Create registry query
    - 4.2.6.3.9. Query across all entities
  - 4.2.6.4. Overview of the Query Center
    - 4.2.6.4.1. Edit and run queries in Query Center
      - 4.2.6.4.1.1. Query Center reference information
  - 4.2.6.5. Manage scheduled queries
    - 4.2.6.5.1. Scheduled Queries reference information
  - 4.2.6.6. Manage your query library
- 4.2.7. Quick Launcher

### 4.3. Customize cases and issues

- 4.3.1. Customize cases and issues
  - 4.3.1.1. Set up case scoring
  - 4.3.1.2. Create a starring configuration
  - 4.3.1.3. Create custom case statuses and resolution reasons
  - 4.3.1.4. Create a sync profile

## 5. Agentic Assistant chat

- 5.1. Get started with Agentic Assistant chat
- 5.2. Choose an Agentic Assistant agent
- 5.3. Chat with an Agentic Assistant agent
- 5.4. Create and run XQL queries with Agentic Assistant chat
- 5.5. Manage chat history

## 6. Review and report your security posture and progress

- 6.1. Monitor dashboards and reports
  - 6.1.1. About dashboards
    - 6.1.1.1. Command Center dashboards
      - 6.1.1.1.1. Cortex Agentic Assistant dashboard
      - 6.1.1.1.2. Cloud Security Operations
      - 6.1.1.1.2.1. Cloud Security Operations
      - 6.1.1.1.3. Cortex Cloud Command Center
    - 6.1.1.2. Predefined dashboards
    - 6.1.1.3. Reports
      - 6.1.1.3.1. Report templates
  - 6.1.2. Build custom dashboards and reports
    - 6.1.2.1. Build a custom dashboard
    - 6.1.2.2. Manage your Widget Library
  - 6.1.3. Fine-tune dashboards and reports
    - 6.1.3.1. Create a custom widget using a script
      - 6.1.3.1.1. Script-based widget examples
    - 6.1.3.2. Create custom XQL widgets
      - 6.1.3.2.1. Configure filters and inputs for custom XQL widgets
      - 6.1.3.2.2. Configure dashboard drilldowns
        - 6.1.3.2.2.1. Variables in drilldowns
  - 6.1.4. Run or schedule reports

## 7. Monitor and track compliance adherence

- 7.1. Cortex compliance flow



## 7.2. Choose compliance standards from the compliance catalog

### 7.2.1. Standards Catalog

7.2.1.1. Use a built-in or custom standard

### 7.2.2. Controls catalog

7.2.2.1. Use a built-in or custom control

7.2.2.1.1. Add a custom detection rule to a custom control

7.2.2.1.2. Create a new Custom Detection Rule

## 7.3. Use an assessment profile to run compliance checks on your assets

## 7.4. View and manage compliance assessments and reports

### 7.4.1. Assessments

### 7.4.2. Reports

## 7.5. View the compliance assessment of an individual asset

# 8. Discovery Engine

## 8.1. What is the Discovery Engine?

# 9. Cortex Cloud AI Security

## 9.1. What is Cortex Cloud AI Security?

## 9.2. Supported services in Cortex Cloud AI Security

## 9.3. Cortex Cloud AI Security concepts

## 9.4. Cortex Cloud AI Security use cases

## 9.5. How to perform advanced AI Security investigations using XQL

# 10. Cortex Cloud Application Security

## 10.1. Onboard Data Sources

### 10.1.1. Onboard version control systems

10.1.1.1. AWS CodeCommit

10.1.1.2. Azure DevOps

10.1.1.2.1. Azure DevOps onboarding system architecture

10.1.1.3. Bitbucket Cloud

10.1.1.4. Bitbucket Data Center

10.1.1.5. GitHub Cloud

10.1.1.6. GitHub Enterprise (On-Prem)

10.1.1.7. GitLab SaaS

10.1.1.8. GitLab Self Managed (On-Prem)

### 10.1.2. Onboard CI/CD systems

10.1.2.1. Onboard CircleCI for CI/CD pipeline scans

10.1.2.2. Onboard Jenkins for CI/CD pipeline scans

### 10.1.3. Integrate CI tools

10.1.3.1. AWS CodeBuild

10.1.3.2. Onboard CircleCI for code scans

10.1.3.3. Connect Cortex CLI

10.1.3.4. GitHub Actions

10.1.3.5. Onboard Jenkins for code scans

10.1.3.6. Onboard Terraform Cloud (Run Tasks)

10.1.3.7. Onboard Terraform Enterprise (Run Tasks)

### 10.1.4. CLI pipeline code snippets

### 10.1.5. Onboard private package registries

10.1.5.1. JFrog Artifactory

10.1.5.2. Onboard JFrog Artifactory

### 10.1.6. Supported third-party data sources

10.1.6.1. Ingest Semgrep data

10.1.6.2. Ingest Snyk data

10.1.6.3. Ingest SonarQube SAST data

10.1.6.4. Ingest Veracode SAST data

10.1.6.5. Generic 3rd Party AppSec Collector

10.1.6.5.1. Onboard the 3rd Party AppSec Collector

### 10.1.7. Manage data source integrations

### 10.1.8. Transporter over Broker VM

10.1.8.1. Set up a Transporter applet on Broker VM

10.1.8.2. Set up a Transporter on your VCS

## 10.2. Cortex Cloud Application Security dashboard

## 10.3. Application Security Posture Management (ASPM)

### 10.3.1. ASPM use cases

### 10.3.2. ASPM key features

### 10.3.3. ASPM user roles and permissions

### 10.3.4. Code to Cloud

10.3.4.1. Supported integrations

10.3.4.2. Code to Cloud visibility

10.3.4.3. Code to Cloud troubleshooting

### 10.3.5. ASPM Command Center

10.3.5.1. ASPM Command Center workflow

### 10.3.6. Coverage

10.3.6.1. Coverage in the user interface



- 10.3.7. Compliance for Cortex Cloud Application Security
  - 10.3.7.1. Infrastructure-as-Code (IaC) compliance
  - 10.3.7.2. Manage IaC compliance
  - 10.3.7.3. CI/CD Compliance
    - 10.3.7.3.1. Create CI/CD compliance reports
- 10.3.8. Urgency
  - 10.3.8.1. Urgency metrics
- 10.3.9. Backlog baseline
  - 10.3.9.1. Backlog use cases
  - 10.3.9.2. Issue/Finding classification by scanner
  - 10.3.9.3. Using Backlog
- 10.3.10. Service Lead Agreements (SLA)
  - 10.3.10.1. Configure and monitor Cortex Cloud Application Security SLAs
- 10.3.11. Applications
  - 10.3.11.1. Defining Business Applications
    - 10.3.11.1.1. Defining business applications by Criteria
    - 10.3.11.1.2. Define applications by VCS criteria
    - 10.3.11.1.3. Manage application criteria
    - 10.3.11.1.4. Define applications by cloud tag-based criteria
    - 10.3.11.1.5. How to manually build an application
  - 10.3.11.2. Application management and visibility
  - 10.3.11.3. Business application assets
    - 10.3.11.3.1. Business application expanded asset details
    - 10.3.11.3.2. Export business application data
  - 10.3.11.4. Scope user access to applications (Application SBAC)
    - 10.3.11.4.1. Enable SBAC in the Cortex Cloud tenant
    - 10.3.11.4.2. Create an application-based Asset Group
    - 10.3.11.4.3. Scope user access to an application
    - 10.3.11.4.4. Create application-scoped policies
- 10.3.12. Repositories as assets
  - 10.3.12.1. Explore repository assets
  - 10.3.12.2. In-depth repository asset information
  - 10.3.12.3. Manage Repository assets
  - 10.3.12.4. Export Software Bill of Materials (SBOM)
  - 10.3.12.5. Manage issues detected in repositories
- 10.3.13. Manage 3rd party findings and generated issues
- 10.3.14. Manage code weaknesses
  - 10.3.14.1. Code weaknesses issue inventory
  - 10.3.14.2. Detailed code weakness issue information
  - 10.3.14.3. Code weakness findings

#### 10.4. CI/CD Security

- 10.4.1. CI/CD Security user roles and permissions
- 10.4.2. CI/CD Assets
  - 10.4.2.1. CI/CD Instances as assets
    - 10.4.2.1.1. Explore CI/CD Instance assets
    - 10.4.2.1.2. In-depth CI/CD pipeline instance asset information
    - 10.4.2.1.3. Manage CI/CD pipeline instances
  - 10.4.2.2. CI/CD Pipelines as assets
    - 10.4.2.2.1. Explore CI/CD Pipeline assets
    - 10.4.2.2.2. In-depth CI/CD pipeline asset information
    - 10.4.2.2.3. Manage CI/CD pipeline assets
  - 10.4.2.3. Version Control System (VCS) Organizations as assets
    - 10.4.2.3.1. Explore VCS Organization assets
    - 10.4.2.3.2. In-depth VCS Organization asset information
    - 10.4.2.3.3. Manage VCS organization assets
  - 10.4.2.4. VCS Collaborators-as-assets
    - 10.4.2.4.1. In-depth Collaborator asset information
    - 10.4.2.4.2. Manage Collaborator assets
- 10.4.3. Supply Chain Inventories
  - 10.4.3.1. Supply Chain Tools
    - 10.4.3.1.1. Supply Chain Tools
    - 10.4.3.1.2. Expanded Supply Chain tool information
  - 10.4.3.2. Supply Chain Catalog
- 10.4.4. CI/CD Risks
  - 10.4.4.1. CI/CD pipeline issues
  - 10.4.4.2. Expanded CI/CD risks issue information
  - 10.4.4.3. VCS and CI/CD pipeline risk findings
- 10.4.5. CI/CD Rules
  - 10.4.5.1. CI/CD rules roles and permissions
  - 10.4.5.2. CI/CD rules inventory
- 10.4.6. CI/CD Policies
  - 10.4.6.1. CI/CD policies user roles and permissions
  - 10.4.6.2. CI/CD policies inventory
  - 10.4.6.3. Create custom CI/CD policies
  - 10.4.6.4. Manage CI/CD policies

#### 10.5. Code Security

- 10.5.1. Code Security user roles and permissions
- 10.5.2. Code Security assets
- 10.5.3. Software packages as assets
  - 10.5.3.1. Explore software package assets
  - 10.5.3.2. In-depth software package asset information
- 10.5.4. Infrastructure-as-Code (IaC) resources as assets
  - 10.5.4.1. Explore IaC assets
  - 10.5.4.2. In-depth IaC resource asset information
- 10.5.5. Code Security scanners
- 10.5.6. Secrets scanners
  - 10.5.6.1. Secrets issues
  - 10.5.6.2. Secrets issues inventory



- 10.5.6.3. Detailed Secrets issue information
- 10.5.6.4. Secrets findings
- 10.5.6.5. Manage Secrets issues
- 10.5.7. Infrastructure as Code (IaC) misconfiguration scanner
  - 10.5.7.1. Supported frameworks and languages
  - 10.5.7.2. IaC misconfiguration issues
  - 10.5.7.3. IaC misconfiguration issues inventory
  - 10.5.7.4. Detailed IaC misconfiguration issue information
  - 10.5.7.5. IaC misconfiguration findings
  - 10.5.7.6. Manage IaC misconfiguration issues
- 10.5.8. IaC Drift Detection scans
  - 10.5.8.1. IaC Drift Detection issues
  - 10.5.8.2. IaC Drift Detection issue inventory
  - 10.5.8.3. Detailed IaC drift detection issue information
  - 10.5.8.4. IaC Drift Detection findings
- 10.5.9. Software Composition Analysis (SCA ) scanners
  - 10.5.9.1. Supported Software Composition Analysis (SCA) frameworks and languages
  - 10.5.9.2. Software Composition Analysis (SCA) vulnerability issues
    - 10.5.9.2.1. Vulnerability issues inventory
    - 10.5.9.2.2. Detailed vulnerability issue information
    - 10.5.9.2.3. CVE vulnerabilities findings
    - 10.5.9.2.4. Manage SCA CVE vulnerability issues
  - 10.5.9.3. License miscompliance issues
    - 10.5.9.3.1. License miscompliance issues inventory
    - 10.5.9.3.2. Expanded License miscompliance issues information
    - 10.5.9.3.3. License miscompliance findings
    - 10.5.9.3.4. Open-source software license categories
    - 10.5.9.3.5. Manage license miscompliance issues
  - 10.5.9.4. Package Integrity
    - 10.5.9.4.1. Package Integrity inventory
    - 10.5.9.4.2. Expanded Package Integrity issues inventory information
    - 10.5.9.4.3. Package Integrity findings
    - 10.5.9.4.4. Manage Package Integrity issues
- 10.5.10. Application Security scans management
  - 10.5.10.1. Overview
  - 10.5.10.2. Branch periodic scans
  - 10.5.10.3. Pull Request scans
  - 10.5.10.4. CI scans
  - 10.5.10.5. Manage repository scan configurations
  - 10.5.10.6. Monitor data source instances health
- 10.5.11. Application Security Policies
  - 10.5.11.1. User roles and permissions
  - 10.5.11.2. Policies inventory
  - 10.5.11.3. AI-recommended guardrails
    - 10.5.11.3.1. Manage AI-recommended guardrails
  - 10.5.11.4. Create Cortex Cloud Application Security policies
    - 10.5.11.4.1. Create code security policies
      - 10.5.11.4.1.1. Cortex Cloud Application Security code policy Condition attributes
    - 10.5.11.4.2. Create IaC Drift Detection policies
    - 10.5.11.4.3. Manage Cortex Cloud Application Security policies
- 10.5.12. Application Security Rules
  - 10.5.12.1. Roles and permissions
  - 10.5.12.2. Rules inventory
  - 10.5.12.3. Create custom Cortex Cloud Application Security rules
  - 10.5.12.4. Manage Cortex Cloud Application Security custom rules
  - 10.5.12.5. Configure YAML file properties
- 10.5.13. Application Security CLI
  - 10.5.13.1. Connect Cortex CLI
  - 10.5.13.2. Cortex CLI usage for Cortex Cloud Application Security
  - 10.5.13.3. CLI pipeline code snippets
  - 10.5.13.4. Cortex CLI Cortex Cloud Application Security command line reference
  - 10.5.13.5. Cortex CLI common command line reference guide
  - 10.5.13.6. Git Hooks
    - 10.5.13.6.1. Cortex CLI pre-commit hooks
      - 10.5.13.6.1.1. Pre-commit hook usage
    - 10.5.13.6.2. Cortex CLI pre-receive hooks
      - 10.5.13.6.2.1. Pre-receive hook usage
- 10.5.14. IDE
  - 10.5.14.1. System requirements
  - 10.5.14.2. Visual Studio (VS) Code and VS Code compatible IDEs
    - 10.5.14.2.1. How to use the Cortex Cloud extension in VS Code
  - 10.5.14.3. JetBrains
    - 10.5.14.3.1. How to use the JetBrains Cortex Cloud extension
- 10.5.15. Developer Suppressions

## 10.6. API documentation

# 11. Cortex Cloud Data Classification

- 11.1. What is Cortex Cloud Data Classification?
- 11.2. How to create and validate a custom data pattern
- 11.3. How to disable and enable data patterns in Data Classification
- 11.4. How to create and validate a custom data profile
- 11.5. How to disable and enable data profiles in Cortex Cloud Data Classification
- 11.6. How to report a false positive in Cortex Cloud Data Classification

# 12. Cortex Cloud Data Security



- 12.1. What is Cortex Cloud Data Security?
- 12.2. Supported assets in Cortex Cloud Data Security
- 12.3. Cortex Cloud Data Security concepts
- 12.4. Cortex Cloud Data Security use cases
- 12.5. Data Inventory
- 12.6. How to review errors in Cortex Cloud Data Security
- 12.7. How to configure the scanning settings for supported services
- 12.8. How to perform advanced Data Security investigations using XQL
- 12.9. How to onboard Databricks
- 12.10. How to onboard Microsoft 365
- 12.11. How to onboard on-premise file shares to Cortex Cloud Data Security
- 12.12. How to onboard Snowflake
- 12.13. How to use information protection labels in Cortex Cloud Data Security

## 13. Cortex Cloud Identity Security

- 13.1. What is Cortex Cloud Identity Security?
- 13.2. Review and improve your Identity Security posture
- 13.3. How does Effective Permission Calculation work?
- 13.4. Cortex Cloud Identity Security functionality
- 13.5. Achieve the principle of least privilege access
- 13.6. Explore permissions using the simple and advanced access tables
- 13.7. Create a custom detection rule in Cortex Cloud Identity Security
- 13.8. Perform advanced Identity Security investigations using XQL
- 13.9. Enable inactive human identity logs on Azure in Cortex Cloud Identity Security
- 13.10. Manage RBAC and SBAC in Cortex Cloud Identity Security

## 14. Cloud ASM

- 14.1. What is Cloud ASM?
- 14.2. Cloud ASM concepts
  - 14.2.1. Scanning
    - 14.2.1.1. Scanning cadences
    - 14.2.1.2. Scanning ports and protocols
    - 14.2.1.3. Scanning activity
  - 14.2.2. Network mapping
- 14.3. Enable Cloud ASM
- 14.4. Attack Surface Management detections
  - 14.4.1. Attack surface rules
  - 14.4.2. Externally inferred CVEs
- 14.5. Attack surface assets
- 14.6. Review your unmanaged cloud services
- 14.7. Review unmanaged cloud issues
- 14.8. Attack Surface Management FedRAMP support

## 15. Network exposure detection

- 15.1. What is Cloud Network Analyzer?
- 15.2. Internet exposure detection
- 15.3. Outbound exposure detection
- 15.4. East-west exposure detection
- 15.5. Investigate an internet exposure

## 16. Vulnerability management

- 16.1. Vulnerability management in Cortex Cloud
  - 16.1.1. Cortex Cloud vulnerability concepts
  - 16.1.2. Vulnerability Management dashboard
- 16.2. Cortex Vulnerability Risk Score
- 16.3. Vulnerability policies
  - 16.3.1. Create a vulnerability policy



- 16.3.2. Update the Ignored CVEs, Asset Groups, and Assets policy
- 16.3.3. Modify a vulnerability policy
- 16.3.4. Configure a block grace period
- 16.3.5. Enable or disable a vulnerability policy

#### 16.4. Investigate and remediate vulnerabilities

- 16.4.1. View all Vulnerabilities
- 16.4.2. View vulnerability issues
- 16.4.3. View All Vulnerability Findings
- 16.4.4. View vulnerable assets

#### 16.5. Vulnerability Intelligence

#### 16.6. Recast CVSS scores and CVSS severities

### 17. Cloud Security Rules and Policies

#### 17.1. Overview

#### 17.2. Cloud Security Rules

#### 17.3. Cloud Security Policies

- 17.3.1. Issues

#### 17.4. Create Rules

- 17.4.1. Create a configuration rule
  - 17.4.1.1. Guidelines for creating cloud security rules
  - 17.4.1.2. Cloud security rule status for custom configuration rules
- 17.4.2. Create a Data Rule
- 17.4.3. Create a Network Exposure Rule
- 17.4.4. Edit a Rule

#### 17.5. Create Policies

- 17.5.1. Edit a Policy
- 17.5.2. Use an Existing Policy to Create a New One

### 18. Cloud Workload Policies and Rules

#### 18.1. How policies and rules work together

#### 18.2. Cloud Workload Policies

- 18.2.1. Types of Cloud Workload Policies
  - 18.2.1.1. Trusted image cloud workload policies
- 18.2.2. Cloud Workload Policies page
  - 18.2.2.1. Widgets panel
    - 18.2.2.1.1. Show or hide the widget panel
  - 18.2.2.2. Change the layout of the policies table
  - 18.2.2.3. Policy Details Panel
- 18.2.3. Enable or disable a Cloud Workload Policy
- 18.2.4. Create a Cloud Workload Policy
- 18.2.5. Use an existing policy to create a new Cloud Workload policy
- 18.2.6. Edit a Cloud Workload Policy
- 18.2.7. Delete a Cloud Workload Policy
- 18.2.8. Cloud Workload Preventive Action

#### 18.3. Cloud Workload Rules

- 18.3.1. Default (pre-defined) Rules
- 18.3.2. Custom (user-defined) Rules
- 18.3.3. Cloud Workload Rules page
  - 18.3.3.1. Filter page results
  - 18.3.3.2. Change the layout of the rules table
  - 18.3.3.3. Rule details panel
- 18.3.4. Create a new Custom Detection Rule
- 18.3.5. Use an existing rule to create a new Custom Detection Rule
- 18.3.6. Edit a Custom Detection Rule
- 18.3.7. Delete a Custom Detection Rule

### 19. Serverless function posture security

#### 19.1. Onboard cloud providers for serverless functions

#### 19.2. Serverless function posture policies

- 19.2.1. Manage serverless function policies
- 19.2.2. Create serverless function policies

#### 19.3. Serverless function posture rules

- 19.3.1. Manage serverless function rules
- 19.3.2. Create serverless function rules
- 19.3.3. Create an attack path rule for serverless functions
- 19.3.4. Create a configuration rule for serverless functions
- 19.3.5. Create a network exposure rule for serverless functions

#### 19.4. Serverless function usage



## 20. Data management

### 20.1. Broker VM

- 20.1.1. What is the Broker VM?
- 20.1.2. Set up and configure Broker VM
  - 20.1.2.1. Broker VM image installations
    - 20.1.2.1.1. Set up Broker VM on Microsoft Azure
    - 20.1.2.1.2. Set up Broker VM on Alibaba Cloud
    - 20.1.2.1.3. Set up Broker VM on Amazon Web Services
    - 20.1.2.1.4. Set up Broker VM on Google Cloud Platform (GCP)
    - 20.1.2.1.5. Set up Broker VM on KVM using Ubuntu
    - 20.1.2.1.6. Set up Broker VM on Microsoft Azure
    - 20.1.2.1.7. Set up Broker VM on Nutanix Hypervisor
    - 20.1.2.1.8. Set up Broker VM on VMware ESXi using vSphere Client
  - 20.1.2.2. Broker VM data collector applets
    - 20.1.2.2.1. Activate DSPM Fileshare
    - 20.1.2.2.2. Activate Registry Scanner
    - 20.1.2.2.3. Activate Transporter
- 20.1.3. Manage Broker VM
  - 20.1.3.1. Edit Broker VM Configuration
  - 20.1.3.2. Increase Broker VM storage allocated for data caching
  - 20.1.3.3. Monitor Broker VM using Prometheus
  - 20.1.3.4. Collect Broker VM Logs
  - 20.1.3.5. Upgrade Broker VM
  - 20.1.3.6. Import Broker VM Configuration
  - 20.1.3.7. Open Live Terminal
  - 20.1.3.8. Add Broker VM to cluster
  - 20.1.3.9. Switchover Primary Node in Cluster
  - 20.1.3.10. Remove from Cluster
- 20.1.4. Broker VM High Availability Cluster
  - 20.1.4.1. Configure High Availability Cluster
  - 20.1.4.2. Manage Broker VM clusters
    - 20.1.4.2.1. View cluster details
    - 20.1.4.2.2. Edit cluster
    - 20.1.4.2.3. Add applet to cluster
    - 20.1.4.2.4. Add Broker VM to cluster
    - 20.1.4.2.5. Remove cluster
- 20.1.5. Broker VM notifications
- 20.1.6. Monitor Broker VM activity

### 20.2. Dataset management

- 20.2.1. What are datasets?
- 20.2.2. Lookup datasets
  - 20.2.2.1. Import a lookup dataset
  - 20.2.2.2. Download JSON file of lookup dataset
  - 20.2.2.3. Set time to live for lookup datasets
- 20.2.3. Monitor datasets and dataset views activity

### 20.3. Manage compute units

- 20.3.1. Compute units usage

### 20.4. Manage instances

- 20.4.1. Add a new data source or instance
- 20.4.2. Manage cloud instances
- 20.4.3. Update cloud permissions after Cortex release updates
- 20.4.4. Pending cloud instances
- 20.4.5. Manage Kubernetes Connector instances
- 20.4.6. Troubleshoot errors on cloud instances
- 20.4.7. Monitor serverless function scan health and status

### 20.5. About health issues

- 20.5.1. Investigate and resolve health issues

## 21. Marketplace

- 21.1. Cortex Marketplace
- 21.2. Content Pack Support Types
- 21.3. Cortex Cloud content
- 21.4. Manage content packs
- 21.5. Marketplace FAQs
- 21.6. Content changes when upgrading Cortex Cloud versions

## 22. Cortex CLI

- 22.1. Connect Cortex CLI
- 22.2. Cortex CLI common command line reference guide
- 22.3. Cortex CLI for API Security
  - 22.3.1. Cortex CLI API Security command line reference guide
- 22.4. Cortex CLI for Cloud Workload Protection
  - 22.4.1. Cloud Workload Protection command line reference



## 22.5. Cortex CLI for Code Security

- 22.5.1. Cortex CLI usage for Cortex Cloud Application Security
- 22.5.2. Cortex CLI Cortex Cloud Application Security command line reference

# 23. Cortex Cloud XQL

## 23.1. Get started with XQL

- 23.1.1. XQL language features
- 23.1.2. XQL Language Structure
  - 23.1.2.1. Adding comments in queries
- 23.1.3. Supported operators
- 23.1.4. Datasets and presets
- 23.1.5. About examples
- 23.1.6. JSON functions
- 23.1.7. How to filter for empty values in the results table
- 23.1.8. Understanding string manipulation in XQL

## 23.2. Build XQL queries

- 23.2.1. About the Query Builder
- 23.2.2. How to build XQL queries
  - 23.2.2.1. Get started with XQL queries
  - 23.2.2.2. Useful XQL user interface features
  - 23.2.2.3. XQL Query best practices
  - 23.2.2.4. Expected results when querying fields
  - 23.2.2.5. Create XQL query
  - 23.2.2.6. Review XQL query results
  - 23.2.2.7. Translate to XQL
  - 23.2.2.8. Graph query results
- 23.2.3. XQL query entities
  - 23.2.3.1. Create authentication query
  - 23.2.3.2. Create event log query
  - 23.2.3.3. Create file query
  - 23.2.3.4. Create image load query
  - 23.2.3.5. Create network connections query
  - 23.2.3.6. Create network query
  - 23.2.3.7. Create process query
  - 23.2.3.8. Create registry query
  - 23.2.3.9. Query across all entities
- 23.2.4. Overview of the Query Center
  - 23.2.4.1. Edit and run queries in Query Center
    - 23.2.4.1.1. Query Center reference information
- 23.2.5. Manage scheduled queries
  - 23.2.5.1. Scheduled Queries reference information
- 23.2.6. Manage your query library

## 23.3. Stages

- 23.3.1. alter
- 23.3.2. arrayexpand
- 23.3.3. bin
- 23.3.4. call
- 23.3.5. comp
- 23.3.6. config
  - 23.3.6.1. case\_sensitive
  - 23.3.6.2. timeframe
  - 23.3.6.3. max\_runtime\_minutes
- 23.3.7. dedup
- 23.3.8. fields
- 23.3.9. filter
- 23.3.10. getrole
- 23.3.11. iploc
- 23.3.12. join
- 23.3.13. limit
- 23.3.14. replacenull
- 23.3.15. sort
- 23.3.16. Tag
- 23.3.17. target
- 23.3.18. top
- 23.3.19. transaction
- 23.3.20. union
- 23.3.21. view
- 23.3.22. windowcomp

## 23.4. Functions

- 23.4.1. add
- 23.4.2. approx\_count
- 23.4.3. approx\_quantiles
- 23.4.4. approx\_top
- 23.4.5. array\_all
- 23.4.6. array\_any
- 23.4.7. arrayconcat



23.4.8. `arraycreate`  
23.4.9. `arraydistinct`  
23.4.10. `arrayfilter`  
23.4.11. `arrayindex`  
23.4.12. `arrayindexof`  
23.4.13. `array_length`  
23.4.14. `arraymap`  
23.4.15. `arraymerge`  
23.4.16. `arrayrange`  
23.4.17. `arraystring`  
23.4.18. `avg`  
23.4.19. `coalesce`  
23.4.20. `concat`  
23.4.21. `convert_from_base_64`  
23.4.22. `count`  
23.4.23. `count_distinct`  
23.4.24. `current_time`  
23.4.25. `date_floor`  
23.4.26. `divide`  
23.4.27. `earliest`  
23.4.28. `extract_time`  
23.4.29. `extract_url_host`  
23.4.30. `extract_url_pub_suffix`  
23.4.31. `extract_url_registered_domain`  
23.4.32. `first`  
23.4.33. `first_value`  
23.4.34. `floor`  
23.4.35. `format_string`  
23.4.36. `format_timestamp`  
23.4.37. `if`  
23.4.38. `incidr`  
23.4.39. `incidr6`  
23.4.40. `incidrlist`  
23.4.41. `int_to_ip`  
23.4.42. `ip_to_int`  
23.4.43. `is_ipv4`  
23.4.44. `is_known_private_ipv4`  
23.4.45. `is_ipv6`  
23.4.46. `is_known_private_ipv6`  
23.4.47. `json_extract`  
23.4.48. `json_extract_array`  
23.4.49. `json_extract_scalar`  
23.4.50. `json_extract_scalar_array`  
23.4.51. `json_path_extract`  
23.4.52. `lag`  
23.4.53. `last`  
23.4.54. `last_value`  
23.4.55. `latest`  
23.4.56. `len`  
23.4.57. `list`  
23.4.58. `lowercase`  
23.4.59. `ltrim, rtrim, trim`  
23.4.60. `max`  
23.4.61. `median`  
23.4.62. `min`  
23.4.63. `multiply`  
23.4.64. `object_create`  
23.4.65. `object_merge`  
23.4.66. `parse_epoch`  
23.4.67. `parse_timestamp`  
23.4.68. `pow`  
23.4.69. `rank`  
23.4.70. `regexecapture`  
23.4.71. `regextract`  
23.4.72. `replace`  
23.4.73. `replex`  
23.4.74. `round`  
23.4.75. `row_number`  
23.4.76. `split`  
23.4.77. `stddev_population`  
23.4.78. `stddev_sample`  
23.4.79. `string_count`  
23.4.80. `subtract`  
23.4.81. `sum`  
23.4.82. `time_frame_end`



23.4.83. timestamp\_diff  
23.4.84. timestamp\_seconds  
23.4.85. to\_boolean  
23.4.86. to\_epoch  
23.4.87. to\_float  
23.4.88. to\_integer  
23.4.89. to\_json\_string  
23.4.90. to\_number  
23.4.91. to\_string  
23.4.92. to\_timestamp  
23.4.93. uppercase  
23.4.94. values  
23.4.95. var  
23.4.96. wildcard\_match

## 24. Graph Search

- 24.1. What is Graph Search?
- 24.2. Get started with Graph Search queries
- 24.3. How to build Graph Search queries?
- 24.4. Understand Graph Search query results
- 24.5. Create Graph Search query
- 24.6. Graph Search examples
- 24.7. Manage the Graph Search Query Library
- 24.8. Edit and run queries in Query Center
  - 24.8.1. Query Center reference information
- 24.9. Supported assets and findings
- 24.10. FAQ on Graph Search

## 25. API specification inventory

- 25.1. Import API specification



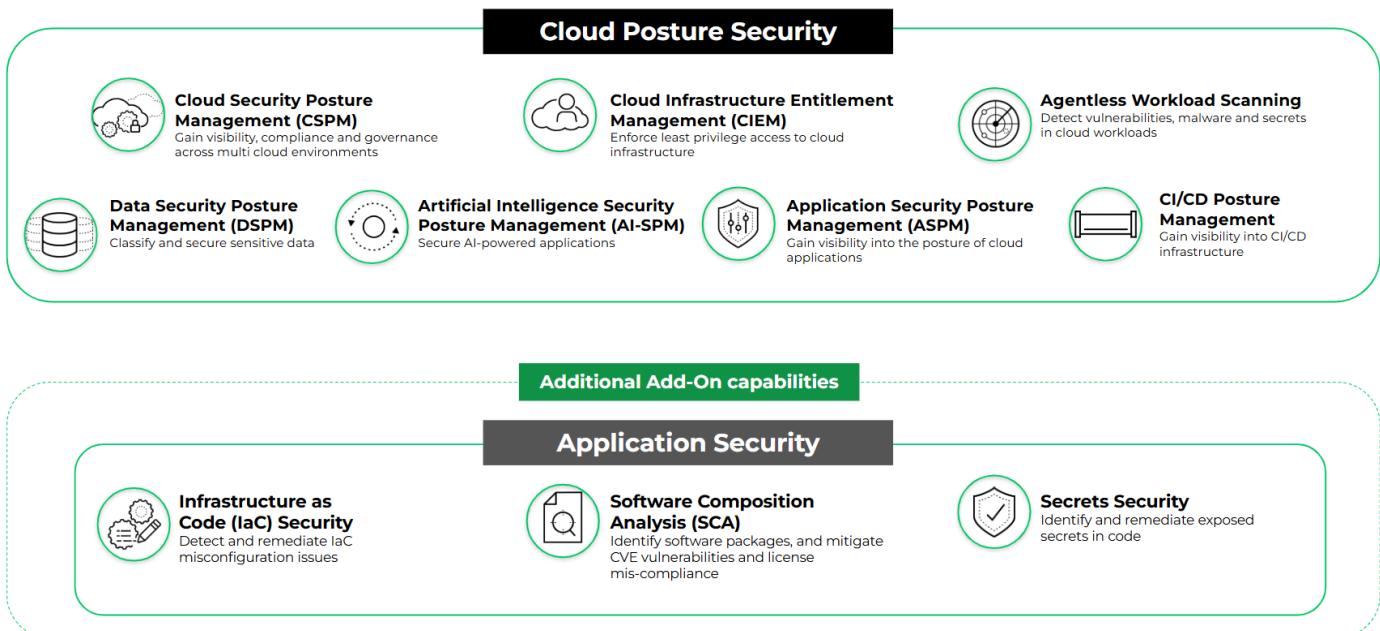
# 1 | Get started with Cortex Cloud

## 1.1 | What is Cortex Cloud?

Cortex Cloudâ€s comprehensive security solution helps you take a platform-based, proactive approach to securing your cloud estate from Code to Cloud to SOC. It provides real-time cloud security that allows you to investigate and remediate your cloud security issues from a single platform with all the signals in a single data lake.

Cortex Cloud is an easily extensible platform to consolidate Application Security, Cloud Posture Security, Runtime Security, and Security Operations (SOC). It is enterprise-ready for regulated organizations with data residency preserving scanning worldwide. It provides consolidated and flexible reporting for executives and operators for all cloud security postures. It also includes an AI Copilot across the platform to simplify your day-to-day activities.

- **Application Security:** Prevent issues from getting into your production environment.
- **Cloud Posture Security:** Reduce and prioritize risks already present in your cloud environment.
- **Cloud Runtime:** Stop an attacker from exploiting risks present in your cloud environment.
- **SOC:** Detect and respond.



### 1.1.1 | Key features

- **Visibility**: Get complete visibility across your entire cloud estate:
  - Discover your cloud inventory: Comprehensive and uniform inventory across all types of infrastructure across all cloud providers: Compute, APIs, Containers, Serverless, Data, AI Services, Identities, Networks.
  - Visualize asset relationships: Rich relationship graph demonstrates how assets and findings impact each other.
  - Simple, frictionless onboarding: View your entire cloud estate with agentless scanning.
- **Cloud risk assessment**: Comprehensive cloud risk assessment across all major cloud security posture domains:
  - Vulnerabilities
  - Misconfigurations
  - Access and permissions
  - Non-human identities and third-party exposure
  - AI risk and supply chain
  - Data exposure, sovereignty, and residency
  - Network exposure



- **Cloud vulnerability management** Vulnerability management across VMs, Containers, Serverless, and OSS packages:
  - Prioritize impactful vulnerabilities with context: Understand environmental factors such as severity, exploitability, patch availability, internet exposure and others.
  - Reduce the number of fixes: AI-driven detection consolidates related vulnerabilities with the same root cause— one fix resolves multiple issues.
  - Track KPIs: Understand Insights about the state of vulnerabilities in cloud native environments and their evolution over time.
- **Compliance** Uniform compliance management:
  - Validate industry regulation with dozens of built-in standards across security, privacy, and AI: PCI DSS, HIPAA, GDPR, NIST, ISO, and more.
  - Meet unique organizational requirements: Create custom compliance rules and standards.
  - Generate audit-ready reports: Export, schedule, and share compliance reports with stakeholders.
- **Attack path analysis:**
  - Detect critical risks: Discover combinations of individual risk signals that form attack paths.
  - Overly permissive identities, network exposures, sensitive data, misconfigurations, vulnerabilities
  - Prioritize harmful risks: Uncover which misconfigurations enable lateral movement to high-value assets such as sensitive data stores.
  - Gain end-to-end visibility: Visualize attack paths in a rich graph, gaining full risk context.
- **Cases:**
  - Dramatically reduce alerts: AI-driven detection consolidates related risks and attack paths into a high priority case.
  - Enable full context for effective mitigation: Clearly identify high-impact posture issues, preventing wasted resources on less significant threats.
  - Resolve numerous issues with a single action driven by AI and automation.
- **Ecosystem Integration and Automation:**
  - Powerful Ecosystem: Cortex Cloud integrates with your entire ecosystem with thousands of third-party integrations ranging from workflow solutions to security vendors.
  - Out Of the Box Remediation Playbooks: Cortex Cloud offers many playbooks for remediating security issues to reduce MTTR.
  - Build your own Remediation Playbooks: Cortex Cloud offers a no code automation wizard to build your own security playbooks.

## 1.2 | What is Cortex Cloud Posture Management?

### Abstract

Learn about Cortex Cloud Posture Management and the key integrated capabilities.

Cortex Cloud Posture Management includes:

- **Visibility:** Provides agentless, comprehensive visibility across cloud environments, including IaaS, PaaS, Kubernetes, containers, serverless functions, networks, and storage services in a unified cloud asset inventory.
- **Posture Management:** Supports configuration assessment, compliance monitoring, vulnerability management, code-to-cloud remediation, and reporting. Includes attack path analysis to aggregate potential risks.
- **Data, Identity, and Application Security:** Deploys quickly to deliver real-time visibility and protection across cloud environments.



## 1.3 | Agentic AI in Cortex Cloud

### Abstract

Use the Cortex Agentic Assistant to investigate cases, perform threat hunting, and create scripts. Embed and run LLM prompts in playbooks. View AI case summaries.

Cortex Cloud integrates advanced artificial intelligence to streamline security operations. Through the Cortex Agentic Assistant, the platform provides a unified interface for interacting with both system-provided and custom AI agents capable of creating and executing multi-step plans. These agents leverage specific capabilities to perform actions across your infrastructure, facilitating deep case investigations and proactive threat hunting while allowing for the creation of tailored automation.

### Key AI Capabilities

- **Agents Hub:** A centralized hub for managing agents and actions. System agents can be enabled and disabled, and you can create custom agents tailored to your organizational needs, including the ability to execute custom scripts.
- **Automation Engineer Agent:** Provides a natural language interface to draft, refine, and deploy automation scripts.
- **MCP Integration:** Supports the configuration of integrations that communicate with external MCP servers, enabling agents to access third-party tools and data sources via a standardized protocol.
- **Embedded AI Prompts:** Facilitates the inclusion of generative AI tasks within playbooks. These prompts function as standalone workflow steps to analyze data or generate content without requiring a dedicated agent.
- **AI-Generated Case Summaries:** Automatically generate technical overviews of security incidents. These summaries consolidate complex telemetry and impact data into high-level reports to accelerate initial triage and stakeholder reporting.

### 1.3.1 | Cortex Agentic Assistant

#### Abstract

Learn about the Cortex Agentic Assistant and key integrated capabilities.

Cortex Agentic Assistant is the autonomous "brain" of Cortex Cloud. It utilizes AI agents that plan, reason, and investigate complex threats, such as cloud identity theft or container breaches. Cortex Agentic Assistant enables security operations teams to use natural language prompts to interact with AI agents. The agents have access to case context and can create plans and perform actions such as running commands, playbooks, and scripts.

To enable the Cortex Agentic Assistant, go to Settings → Configurations → General → Server Settings → Agentic Assistant.

#### NOTE:

By default, you have access to the Cortex Assistant, which includes a natural language interface for entity investigation and provides a list of recommended responses such as running a playbook, performing a scan, or collecting support files.

If you enable the Cortex Agentic Assistant, it replaces the Cortex Assistant interface entirely.

For more information, see [Compare Agentic Assistant with Cortex Assistant](#).

#### Supported regions for Cortex Agentic Assistant

The Cortex Agentic Assistant is currently available for tenants in the following regions:

- Australia (AU)
- Canada (CA)
- France (FA)
- Germany (DE)
- India (IN)
- Japan (JP)
- Netherlands (EU)
- Singapore (SG)
- South Korea (KR)
- United Kingdom (UK)
- United States (US)

Cortex Agentic Assistant is based on an ecosystem of agents and actions.

The Cortex Agentic Assistant includes system agents that are mission-focused, as well as the ability to create custom agents. Analysts focused on general investigations might build custom agents that include all the actions required to perform their daily tasks.



Each agent is assigned actions it can execute. System actions can be based on playbooks, scripts, commands, or AI prompts. You can also register custom actions, which are based on scripts, commands, or AI prompts.

Access to the Cortex Agentic Assistant and the ability to manage agents and actions is restricted by role-based access controls. Actions marked as sensitive require manual approval, and all actions an agent executes are logged.

#### TIP:

The system Help Center Agent provides fast access to documentation. You can ask natural language questions, such as "How do I create a dashboard?" or "Where can I review my data retention policies?" and the agent retrieves concise, relevant information from the official documentation site.

To view how your organization utilizes the Cortex Agentic Assistant, including information on agent plans, user prompts, as well as open cases, see the Cortex Agentic Assistant dashboard.

### 1.3.1.1 | Agentic Assistant use cases

#### Abstract

Recommended prompts to automate your SOC using the Cortex Agentic Assistant

Discover how Cortex Cloud can streamline your security operations by exploring some key use cases.

#### Chat prompt examples

Using chat prompt conversation starters in the Agentic Assistant simplifies and speeds up your interactions by providing pre-defined, common queries that guide you to relevant actions and information.

For example, a SOC analyst may see the following conversation starters under the chat prompt:

- What are the top issues I should prioritize today?
- Show me all issues with an overdue SLA
- Which automations are waiting for my input?

Additional examples of possible relevant prompts are:

- Read this Unit42 blog and get all the CVEs. For every critical CVE found, check if my assets are vulnerable and isolate them.
- List recent security issues with high severity and an affected hostname that includes 'server'.
- Summarize the latest security issues from the past 24 hours
- How do I make a loop inside a playbook?
- What is the riskiest unresolved issue affecting our critical infrastructure?
- Show recent SSO-related issues
- Investigate this phishing issue and determine the source of the email and block any malicious indicators.

For more information on investigations, see Use Cortex Agentic Assistant chat in an investigation.

### 1.3.1.2 | Agentic Assistant security

#### Abstract

Learn about how the Agentic Assistant is built using responsible AI principles.

The Agentic Assistant is built on responsible AI principles to ensure its use is safe, fair, and trustworthy. We design our AI to be transparent about its actions, accountable for its decisions, and fair in its operations, avoiding biases.

The following describes how the Agentic Assistant protects sensitive data and gives you control and understanding over its automated actions.

#### Access control and permissions

#### User roles and RBAC options

Instance and Account admins have full control over the permissions and access that users have to the Cortex Agentic Assistant. Cortex Cloud uses Role-Based Access Control (RBAC) to manage access to the chat, as well as access to view, create, edit, delete, disable, and enable Agents and Actions in the Agents Hub.

#### Action Execution Scope

Agents can only use actions that have been assigned to them, and execution is limited to the user's existing permissions in your Cortex Cloud tenant. If a required integration is not active, its commands and any actions that wrap them will not work.



#### How sensitive data is protected

Data is hosted and encrypted by default on a dedicated Google Cloud Platform (GCP) project, and is isolated and protected by your specific IAM permissions. Google's multi-tenant architecture enforces strict data separation between customers.

#### User approval for sensitive actions

Actions marked as sensitive require explicit user approval before execution and are never run automatically. This gives you final control over critical or data-modifying steps.

#### Data user policy

Your prompts and outputs are processed only to generate the immediate response. They are not collected for model training or shared with third parties.

#### Data residency

All prompts and responses stay inside that regionâ€ s compute boundary, aligning with modern data-residency practices.

#### Transparency

#### How the Cortex Agentic Assistant maintains transparency

You can see how the agent reaches its answer. Click the down arrow next to Plan, to view how the user input was interpreted, the planned steps, and the actions used. You can view JSON artifacts created during the plan execution, when data was retrieved or an object was created.

In addition, all actions an agent takes are saved in an audit dataset. You can see which agent ran which action, and which user invoked it.

## 1.4 | Use the interface

With Cortex Cloud you can see your cloud environment mapped in a more visual way to get a better understanding of your cloud estate. Once you log in to Cortex Cloud, the Cloud Security Command Center is displayed, which provides you with a birdâ€ s eye view of your entire cloud ecosystem.

After you onboard your cloud or code providers, the data collected by Cortex Cloud is mapped into Asset groups.

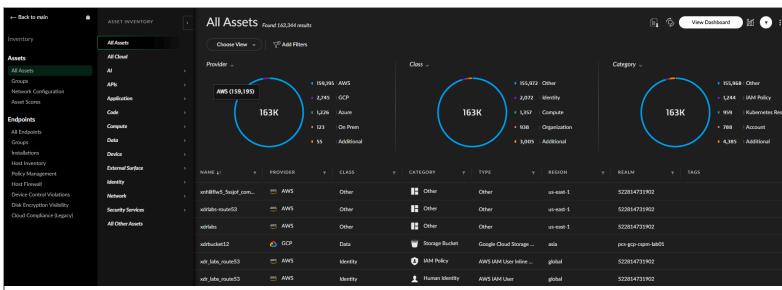
- The different types of data being ingested such as, audit logs, configurations, data coming from workloads is displayed on the left.
- The breakdown of the different parts of your environment including:
  - Compute (VMs, images, repositories)
  - Data (databases, storage)
  - Identities (human, non-human such as, service accounts), are displayed in the center.
- Finally, the several hundred posture risk issues that Cortex Cloud detected are now grouped into few Posture Cases that you can remediate are displayed on the right of the Command Center UI.



The Command Center also provides you details on the total number of assets in your environment, number of issues closed as well as the amount of time saved.

Cortex Cloud includes a unified **Asset Inventory**, which provides a complete list of your different assets in a single place. Here you can see your AI models and deployments, Applications, APIs, and all your Compute instances, Data assets, and Identities.

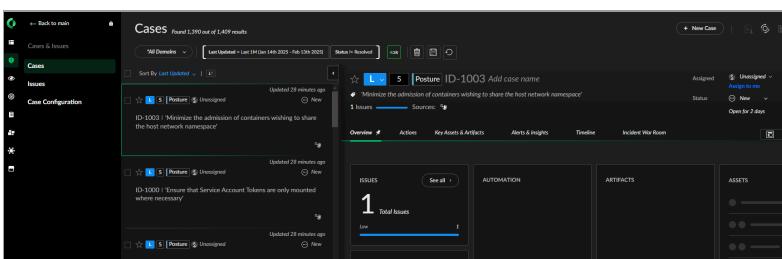




Select View Dashboard to get an in-depth view of all your assets.



Now that you have an overview of your environment and all the assets, you can navigate to **Cases** to view and resolve your issues as well as create a New Case.



Now that you have familiarized yourself with Cortex Cloud, consider taking the following actions to begin securing your cloud resources:

- Configure user roles and permissions
- Onboard your cloud accounts and data sources
- View dashboards and assets

## 1.5 | In-product support case creation

### Abstract

Open a support case directly in Cortex Cloud and record your console to capture your issues and have the case handled efficiently.

To simplify the process of creating a support case, you can open a support case directly in Cortex Cloud. Opening the case in Cortex Cloud allows all of the relevant context to be included, such as the option to record the console and upload relevant logs. When relevant, Cortex Cloud will create and send the agent tech support file (TSF) for the endpoint you select. All relevant data about your tenant is logged and included in the support case, including license details. Using the Cortex Cloud Create Support Case Wizard makes it easier for you to include all of the necessary details and log files while first submitting your support case, thereby enabling the support team to solve it more quickly and easily.

To use the embedded support case feature, you must have a user account in the Customer Support Portal, and your Cortex Cloud user must be granted the Help permission in Cortex Gateway.

- From Cortex Cloud, select Help → Submit a Support Case.
- In the Submit Support Case wizard, enter the requested case information. Be precise when indicating the impact of the issue. When an issue is critical, you will be asked to input the most critical information so that support can understand the issue and start addressing it immediately.

### NOTE:



When opening a support case through the Customer Support Portal, you need to manually select Cortex Cloud as the product. While there may be discrepancies between the categories in this wizard and the Customer Support Portal process, that's because this wizard is designed specifically to focus on options relevant to Cortex Cloud.

3. To provide more context for your support case, you can record the Cortex Cloud console directly from the support case wizard. If you choose to record the console, you can also opt to have the HAR file generated and sent to further assist support in solving the case. To record the console, select Record Console. To submit your support case without recording the console, select Skip.

4. If you choose to record the console, your browser may prompt you for permission for Cortex Cloud to see the contents of the tab. To allow recording, select Allow. You can now recreate the issue in your Cortex Cloud environment and all of your actions are recorded. The console recording and HAR file generation only take place within the context of the browser tab that Cortex Cloud is running in. When you are ready to stop recording, select Stop Sharing.

If you wish to recreate the recording, you must first delete the existing console recording by clicking the x symbol next to the Console Recording. Then select Record Console.

**NOTE:**

Console recordings cannot exceed 10 minutes. The current recording time is displayed at the top of the window.

5. To submit the support case, click Submit Support Case.

While the case attachments are uploading, do not refresh or navigate away from Cortex Cloud until you get a notification in the Notification Center that uploading is complete. In the meantime, you can close this wizard and continue working in Cortex Cloud.

Once the support case is created successfully, the support case number is displayed and you will receive an email notification from Palo Alto Networks Support. You can manage the support case and monitor its progress in the Customer Support Portal.

## 1.6 | Understand your user persona

### Cloud security engineers

Cloud security engineers or architects design and maintain a system that protects everything their organization hosts across various cloud service providers. Their goal is to achieve zero critical risks and compliance violations without blocking the productivity of other teams. Their responsibilities include:

- Deploying and managing cloud security tooling
- Performing cloud risk assessments (zero day vulnerability impact analysis)
- Detecting, prioritizing, and remediating cloud security alerts
- Collaborating with cross-functional teams to reduce risk (DevOps, App owners)
- Maintaining and monitoring compliance posture
- Generating security reports

With Cortex Cloud, cloud security engineers can:

- Get complete visibility without blind spots across multi cloud environments
- Manageable alerts
- Avoid manual parsing that prolongs risk assessment and reporting efforts
- Get better risk context that aids prioritization and remediation efforts with cross-functional teams

## 1.7 | Fair Usage policy for Cortex Cloud

To ensure the reliability, efficiency, and availability of Cortex Cloud for all the users, we expect our customers to use it fairly, reasonably, and in a manner that does not adversely impact the productâ€¢'s overall system performance. Cortex Cloud offers various features for connecting external resources to Cortex Cloud, including without limitation, frequency and/or volume of data ingestion, number of connected data sources, and API usages. Overuse or misuse of these features may adversely affect the reliability, efficiency, and/or availability of Cortex Cloud.

You are therefore required to utilize a reasonable volume of data ingestion, number of connected data sources, and API usage, based on your number of cloud assets protected by Cortex Cloud (â€¢ Fair Usage Policyâ€¢). If, in our sole and reasonable discretion, we determine that your usage of Cortex Cloud violates this Fair Usage Policy, we reserve the right to take appropriate action regarding such use, including without limitation, limiting the frequency and/or volume of data ingestions, limiting the number of connected data sources, and/or limiting the API usage, to bring your usage of Cortex Cloud in alignment with this Fair Usage policy.

## 1.8 | Understand license plans



Cortex Cloud Posture Management and Cortex Cloud Runtime Security licensing is provided via an annual subscription, based on the number and type of cloud resources protected. The fundamental metric for consumption is the protected workload. You must procure a license capacity sufficient to cover the total number of workloads you intend to secure.

Licensing is subject to a metering system or Fair Usage policy. This mechanism defines how usage is tracked and what happens when the average consumption of protected workloads exceeds the purchased license capacity. Cortex Cloud accounts for workload utilization based on a 90-day average to smooth spikes and drops in usage of highly ephemeral workloads. Exceeding capacity often triggers a notification, but usually does not immediately disable security functions to ensure your workloads don't lose their protection.

To view the product license and add-ons associated with your tenant, go to Settings → [Cortex License](#).

#### Protected workloads

A workload represents any active compute entity that requires protection. These workloads count toward your Cortex Cloud license usage. Examples include:

Table 1. Billable Workload Units

Workload Type	Billable Units
VMs not running containers	1 VM
VMs running containers	1 VM
Endpoint	1 Endpoint
CaaS (Container As A Service)	10 Agent Protected Managed Containers
Cloud Buckets	10 Cloud Buckets
Managed Cloud Database (PaaS)	2 PaaS Databases
DBaaS TB Stored	DBaaS 1TB Stored
SaaS Users	10 SaaS Users
On-Premise Data assets	1 Connection
Cloud ASM → Service	4 Unmanaged Assets
Container Images in Registries	<p><b>Free quota:</b> 10 container image scans per deployed workload (VM/CaaS)</p> <p><b>Beyond free quota:</b> 10 container image scans</p>
CLI Image Scans	-

Cortex Cloud Posture Management and Cortex Cloud Runtime Security are available in multiple license configurations, either individually or as part of a bundled package. For more information on bundling options with other Cortex products, see [Cortex XSIAM product licenses](#).



License	Configuration
Cloud Posture Management	<p>Agentless comprehensive visibility across your cloud environment. Includes the following:</p> <ul style="list-style-type: none"> <li>• Cloud Security Posture Management (CSPM)</li> <li>• Cloud Infrastructure Entitlement Management (CIEM)</li> <li>• Application Security Posture Management (ASPM)</li> <li>• Data Security Posture Management (DSPM)</li> <li>• Artificial Intelligence Security Posture Management (AI-SPM)</li> <li>• Cloud Attack Surface Management (ASM)</li> <li>• Kubernetes Security Posture Management (KSPM)</li> <li>• CI/CD Posture Management</li> <li>• Agentless Workload Scanning</li> </ul>
Cloud Runtime Security	<p>Full cloud protection, detection, and response. Includes the following:</p> <ul style="list-style-type: none"> <li>• Cloud Posture Management</li> <li>• Cloud Workload Protection (CWP)</li> <li>• Web Application &amp; API Security (WAAS)</li> </ul>

#### Add-ons

- **Security add-ons:** You can purchase security add-ons to expand the core capabilities of your Cortex Cloud Posture Management and Cortex Cloud Runtime Security licenses.
  - Data Ingestion
  - Application Security (IAC Security, SCA, Secrets Security)
  - Enterprise Runtime Security (XDR)
  - Identity Threat Detection and Response (IDTR)
  - Forensics investigation
  - Host Insights
  - Extended Threat Hunting (XTH)
  - Advanced Email Security
  - Data Loss Prevention (DLP) - Beta
- **Capacity add-ons:** You can purchase capability add-ons to extend the duration that security and telemetry data are retained for investigation and compliance purposes
  - Data Retention: Cortex Cloud Posture Management and Cortex Cloud Runtime Security retention per dataset.
  - Query Capacity (compute units): A single Compute Unit add-on.

#### License usage and overflow rules

Cortex tracks license usage to ensure that your purchased capacity is used efficiently. The system distinguishes between different workload types and applies clear rules to avoid double-counting and handle usage that exceeds purchased limits.

Cortex categorizes workloads as follows:

- Cloud Posture Workloads – Total workloads purchased with a Cloud Posture Management license, including any security add-ons.
- Cloud Runtime Workloads – Total workloads purchased with a Cloud Runtime license.

#### NOTE:



A Cloud Runtime license includes both Posture Scanning and Runtime Protection on the same asset. Usage, including any overflow, is tracked automatically to ensure accurate reporting across both licenses without duplicate counting.

#### Overflow rules

The following table outlines how the system counts workloads based on your purchased licenses and current usage:

Licenses Purchased	Usage Scenario	License Counter Display	Overflow Behaviour
Cloud Posture Only	Total posture workloads exceed quota.	All usage counts are shown under Cloud Posture Workload	All workload usage, including over-quota workloads, counts toward the Posture license.
Cloud Runtime Only	Total runtime workloads exceed quota.	All usage counts are shown under Cloud Runtime Workload	All workload usage, including over-quota workloads, counts toward the Runtime license.
Both Cloud Posture and Cloud Runtime	Workloads are within quota limits.	Posture: Counts toward Posture quota.  Runtime: Counts toward Runtime quota.	No workload overflow. Counters show usage within purchased quotas.
Both Cloud Posture and Cloud Runtime	Posture exceeds quota, Runtime has remaining capacity	Posture: 100% full usage.  Runtime: Partial or full usage count due to spillover.	Spillover occurs only from Posture to Runtime; it does not occur in reverse. Excess Posture workloads use the available Runtime quota until it's full.
Both Cloud Posture and Cloud Runtime	Runtime quota full	Posture: Total usage (including excess).  Runtime: Total usage (over-quota)	Spillover only occurs from Posture to Runtime; it does not occur in the reverse. Excess Posture workloads are added back to the Posture counter, and any over-quota usage is shown there.

#### 1.8.1 | Data retention

##### Abstract

Learn more about the default retention periods for all Cortex Cloud licenses and the available retention add-ons.

After purchasing your license retention add-ons, you can view details about your Cortex Cloud licenses and retention add-ons by selecting Settings à Cortex Cloud License. For more information on your storage license details, see Dataset Management.

##### Default retention periods

The following table summarizes the default retention periods for Cortex Cloud:

Data Type	Default Retention Period
Ingested data	31 days
Cases and Issues data	186 days

##### NOTE:

Case data is retained according to the Last Updated date.

Issue data is retained according to the Observation Time. Data collected within these dates is kept and displayed for 186 days. To ensure the accuracy of issues, Cortex Cloud provides a grace period of up to 31 days for issues displayed in the Issues View, Issues table, and Cases View.



Data Type	Default Retention Period
Forensic data	<p>365 days</p> <p><b>NOTE:</b> Requires the Forensics add-on.</p>
Audit logs	365 days
Query data	186 days

#### Retention add-ons

Retention add-ons are provided for ingested data and Cases and Issues data. Minimum requirements are dependent on the license type. You can purchase one or more of the following add-ons:

Feature	Description
Additional Cases and Issues Retention	<p>An additional 31-day hot storage of Case and Issue data apart from the default 186 days.</p> <p>Available for purchase per month for each endpoint.</p>
Period-Based Retention - Hot Storage (All datasets)	<p>Fully searchable storage for investigation and threat hunting of ingested data, and Cases and Issues data.</p> <p>Requires purchasing a minimum of one month of the additional retention.</p>
Additional Hot Storage (Selected datasets)	<p>Flexible hot storage-based retention to help accommodate varying storage requirements for different retention periods and datasets. Fully searchable storage for investigation and threat hunting of ingested data.</p> <p>Available for purchase with storage for a minimum of 1,000 GB.</p>
Period-Based Retention - Cold Storage	<p>Lower-cost storage of ingested data for long-term compliance needs with limited search options.</p> <p>Requires purchasing a minimum of six months of additional retention.</p>

## 2 | Onboard and configure Cortex Cloud

### Abstract

Learn about the deployment preparation and procedures to onboard and configure Cortex Cloud.

Plan and prepare your Cortex Cloud deployment. Then, activate and configure your Cortex Cloud tenant using the Deployment steps.

Onboard your cloud assets for automation and core analytics, data ingestion, enterprise runtime security, cloud posture security and cloud runtime security.

Depending on your license and add-ons, onboard your cloud assets and modules.

### 2.1 | Plan and prepare

#### Abstract

Learn more about deployment considerations and onboarding steps.

#### Prepare for deployment

Before you get started with Cortex Cloud, consider the following:



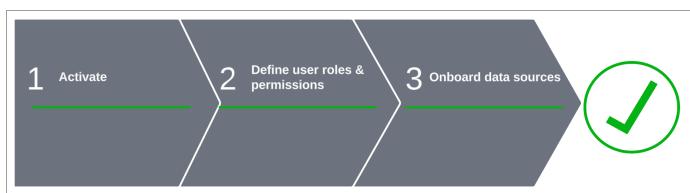
- Determine the amount of log storage you need for your Cortex Cloud deployment. Talk to your partner or sales representative to determine whether you must purchase additional storage within the Cortex Cloud tenant.
- Determine the region in which you want to host Cortex Cloud and any associated services, such as Directory Sync Service. If you plan to stream data from a Strata Logging Service instance, it must be in the same region as Cortex Cloud. For more information, see Cortex Cloud supported regions.

## 2.2 | Deployment steps and checklist

### Abstract

Review the steps to onboard and configure Cortex Cloud.

Review the plan and prepare considerations, and then use the onboarding checklist to deploy and onboard successfully Cortex Cloud.



- Step 1: Activate Cortex Cloud. Activate and log in to Cortex Gateway.
- Step 2: Configure user roles and access.
- Step 3: Onboard data sources.
- Perform a health check.

### 2.2.1 | Activate Cortex Cloud

#### Abstract

Learn how to activate your tenant.

To activate a tenant, you need to log in to Cortex Gateway, a centralized portal for activating and managing tenants, users, roles, and user groups. After activating the tenant, you can then access the tenant. You must repeat this task for each tenant if you have multiple tenants. The activation process involves accessing Cortex Gateway, activating the tenant, and then accessing the tenant's resources.

#### PREREQUISITE:

- The Cortex Cloud activation email.
- A Customer Support Portal (CSP) account.

You need to set up your CSP account. For more information, see [How to Create Your CSP User Account](#).

When you create a CSP account, you can set up two-factor authentication (2FA) to log into the CSP by using an Email, Okta Verify, or Google Authenticator (non-FedRAMP accounts). For more information, see [How to Enable a Third Party IdP](#).

- You have one of the following roles assigned:

Role	Description
CSP role	The Super User role is assigned to your CSP account. The user who creates the CSP account is granted the Super User role.
Cortex role	<p>You must have the Account Admin role.</p> <p>If you are the first user to access Cortex Gateway with the CSP Super User role, you are automatically granted Account Admin permissions for the Cortex Gateway. You can also add Account Admin users as required.</p> <p>In the Cortex Gateway, you can activate new tenants, access existing tenants, and create and manage role-based access control (RBAC) for all of your tenants.</p>

#### How to activate Cortex Cloud

1. Log in to Cortex Gateway.

You can also access the link from the activation email.

2. Enter your username and password or multi-factor authentication (if set up) by using your Customer Support Portal account credentials to sign in.

After you sign in, you can view the following:



- If you are a CSP Account Admin, you can see tenants allocated to your CSP account and ready for activation. After activation, you cannot move your tenant to a different CSP account.
- Tenant details such as license type, number of endpoints, and purchase date.
- Tenants that were activated and are now available. If you have more than one Customer Support Portal account, the tenants are displayed according to the Customer Support Portal account name.

3. In the Available for Activation section, use the serial number to locate the tenant that needs activation, and then click Activate.

4. On the Tenant Activation page, define the following:

Parameter	Description
Tenant Name	Enter the name of the tenant. Use a unique name across your company account up to 59 characters long.
Region	
Tenant Subdomain	DNS record associated with your tenant. Enter a name that will be used to access the tenant directly using the full URL: <code>https://&lt;subdomain&gt;xdr.&lt;region&gt;.paloaltonetworks.com</code>

5. Review and agree to the terms and conditions of the Privacy policy, Terms of Use, and EULA , and then Activate your tenant.

**NOTE:**

Activation can take about an hour and does not require you to remain on the activation page. Cortex Cloud sends a notification to your email when the process is complete.

6. After activation, from Cortex Gateway, in the Available Tenants, when hovering over the activated tenant, do the following:

- Ensure that you can successfully access the tenant by clicking the Cortex Cloud tenant name (when the tenant is active).
- In the dialog box, view the tenant status, region, serial number, and license details.

**NOTE:**

You can only change the subdomain once, and it cannot be undone.

After deleting the subdomain, you can reuse it after 7 days.

7. Enable and verify access to Cortex Cloud communication servers, storage buckets, and various resources in your firewall configuration. For more information, see Enable access to required PANW resources.

#### 2.2.1.1 | Cortex Cloud supported regions

##### Abstract

Supported regions in which you want to host Cortex Cloud and any associated services.

The following table lists the regions available to host Cortex Cloud and any associated Cortex services:

Country	Description
Australia (AU)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Australia.
Canada (CA)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Canada. However, if you have a WildFire Canada cloud subscription, consider the following: <ul style="list-style-type: none"> <li>• You cannot send file submissions for bare-metal analysis.</li> <li>• You will not be protected against macOS-borne zero-day threats. However, you will receive protection against other macOS malware in regular WildFire updates.</li> </ul>
Europe (EU)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Europe.



<b>Country</b>	<b>Description</b>
France (FR)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of France.
Germany (DE)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Germany.
India (IN)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of India.
Indonesia (ID)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Indonesia.
Israel (IL)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Israel.
Italy (IT)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Italy.
Japan (JP)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Japan.
Poland (PL)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Poland.
Qatar (QT)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Qatar.
Saudi Arabia (SA)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Saudi Arabia.
Singapore (SG)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Singapore.
South Africa (ZA)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of South Africa.
South Korea (KR)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of South Korea.
Spain (ES)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Spain.
Switzerland (CH)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Switzerland.
Taiwan (TW)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of Taiwan.
United Kingdom (UK)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of the United Kingdom.
United States (US)	All Cortex Cloud logs and ingested data remain hosted within the boundaries of the United States.

#### 2.2.1.2 | Enable access to required PANW resources

##### Abstract

Learn more about enabling network access to the Cortex Cloud resources.



After you receive your account details, enable and verify access to Cortex Cloud communication servers, storage buckets, and various resources in your firewall configuration. Some of the IP addresses required for access are registered in the United States. As a result, some GeoIP databases do not correctly pinpoint the location where IP addresses are used. All customer data is stored in your deployment region, regardless of the IP address registration, and data transmission is restricted through any infrastructure to that region.

Before configuring your firewall, review these guidelines:

- Palo Alto Networks App-IDs (firewall policy): If you are using a Palo Alto Networks Firewall, you can simplify your configuration by using App-IDs. If you add the specific App-IDs (for example, `cortex-xdr`, `traps-management-service`) to your firewall security policy, you do not need to allow specific IP addresses listed below manually
- App-ID limitations: A dash (–) indicates there is no App-ID coverage for a specific resource. For these rows, you must configure your firewall to allow access based on the IP address and port.
- Rule direction: Enable access from the Cortex XDR Agent to the tenant (outbound); this traffic does not need to be bidirectional.
- Google Cloud Platform (GCP): For resources listing IP ranges in the GCP, go to the official JSON feeds for the specific IP addresses required for your deployment:
  - Global subnets: <https://www.gstatic.com/ipranges/goog.json>
  - Regional ranges: <https://www.gstatic.com/ipranges/cloud.json>
- SSL decryption: If you use SSL decryption and experience difficulty connecting the Cortex XDR agent to the server, we recommend that you add the FQDNs required for access to your SSL Decryption Exclusion list in Device → Certificate Management → SSL Decryption Exclusion.

**NOTE:**

`<tenant-name>` refers to the selected subdomain of your Cortex Cloud tenant, and `<region>` is the region in which your tenant is deployed. For more information, see Cortex Cloud supported regions.

The following table lists the required resources by region, including FQDNs, IP addresses, ports, and App-ID coverage for your deployment:

FQDN	IP Addresses And Port	App-ID Coverage
Egress		



FQDN	IP Addresses And Port	App-ID Coverage
<p>&lt;tenant-name&gt;.xdr. &lt;region&gt;.paloaltonetworks.com</p> <p>Used to connect to the Cortex Cloud tenant.</p>	<p>IP address by region:</p> <ul style="list-style-type: none"> <li>• US (United States): 35.244.250.18:443</li> <li>• EU (Europe): 35.227.237.180:443</li> <li>• CA (Canada): 34.120.31.199:443</li> <li>• UK (United Kingdom): 34.120.87.77:443</li> <li>• JP (Japan): 35.241.28.254:443</li> <li>• SG (Singapore): 34.117.211.129:443</li> <li>• AU (Australia): 34.120.229.65:443</li> <li>• DE (Germany): 34.98.68.183:443</li> <li>• IN (India): 35.186.207.80:443</li> <li>• DL (Delhi): 34.8.67.192:443</li> <li>• CH (Switzerland): 34.111.6.153:443</li> <li>• PL (Poland): 34.117.240.208:443</li> <li>• TW (Taiwan): 34.160.28.41:443</li> <li>• QT (Qatar): 35.190.0.180:443</li> <li>• FA (France): 34.111.134.57:443</li> <li>• IL (Israel): 34.111.129.144:443</li> <li>• SA (Saudi Arabia): 35.244.157.127:443</li> <li>• ID (Indonesia): 34.111.58.152:443</li> <li>• ES (Spain): 34.111.188.248:443</li> <li>• IT (Italy): 34.8.224.70:443</li> <li>• KR (South Korea): 34.54.5.247:443</li> <li>• ZA (South Africa): 34.149.165.12:443</li> <li>• BR (Brazil): 34.96.83.202:443</li> </ul>	cortex-xdr
<p>distributions.traps.paloaltonetworks.com</p> <p>Used for the first request in registration flow where the agent passes the distribution id and obtains the ch-&lt;tenant-name&gt;.traps.paloaltonetworks.com of its tenant.</p>	<ul style="list-style-type: none"> <li>• IP address: 35.223.6.69</li> <li>• Port: 443</li> </ul>	traps-management-service



FQDN	IP Addresses And Port	App-ID Coverage
<p><a href="https://lrc-&lt;region&gt;.paloaltonetworks.com">https://lrc-&lt;region&gt;.paloaltonetworks.com</a></p> <p><a href="wss://lrc-&lt;region&gt;.paloaltonetworks.com">wss://lrc-&lt;region&gt;.paloaltonetworks.com</a></p> <p>Used in live terminal flow.</p>	<p>IP address by region:</p> <ul style="list-style-type: none"> <li>• US (United States): 35.190.88.43:443</li> <li>• EU (Europe): 35.244.251.25:443</li> <li>• CA (Canada): 35.203.99.74:443</li> <li>• UK (United Kingdom): 35.242.159.176:443</li> <li>• JP (Japan): 34.84.201.32:443</li> <li>• SG (Singapore): 34.87.61.186:443</li> <li>• AU (Australia): 35.244.66.177:443</li> <li>• DE (Germany): 34.107.61.141:443</li> <li>• IN (India): 35.200.146.253:443</li> <li>• DL (Delhi): 34.131.116.135:443</li> <li>• CH (Switzerland): 34.65.213.226:443</li> <li>• PL (Poland): 34.118.62.80:443</li> <li>• TW (Taiwan): 34.80.34.30:443</li> <li>• QT (Qatar): 34.18.34.73:443</li> <li>• FA (France): 34.163.57.57:443</li> <li>• IL (Israel): 34.165.43.106:443</li> <li>• SA (Saudi Arabia): 34.166.54.6:443</li> <li>• ID (Indonesia): 34.101.214.157:443</li> <li>• ES (Spain): 34.175.18.78:443</li> <li>• IT (Italy): 34.154.154.5:443</li> <li>• KR (South Korea): 34.22.66.91:443</li> <li>• ZA (South Africa): 34.35.56.170:443</li> <li>• BR (Brazil): 34.151.236.197:443</li> </ul>	cortex-xdr
<p><a href="panw-xdr-installers-prod-us.storage.googleapis.com">panw-xdr-installers-prod-us.storage.googleapis.com</a></p> <p>Used to download installers for upgrade actions from the server.</p> <p>This storage bucket is used for all regions.</p>	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	cortex-xdr
<p><a href="panw-xdr-payloads-prod-us.storage.googleapis.com">panw-xdr-payloads-prod-us.storage.googleapis.com</a></p> <p>Used to download the executable for the live terminal for XDR agents earlier than version 7.1.0.</p> <p>This storage bucket is used for all regions.</p>	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	cortex-xdr
<p><a href="global-content-profiles-policy.storage.googleapis.com">global-content-profiles-policy.storage.googleapis.com</a></p> <p>Used to download content updates.</p>	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	cortex-xdr



FQDN	IP Addresses And Port	App-ID Coverage
<b>panw-xdr-evr-prod- &lt;region&gt;.storage.googleapis.com</b>  Used to download extended verdict request results in scanning.	<ul style="list-style-type: none"> <li>IP ranges in GCP</li> <li>Port: 443</li> </ul>	<b>cortex-xdr</b>
<b>https://&lt;region&gt;-docker.pkg.dev</b>  Used to download the Kubernetes image from the registry for Kubernetes agents installation.	<ul style="list-style-type: none"> <li>IP ranges in GCP</li> <li>Port: 443</li> </ul>	
<b>dc-&lt;tenant-name&gt;.traps.paloaltonetworks.com</b>  Used for EDR data upload.	IP address by region: <ul style="list-style-type: none"> <li>US (United States): 34.98.77.231:443</li> <li>EU (Europe): 34.102.140.103:443</li> <li>CA (Canada): 34.96.120.25:443</li> <li>UK (United Kingdom): 35.244.133.254:443</li> <li>JP (Japan): 34.95.66.187:443</li> <li>SG (Singapore): 34.120.142.18:443</li> <li>AU (Australia): 34.102.237.151:443</li> <li>DE (Germany): 34.107.161.143:443</li> <li>IN (India): 34.120.213.187:443</li> <li>DL (Delhi): 136.110.132.208:443</li> <li>CH (Switzerland): 34.149.180.250:443</li> <li>PL (Poland): 35.190.13.237:443</li> <li>TW (Taiwan): 34.149.248.76:443</li> <li>QT (Qatar): 34.107.129.254:443</li> <li>FA (France): 34.36.155.211:443</li> <li>IL (Israel): 34.128.157.130:443</li> <li>SA (Saudi Arabia): 34.107.213.85:443</li> <li>ID (Indonesia): 34.128.156.84:443</li> <li>ES (Spain): 34.120.102.147:443</li> <li>IT (Italy): 34.8.234.58:443</li> <li>KR (South Korea): 34.54.155.245:443</li> <li>ZA (South Africa): 35.190.79.68:443</li> <li>BR (Brazil): 136.110.146.246:443</li> </ul>	<b>traps-management-service</b>



FQDN	IP Addresses And Port	App-ID Coverage
<p><code>ch-&lt;tenant-name&gt;.traps.paloaltonetworks.com</code></p> <p>Used for all other requests between the agent and its tenant server, including heartbeat, uploads, action results, and scan reports.</p>	<p>IP address by region:</p> <ul style="list-style-type: none"> <li>• US (United States): 34.98.77.231:443</li> <li>• EU (Europe): 34.102.140.103:443</li> <li>• CA (Canada): 34.96.120.25:443</li> <li>• UK (United Kingdom): 35.244.133.254:443</li> <li>• JP (Japan): 34.95.66.187:443</li> <li>• SG (Singapore): 34.120.142.18:443</li> <li>• AU (Australia): 34.102.237.151:443</li> <li>• DE (Germany): 34.107.161.143:443</li> <li>• IN (India): 34.120.213.188:443</li> <li>• DL (Delhi): 136.110.132.208:443</li> <li>• CH (Switzerland): 34.149.180.250:443</li> <li>• PL (Poland): 35.190.13.237:443</li> <li>• TW (Taiwan): 34.149.248.76:443</li> <li>• QT (Qatar): 34.107.129.254:443</li> <li>• FA (France): 34.36.155.211:443</li> <li>• IL (Israel): 34.128.157.130:443</li> <li>• SA (Saudi Arabia): 34.107.213.85:443</li> <li>• ID (Indonesia): 34.128.156.84:443</li> <li>• ES (Spain): 34.120.102.147:443</li> <li>• IT (Italy): 34.8.234.58:443</li> <li>• KR (South Korea): 34.54.155.245:443</li> <li>• ZA (South Africa): 35.190.79.68:443</li> <li>• BR (Brazil): 136.110.146.246:443</li> </ul>	<code>traps-management-service</code>



FQDN	IP Addresses And Port	App-ID Coverage
<pre>api-&lt;tenant-name&gt;.xdr. &lt;region&gt;.paloaltonetworks.com</pre> <p>Used for API requests and responses and to connect to an engine.</p>	<p>IP address by region:</p> <ul style="list-style-type: none"> <li>• US (United States): 35.222.81.194:443</li> <li>• EU (Europe): 34.90.67.58:443</li> <li>• CA (Canada): 35.203.82.121:443</li> <li>• UK (United Kingdom): 34.89.56.78:443</li> <li>• JP (Japan): 34.84.125.129:443</li> <li>• SG (Singapore): 34.87.83.144:443</li> <li>• AU (Australia): 35.189.18.208:443</li> <li>• DE (Germany): 34.107.57.23:443</li> <li>• IN (India): 35.200.158.164:443</li> <li>• DL (Delhi): 34.131.165.103:443</li> <li>• CH (Switzerland): 34.65.248.119:443</li> <li>• PL (Poland): 34.116.216.55:443</li> <li>• TW (Taiwan): 35.234.8.249:443</li> <li>• QT (Qatar): 34.18.46.240:443</li> <li>• FA (France): 34.155.222.152:443</li> <li>• IL (Israel): 34.165.156.139:443</li> <li>• SA (Saudi Arabia): 34.166.58.79:443</li> <li>• ID (Indonesia): 34.128.115.238:443</li> <li>• ES (Spain): 34.175.30.176:443</li> <li>• IT (Italy): 34.154.195.120:443</li> <li>• KR (South Korea): 34.64.54.175:443</li> <li>• ZA (South Africa): 34.35.64.191:443</li> <li>• BR (Brazil): 34.39.136.78:443</li> </ul>	â€



FQDN	IP Addresses And Port	App-ID Coverage
<p><code>cc-&lt;tenant-name&gt;.traps.paloaltonetworks.com</code></p> <p>Used for get-verdict requests.</p>	<p>IP address by region:</p> <ul style="list-style-type: none"> <li>• US (United States): 35.224.140.142:443</li> <li>• EU (Europe): 34.90.71.103:443</li> <li>• CA (Canada): 35.203.35.23:443</li> <li>• UK (United Kingdom): 34.89.42.214:443</li> <li>• JP (Japan): 34.84.225.105:443</li> <li>• SG (Singapore): 35.247.161.94:443</li> <li>• AU (Australia): 35.201.23.188:443</li> <li>• DE (Germany): 35.242.201.199:443</li> <li>• IN (India): 35.244.57.196:443</li> <li>• DL (Delhi): 34.131.47.126:443</li> <li>• CH (Switzerland): 34.65.137.215:443</li> <li>• PL (Poland): 34.116.213.71:443</li> <li>• TW (Taiwan): 35.229.186.216:443</li> <li>• QT (Qatar): 34.18.53.229:443</li> <li>• FA (France): 34.155.110.169:443</li> <li>• IL (Israel): 34.165.2.110:443</li> <li>• SA (Saudi Arabia): 34.166.53.160:443</li> <li>• ID (Indonesia): 34.101.155.198:443</li> <li>• ES (Spain): 34.175.205.166:443</li> <li>• IT (Italy): 34.154.230.76:443</li> <li>• KR (South Korea): 34.64.228.117:443</li> <li>• ZA (South Africa): 34.35.13.198:443</li> <li>• BR (Brazil): 34.39.195.104:443</li> </ul>	<code>traps-management-service</code>
<p><b>Broker VM Resources</b></p> <p>Required for deployments that use Broker VM features</p>		
<p>xdr-ova-installers-prod-us.storage.googleapis.com</p> <p>Used to download Broker VM images from the server.</p> <p>This storage bucket is used for all regions.</p>	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	<code>cortex-xdr</code>



FQDN	IP Addresses And Port	App-ID Coverage
br-<tenant-name>.xdr.<region>.paloaltonetworks.com	<p>IP address by region:</p> <ul style="list-style-type: none"> <li>• US (United States): 104.155.131.72:443</li> <li>• EU (Europe): 34.91.128.226:443</li> <li>• CA (Canada): 34.95.8.232:443</li> <li>• UK (United Kingdom): 35.197.219.110:443</li> <li>• JP (Japan): 34.85.74.43:443</li> <li>• SG (Singapore): 34.87.167.125:443</li> <li>• AU (Australia): 35.244.93.0:443</li> <li>• DE (Germany): 35.198.112.13:443</li> <li>• IN (India): 35.200.234.99:443</li> <li>• DL (Delhi): 34.131.131.141:443</li> <li>• CH (Switzerland): 34.65.51.103:443</li> <li>• PL (Poland): 34.116.176.97:443</li> <li>• TW (Taiwan): 34.80.230.166:443</li> <li>• QT (Qatar): 34.18.37.73:443</li> <li>• FA (France): 34.155.90.61:443</li> <li>• IL (Israel): 34.165.24.222:443</li> <li>• SA (Saudi Arabia): 34.166.55.153:443</li> <li>• ID (Indonesia): 34.101.101.170:443</li> <li>• ES (Spain): 34.175.182.55:443</li> <li>• IT (Italy): 34.154.168.139:443</li> <li>• KR (South Korea): 34.64.46.249:443</li> <li>• ZA (South Africa): 34.35.45.251:443</li> <li>• BR (Brazil): 35.198.38.182:443</li> </ul>	â€
distributions.traps.paloaltonetworks.com	<ul style="list-style-type: none"> <li>• IP address: 35.223.6.69</li> <li>• Port: 443</li> </ul>	traps-management-service
<ul style="list-style-type: none"> <li>• time.google.com</li> <li>• pool.ntp.org</li> </ul>	UDP port: 123	â€
App Login and Authentication		
identity.paloaltonetworks.com (SSO)	<ul style="list-style-type: none"> <li>• IP address: 34.120.119.85</li> <li>• Port: 443</li> </ul>	â€
login.paloaltonetworks.com (SSO)	<ul style="list-style-type: none"> <li>• IP address: 34.102.139.110</li> <li>• Port: 443</li> </ul>	â€



FQDN	IP Addresses And Port	App-ID Coverage
In-App Help Center and Notifications		
data.pendo.io	Port: 443	â€
pendo-static-5664029141630976.storage.googleapis.com	Port: 443	â€
Email Notifications		
â€	IP address for all regions: 159.183.150.248	â€
Ingress		
These IPs are used for communication between Cortex Cloud and your resources. Use them when sending data out from your tenant.		



FQDN	IP Addresses And Port	App-ID Coverage
	<ul style="list-style-type: none"> <li>• US (United States) <ul style="list-style-type: none"> <li>◦ 34.132.108.184</li> <li>◦ 34.69.63.16</li> </ul> </li> <li>• EU (Europe) <ul style="list-style-type: none"> <li>◦ 34.147.107.51</li> <li>◦ 34.91.26.125</li> </ul> </li> <li>• CA (Canada) <ul style="list-style-type: none"> <li>◦ 35.203.108.13</li> <li>◦ 35.203.101.162</li> </ul> </li> <li>• UK (United Kingdom) <ul style="list-style-type: none"> <li>◦ 35.242.180.163</li> <li>◦ 34.105.173.229</li> </ul> </li> <li>• JP (Japan) <ul style="list-style-type: none"> <li>◦ 35.200.3.131</li> <li>◦ 34.146.181.233</li> </ul> </li> <li>• SG (Singapore) <ul style="list-style-type: none"> <li>◦ 35.240.243.57</li> <li>◦ 34.126.183.208</li> </ul> </li> <li>• AU (Australia) <ul style="list-style-type: none"> <li>◦ 34.151.83.236</li> <li>◦ 34.116.67.90</li> </ul> </li> <li>• DE (Germany) <ul style="list-style-type: none"> <li>◦ 35.234.118.195</li> <li>◦ 34.89.183.45</li> </ul> </li> <li>• IN (India) <ul style="list-style-type: none"> <li>◦ 35.200.175.78</li> <li>◦ 34.93.9.198</li> </ul> </li> <li>• CH (Switzerland) <ul style="list-style-type: none"> <li>◦ 34.65.108.153</li> <li>◦ 34.65.155.169</li> </ul> </li> <li>• PL (Poland) <ul style="list-style-type: none"> <li>◦ 34.118.48.171</li> <li>◦ 34.116.202.235</li> </ul> </li> <li>• TW (Taiwan) <ul style="list-style-type: none"> <li>◦ 34.80.133.68</li> <li>◦ 35.234.18.10</li> </ul> </li> <li>• QT (Qatar) <ul style="list-style-type: none"> <li>◦ 34.18.34.118</li> <li>◦ 34.18.39.155</li> </ul> </li> </ul>	cortex-xdr



FQDN	IP Addresses And Port	App-ID Coverage
	<ul style="list-style-type: none"> <li>• FA (France) <ul style="list-style-type: none"> <li>◦ 34.155.5.117</li> <li>◦ 34.155.41.247</li> </ul> </li> <li>• IL (Israel) <ul style="list-style-type: none"> <li>◦ 34.165.33.165</li> <li>◦ 34.165.27.131</li> </ul> </li> <li>• SA (Saudi Arabia) <ul style="list-style-type: none"> <li>◦ 34.166.61.81</li> <li>◦ 34.166.58.213</li> </ul> </li> <li>• ID (Indonesia) <ul style="list-style-type: none"> <li>◦ 34.128.126.138</li> <li>◦ 34.128.82.158</li> </ul> </li> <li>• ES (Spain) <ul style="list-style-type: none"> <li>◦ 34.175.46.46</li> <li>◦ 34.175.80.182</li> </ul> </li> <li>• IT (Italy) <ul style="list-style-type: none"> <li>◦ 34.154.23.156</li> <li>◦ 34.154.186.12</li> </ul> </li> <li>• KR (South Korea) <ul style="list-style-type: none"> <li>◦ 34.64.93.168</li> <li>◦ 34.64.237.45</li> </ul> </li> <li>• ZA (South Africa): <ul style="list-style-type: none"> <li>◦ 34.35.42.196</li> <li>◦ 34.35.79.219</li> </ul> </li> </ul>	
Outbound IPs for engines		



FQDN	IP Addresses And Port	App-ID Coverage
	IP addresses by region	â€



FQDN	IP Addresses And Port	App-ID Coverage
	<ul style="list-style-type: none"> <li>• US (United States) <ul style="list-style-type: none"> <li>◦ 35.225.156.101</li> <li>◦ 34.69.88.119</li> </ul> </li> <li>• EU (Europe) <ul style="list-style-type: none"> <li>◦ 34.147.67.188</li> <li>◦ 34.90.16.31</li> </ul> </li> <li>• CA (Canada) <ul style="list-style-type: none"> <li>◦ 35.203.57.162</li> <li>◦ 35.203.90.79</li> </ul> </li> <li>• UK (United Kingdom) <ul style="list-style-type: none"> <li>◦ 34.142.3.42</li> <li>◦ 34.142.44.136</li> </ul> </li> <li>• JP (Japan) <ul style="list-style-type: none"> <li>◦ 34.146.60.215</li> <li>◦ 34.84.93.160</li> </ul> </li> <li>• SG (Singapore) <ul style="list-style-type: none"> <li>◦ 35.240.144.192</li> <li>◦ 35.240.255.15</li> </ul> </li> <li>• AU (Australia) <ul style="list-style-type: none"> <li>◦ 35.244.73.76</li> <li>◦ 35.201.22.63</li> </ul> </li> <li>• DE (Germany) <ul style="list-style-type: none"> <li>◦ 34.107.83.197</li> <li>◦ 34.159.53.97</li> </ul> </li> <li>• IN (India) <ul style="list-style-type: none"> <li>◦ 35.244.5.205</li> <li>◦ 34.93.118.113</li> </ul> </li> <li>• DL (Delhi) <ul style="list-style-type: none"> <li>◦ 34.131.207.151</li> <li>◦ 34.126.212.40</li> </ul> </li> <li>• CH (Switzerland) <ul style="list-style-type: none"> <li>◦ 34.65.222.25</li> <li>◦ 34.65.233.60</li> </ul> </li> <li>• PL (Poland) <ul style="list-style-type: none"> <li>◦ 34.118.92.214</li> <li>◦ 34.116.223.119</li> </ul> </li> <li>• TW (Taiwan) <ul style="list-style-type: none"> <li>◦ 104.199.223.229</li> <li>◦ 34.81.38.132</li> </ul> </li> </ul>	



FQDN	IP Addresses And Port	App-ID Coverage
	<ul style="list-style-type: none"> <li>• QT (Qatar) <ul style="list-style-type: none"> <li>◦ 34.18.39.0</li> <li>◦ 34.18.32.96</li> </ul> </li> <li>• FA (France) <ul style="list-style-type: none"> <li>◦ 34.155.197.131</li> <li>◦ 34.155.5.100</li> </ul> </li> <li>• IL (Israel) <ul style="list-style-type: none"> <li>◦ 34.165.46.47</li> <li>◦ 34.165.17.246</li> </ul> </li> <li>• SA (Saudi Arabia) <ul style="list-style-type: none"> <li>◦ 34.166.58.243</li> <li>◦ 34.166.54.238</li> </ul> </li> <li>• ID (Indonesia) <ul style="list-style-type: none"> <li>◦ 34.101.125.66</li> <li>◦ 34.101.218.184</li> </ul> </li> <li>• ES (Spain) <ul style="list-style-type: none"> <li>◦ 34.175.255.99</li> <li>◦ 34.175.230.35</li> </ul> </li> <li>• IT (Italy) <ul style="list-style-type: none"> <li>◦ 34.154.173.134</li> <li>◦ 34.154.229.60</li> </ul> </li> <li>• KR (South Korea) <ul style="list-style-type: none"> <li>◦ 34.64.189.205</li> <li>◦ 34.64.45.118</li> </ul> </li> <li>• ZA (South Africa) <ul style="list-style-type: none"> <li>◦ 34.35.70.193</li> <li>◦ 34.35.80.189</li> </ul> </li> <li>• BR (Brazil) <ul style="list-style-type: none"> <li>◦ 35.199.96.109</li> <li>◦ 34.39.161.254</li> </ul> </li> </ul>	
Collect third-party data from your SaaS and Cloud resources		



FQDN	IP Addresses And Port	App-ID Coverage
â€	IP address by region.	cortex-xdr



FQDN	IP Addresses And Port	App-ID Coverage
	<ul style="list-style-type: none"> <li>• US (United States) <ul style="list-style-type: none"> <li>◦ 34.66.69.154</li> <li>◦ 35.202.21.123</li> </ul> </li> <li>• AU (Australia) <ul style="list-style-type: none"> <li>◦ 35.197.181.108</li> <li>◦ 35.197.175.44</li> </ul> </li> <li>• CA (Canada) <ul style="list-style-type: none"> <li>◦ 34.95.33.72</li> <li>◦ 34.95.62.136</li> </ul> </li> <li>• SG (Singapore) <ul style="list-style-type: none"> <li>◦ 35.247.148.38</li> <li>◦ 35.247.173.40</li> </ul> </li> <li>• JP (Japan) <ul style="list-style-type: none"> <li>◦ 34.85.68.167</li> <li>◦ 34.84.99.239</li> </ul> </li> <li>• IN (India) <ul style="list-style-type: none"> <li>◦ 34.93.3.196</li> <li>◦ 34.93.175.218</li> </ul> </li> <li>• DL (Delhi) <ul style="list-style-type: none"> <li>◦ 34.131.111.87</li> <li>◦ 34.131.101.138</li> </ul> </li> <li>• DE (Germany) <ul style="list-style-type: none"> <li>◦ 34.89.197.46</li> <li>◦ 34.107.3.224</li> </ul> </li> <li>• UK (United Kingdom) <ul style="list-style-type: none"> <li>◦ 34.105.227.146</li> <li>◦ 34.105.137.22</li> </ul> </li> <li>• EU (Europe) <ul style="list-style-type: none"> <li>◦ 34.90.70.107</li> <li>◦ 35.204.129.196</li> </ul> </li> <li>• CH (Switzerland) <ul style="list-style-type: none"> <li>◦ 34.65.225.124</li> <li>◦ 34.65.89.6</li> </ul> </li> <li>• PL (Poland) <ul style="list-style-type: none"> <li>◦ 34.118.71.237</li> <li>◦ 34.118.124.130</li> </ul> </li> <li>• TW (Taiwan) <ul style="list-style-type: none"> <li>◦ 35.201.142.86</li> <li>◦ 35.189.176.163</li> </ul> </li> </ul>	



FQDN	IP Addresses And Port	App-ID Coverage
	<ul style="list-style-type: none"> <li>• QT (Qatar) <ul style="list-style-type: none"> <li>◦ 34.18.44.71</li> <li>◦ 34.18.30.132</li> </ul> </li> <li>• FA (France) <ul style="list-style-type: none"> <li>◦ 34.163.125.167</li> <li>◦ 34.163.155.105</li> </ul> </li> <li>• IL (Israel) <ul style="list-style-type: none"> <li>◦ 34.165.131.171</li> <li>◦ 34.165.120.206</li> </ul> </li> <li>• SA (Saudi Arabia) <ul style="list-style-type: none"> <li>◦ 34.166.59.20</li> <li>◦ 34.166.53.242</li> </ul> </li> <li>• ID (Indonesia) <ul style="list-style-type: none"> <li>◦ 34.101.158.32</li> <li>◦ 34.101.79.159</li> </ul> </li> <li>• ES (Spain) <ul style="list-style-type: none"> <li>◦ 34.175.27.251</li> <li>◦ 34.175.198.50</li> </ul> </li> <li>• IT (Italy) <ul style="list-style-type: none"> <li>◦ 34.154.208.247</li> <li>◦ 34.154.243.11</li> </ul> </li> <li>• KR (South Korea) <ul style="list-style-type: none"> <li>◦ 34.64.107.163</li> <li>◦ 34.64.84.25</li> </ul> </li> <li>• ZA (South Africa): <ul style="list-style-type: none"> <li>◦ 34.35.69.156</li> <li>◦ 34.35.60.86</li> </ul> </li> <li>• BR (Brazil) <ul style="list-style-type: none"> <li>◦ 34.39.177.125</li> <li>◦ 34.39.140.36</li> </ul> </li> </ul>	
Log Forwarding to a Syslog Receiver		
See Integrate a syslog receiver.		

FedRAMP and US Federal Government required resources

The following table lists the required resources for the federal government of the United States, including FQDNs, IP addresses, ports, and App-ID coverage for your deployment:



FQDN	IP Addresses And Port	App-ID Coverage
Egress		
	FedRAMP Moderate <ul style="list-style-type: none"> <li>• 34.122.220.113:443</li> <li>• 35.223.83.172:443</li> </ul> FedRAMP High <ul style="list-style-type: none"> <li>• 34.136.155.252:443</li> <li>• 34.133.46.50:443</li> </ul>	
Outbound IPs for Engines		
	FedRAMP Moderate <ul style="list-style-type: none"> <li>• 34.123.127.174:443</li> <li>• 34.71.135.18:443</li> </ul> FedRAMP High <ul style="list-style-type: none"> <li>• 34.123.153.175:443</li> <li>• 35.223.253.2:443</li> </ul>	
<b>distributions-prod-fed.traps.paloaltonetworks.com</b>  Used for the first request in registration flow where the agent passes the distribution ID and obtains the ch- <tenant-name>.traps.paloaltonetworks.com of its tenant	<ul style="list-style-type: none"> <li>• IP address: 104.198.132.24</li> <li>• Port: 443</li> </ul>	<b>traps-management-service</b>
<b>wss://lrc-fed.paloaltonetworks.com</b>  Used in live terminal flow.	<ul style="list-style-type: none"> <li>• IP address: 35.188.188.91</li> <li>• Port: 443</li> </ul>	<b>cortex-xdr</b>
<b>panw-xdr-installers-prod-fr.storage.googleapis.com</b>  Used to download installers for upgrade actions from the server.	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	<b>cortex-xdr</b>
<b>panw-xdr-payloads-prod-fr.storage.googleapis.com</b>  Used to download the executable for the live terminal for Cortex XDR agents earlier than version 7.1.0.	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	<b>cortex-xdr</b>
<b>global-content-profiles-policy-prod-fr.storage.googleapis.com</b>  Used to download content updates.	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	<b>cortex-xdr</b>



FQDN	IP Addresses And Port	App-ID Coverage
panw-xdr-evr-prod-fr.storage.googleapis.com  Used to download extended verdict request results in scanning.	<ul style="list-style-type: none"> <li>• IP ranges in GCP</li> <li>• Port: 443</li> </ul>	cortex-xdr
app-proxy.federal.paloaltonetworks.com	<ul style="list-style-type: none"> <li>• IP address: 35.186.217.42</li> <li>• Port: 443</li> </ul>	â€
dc-<tenant-name>.traps.paloaltonetworks.com  Used for EDR data upload.	<ul style="list-style-type: none"> <li>• IP address: 130.211.195.231</li> <li>• Port: 443</li> </ul>	traps-management-service
ch-<tenant-name>.traps.paloaltonetworks.com  Used for all other requests between the agent and its tenant server including heartbeat, uploads, action results, and scan reports.	<ul style="list-style-type: none"> <li>• IP address: 130.211.195.231</li> <li>• Port: 443</li> </ul>	traps-management-service
api-<tenant-name>.xdr.federal.paloaltonetworks.com  Used for API requests and responses.	<ul style="list-style-type: none"> <li>• IP address: 130.211.195.231</li> <li>• Port: 443</li> </ul>	â€
cc-<tenant-name>.traps.paloaltonetworks.com  Used for get-verdict requests.	<ul style="list-style-type: none"> <li>• IP address: 35.222.50.74</li> <li>• Port: 443</li> </ul>	traps-management-service
<b>Broker VM resources</b>		
Required for deployments that use Broker VM features		
br-<tenant-name>.xdr.federal.paloaltonetworks.com:443	<ul style="list-style-type: none"> <li>• IP address: 34.71.185.11</li> <li>• Port: 443</li> </ul>	â€
	<ul style="list-style-type: none"> <li>• Port: 443</li> </ul>	â€
distributions-prod-fed.traps.paloaltonetworks.com	<ul style="list-style-type: none"> <li>• IP address: 104.198.132.24</li> <li>• Port: 443</li> </ul>	traps-management-service
	UDP port: 123	â€
<b>App login and authentication</b>		
identity.paloaltonetworks.com  (SSO)	<ul style="list-style-type: none"> <li>• IP address: 34.107.215.35</li> <li>• Port: 443</li> </ul>	â€



FQDN	IP Addresses And Port	App-ID Coverage
login.paloaltonetworks.com (SSO)	<ul style="list-style-type: none"> <li>IP address: 34.107.190.184</li> <li>Port: 443</li> </ul>	â€
Collect third-party data from your SaaS and Cloud resources		
â€	IP addresses <ul style="list-style-type: none"> <li>34.68.217.16</li> <li>34.69.175.202</li> </ul>	cortex-xdr
Log Forwarding to a Syslog Receiver		
See <a href="#">Integrate a syslog receiver</a> .		

## 2.2.2 | Upgrade from Prisma Cloud to Cortex Cloud

### 2.2.2.1 | About the Upgrade Helper

If you are a Prisma Cloud customer, you can use the Upgrade Helper to copy data from your Prisma Cloud tenant to your new Cortex Cloud tenant. If you have not received your entitlement details to activate your Cortex Cloud tenant, contact your account team to learn more about tenant activation and the upgrade process.

**NOTE:**

Your Prisma Cloud tenant remains available and fully operational during the agreed upgrade period.

The Upgrade Helper provides a gradual and flexible upgrade experience, while Prisma Cloud and Cortex Cloud run in parallel during the transition period. It enables you to copy configurations from your Prisma Cloud tenant into your Cortex Cloud tenant at your own pace.

- Administrators can use the Upgrade Helper at any stage of the upgrade process, as many times as needed. If you copied a record previously, it gets updated and overwritten with the latest details from Prisma Cloud during each run.

For example, when you copy custom permission groups the second time, all custom roles that you previously created in the Cortex Cloud tenant are overwritten with the latest configurations.

- Choose exactly what to copy and what to skip. This allows you to choose a clean start or do a selective migration of content.
- The Upgrade Helper does not modify any existing content in your Prisma Cloud tenant.

The following table lists the types of content that are copied from your Prisma Cloud tenant to your Cortex Cloud tenant during the upgrade process:

Upgrade Helper Section	Content Item Name In Prisma Cloud	Content Item Name In Cortex Cloud
Global Configurations	Permission Groups and Roles	Roles and User Groups
CSPM Configurations	Policies	Rules
	Custom Alert Rules	Custom Policies
	Notifications	Automation Rules
	Custom Compliance Standards	Custom Compliance Standards



<b>Upgrade Helper Section</b>	<b>Content Item Name In Prisma Cloud</b>	<b>Content Item Name In Cortex Cloud</b>
CWP Configurations	Rules and Their Collections	Policies and Their Asset Groups
Application Security Configurations	Policy Labels	Application Security Rule Labels
	Custom Policies	Application Security Custom Rules
	Enforcement Rules	Application Security Policies
	Non-default Scanned Branches	Non-default Scanned Branches
	Git History & Validate Secrets	Git History & Validate Secrets
	Developer Suppressions	Application Security Policies
	AppDNA Discovery Criteria	Application Criteria

#### 2.2.2.2 | Link Cortex Cloud to Prisma Cloud

To link your Cortex Cloud tenant to a Prisma Cloud tenant, first obtain the Access Key from Prisma Cloud, and then paste it in the Link Tenant section of the Upgrade Helper to establish the link.

Obtain the Prisma Cloud tenant access key

1. Log in to your Prisma Cloud tenant as an administrator.
2. Go to Settings → Enterprise Settings .
3. Click Generate Token in the Cortex Cloud Tenant Linking section.
4. Copy the Access Key.

Link from Cortex Cloud

1. Log in to Cortex Cloud as an administrator.
2. Navigate to Settings → Configurations → Upgrade Helper.
3. Click Create Link in the Link Tenant section.
4. Enter the Prisma Cloud Access Key.
5. Review the details of the Prisma Cloud tenant, such as Tenant Name, Tenant ID, and Region.
6. Click Connect.

#### 2.2.2.3 | Copy content

After you successfully link your Cortex Cloud tenant to your Prisma Cloud tenant, you can choose content items to copy. You can either copy all supported content (recommended) or select specific items to copy.



## Upgrade Helper

Select content items to copy from your Prisma Cloud to this tenant. You can repeat this action anytime during onboarding. This action will not delete or modify any content in your Prisma Cloud tenant.

The screenshot shows the 'Content Items' section of the Upgrade Helper. At the top, there's a 'Link Tenant' button with a help icon and a 'Create Link' button. Below that is a 'Content Items' section with a 'Select All (Recommended)' button. The items are categorized under 'GLOBAL CONFIGURATIONS', 'CSPM CONFIGURATIONS', and 'CWP CONFIGURATIONS'. Under 'GLOBAL CONFIGURATIONS', there's one item: 'Roles and User Groups' (Prisma Cloud: Permission Groups and Roles), which is marked as 'Not copied yet'. Under 'CSPM CONFIGURATIONS', there are four items: 'Rules' (Prisma Cloud: Policies), 'Custom Policies' (Prisma Cloud: Custom Alert Rules), 'Automation Rules' (Prisma Cloud: Notifications), and 'Custom Compliance Standards' (Prisma Cloud: Custom Compliance Standards), all marked as 'Not copied yet'. Under 'CWP CONFIGURATIONS', there's one item: 'Policies and Their Asset Groups' (Prisma Cloud: Rules and Their Collections), which is also marked as 'Not copied yet'. At the bottom left, there's a 'Copy Selected' button.

### How to copy selected content

1. In your Cortex tenant, navigate to Settings → Configurations → Upgrade Helper.
2. Select the checkbox next to the item you want to copy and click Copy Selected.
3. Review the message and if you are ready to proceed, click Proceed with Copy.

The Copy content started successfully message is displayed.

Upon successful completion, a message shows the number of items that were copied from the Prisma Cloud tenant.

4. Click View Log to view the error messages (info and warning). The log shows records that were not copied. You can also export the log.

#### 2.2.2.3.1 | Copy Global configurations

##### Roles and user groups

When you copy Roles and User Groups in the Upgrade Helper, the Prisma Cloud Custom Permission Groups and Roles are copied to Cortex Cloud as corresponding roles and user groups.

##### Assign roles and user groups

Users created through the customer support portal are assigned to the relevant user groups. If your organization uses single sign-on (SSO) for authentication, user roles and groups won't be assigned based on Prisma Cloud mappings. In this case, you will need to handle role assignment by SAML group mapping. Learn more about authenticating users.

##### Verify copied roles and user groups

After you follow the steps listed in Copy configurations, navigate to Settings → Configurations → Access Management to view the copied items.

#### NOTE:

Keep the following caveats in mind:



- Scope-Based Access Control (SBAC) configurations, such as resources or account lists are not copied. You can manually assign scope-based access to the relevant users or groups.
  - When migrating permission groups and roles, the total count of items successfully copied may be lower than the initial number selected. This is expected behavior. The discrepancy in counts can occur for the following reasons:
    - Default Entities:** System-default items that are already mapped in the Cortex environment are automatically excluded from the operation, as migration is not required. The initial total count shown for processing will reflect this exclusion.
    - Validation Failures:** Entities that fail validation checks, such as those with duplicate names, will be skipped and not copied.
    - Empty Mappings:** Items that result in an empty configuration after the permission mapping process (e.g., a group that contains no valid permissions in the target system) will be skipped, as no corresponding entity can be created.
- Reference the migration logs for specific details on any skipped entities.

#### 2.2.2.3.2 | Copy CSPM configurations

##### Rules

When you copy Rules in the Upgrade Helper, the following actions occur:

- Prisma Cloud Custom Policies (Config, Attack Path, and Data) are copied as Detection Rules in Cortex Cloud.
- The enabled/disabled state of the default policies is also applied to the corresponding Detection Rules in Cortex Cloud.

##### Verify copied rules

After you follow the steps listed in Copy configurations, navigate to Posture Management → Rules & Policies → Rules → Cloud Security to view the list of rules that were copied.

##### Custom policies

When you copy Custom Policies in the Upgrade Helper, the Prisma Cloud Custom Alert Rules are copied as Policies in Cortex Cloud.

##### Verify copied policies

After you follow the steps listed in Copy configurations, navigate to Posture Management → Rules & Policies → Policies → Cloud Security to view the list of policies that were copied.

When verifying the list of policies, note the following details:

- The policy name will have a prisma\_cloud\_copy suffix.
- To verify that the prisma\_cloud\_alert\_rule label was added to your policies, click the three dots next to Create Policy and select Labels from under Add Columns.
- Click on a policy to view its details and review the issues that were generated.

Alert Rule Name In Prisma Cloud	Result After Copying To Cortex Cloud
Alert rule default config or attack	Policies are created
Alert rule custom config or attack path	
Alert rule with custom compliance standard filter	
Alert rule with Email and Slack notification setup	
Alert rule without Email notification setup	
Alert rule with CIEM policies	Policies are not created: <ul style="list-style-type: none"> <li>IAM policy</li> <li>Attack path with CIEM finding</li> </ul>



Alert Rule Name In Prisma Cloud	Result After Copying To Cortex Cloud
Alert rule with network or audit event policies	<p>Policies are not created:</p> <ul style="list-style-type: none"> <li>• Network</li> <li>• Audit event</li> <li>• Anomaly</li> </ul>

#### Automation rules

When you copy Automation Rules in the Upgrade Helper, the Prisma Cloud Notifications are copied as Automation Rules in Cortex Cloud.

You can copy Prisma Cloud notifications that were configured for:

- Alert rules with default Config or Attack Path policies
- Alert rules with Slack and Email notification setup

#### Verify copied notifications

After you follow the steps listed in Copy configurations, navigate to Investigation & Response â†“ Automation â†“ Automation Rules to view the list of notifications that were copied.

The notification type is Email and has a prisma\_cloud\_copy suffix. You can view the corresponding Policy ID and the email recipient.

Alert Rule In Prisma Cloud	Notification Channels Configured For Alert Rule In Prisma Cloud	Result After Copying To Cortex Cloud
Alert rule with default Config or Attack Path policies	Email	Automation rule is created with Email
Alert rule with Slack and Email	Slack and Email	
Alert rule with no Email	Slack	Automation rule is not created
Alert rule with custom Config or Attack Path policies	Not applicable	

#### Custom compliance standards

When you copy Custom Compliance Standards in the Upgrade Helper, the Prisma Cloud Custom Compliance Standards are copied to Cortex Cloud.

#### Verify copied compliance standards

After you follow the steps listed in Copy configurations, navigate to Posture Management â†“ Compliance â†“ Standards to view the list of custom compliance standards that were copied.

#### 2.2.2.3.1 | Copy CWP configurations

##### Policies and their asset groups

When you copy Policies and Their Asset Groups in the Upgrade Helper, the Prisma Cloud Custom Rules and their Collections are copied as Policies and their Asset Groups in Cortex Cloud.

Prisma Cloud Runtime Rules for vulnerabilities and compliance are copied to equivalent Cortex Cloud Policies for vulnerabilities, malware, and misconfiguration.

Policy scope is handled as follows:



- Each Prisma Cloud rule has a scope of one or more Collections.
- The Cortex Cloud policies are scoped to Asset Groups with properties that match as closely as possible to the relevant Collections.

#### Verify copied rules

After you follow the steps listed in Copy configurations, navigate to Posture Management → Rules & Policies → Cloud Workload to view the list of rules that were copied.

#### 2.2.2.3.4 | Copy Cortex Cloud Application Security configurations

##### Scope

The following configurations can be automatically copied or converted from Prisma Cloud to Cortex Cloud.

##### Copy and apply out-of-the-box Prisma Cloud policy labels to Cortex Cloud Application Security rules

Automatically copy out-of-the-box Prisma Cloud policy labels and apply them to their corresponding Application Security rules in Cortex Cloud.

##### **IMPORTANT:**

If labels are imported into Cortex Cloud less than three hours after they were last added or modified in Prisma Cloud, they may not be included in the import.

##### IMPORTANT:

- **Scope of conversion:** Only default policy labels are converted. Labels for custom policies will be converted as part of the custom policies import process
- **Naming convention:** Labels will be renamed and be added with a `-{prisma_id}_copy` suffix to ensure there is no duplication, particularly in multi-tenant environments
- **Conversion behavior:**
  - Only labels that contain the `-{prisma_id}_copy` suffix will be copied
  - If a label was manually changed after the initial conversion, a subsequent conversion will not override it

##### Import Prisma Cloud custom policies as custom Cortex Cloud Application Security rules

- **Policy creation:** Custom Prisma Cloud policies will be created as new custom Cortex Cloud Application Security rules on Cortex Cloud
- **Naming convention:** Imported policies will be renamed with the suffix `-{prisma_id}_copy`. This ensures no duplication in multi-tenant environments
- **Scope of conversion:** `Build` and `Build & Run` policy types are supported. If the policy type is `Build & Run`, only the `Build` rules component are converted
- **Excluded data:** Compliance data is not copied
- **Info severity level conversion:** Policies with an `Info` severity will be converted to `Low` severity
- **Conversion behavior:** Re-running the import process will override the newly created rules

##### Convert Prisma Cloud Enforcement rules to Cortex Cloud Application Security policies

Prisma Cloud Enforcement rules will be copied and converted into Cortex Cloud Application Security policies. The following outlines the key changes and behaviors of this conversion.

##### Scope

- **Rule merging:** Enforcement rules that share similar logic and conditions will be combined into a single Cortex Cloud Application Security policy
- **Exception rules:** Only default Enforcement rules will be converted. Any custom exception rules will not be carried over and will need to be reconfigured
- **Severity conversion:** Rules with an `Info` severity will be converted to `Low`

##### Behavior

- **Conversion behavior:** Re-running the conversion process will override the newly created policies
- **Multi-tenant use case:** Since a tenant can only have one set of Enforcement rules, running the process from another tenant will override the policies of the previous tenant

##### Copy confirmation

When Cortex Cloud Application Security policies are selected without labels, you will be prompted to confirm your choice with the following options:



- It is recommended to copy labels together with Enforcement rules. In order to automatically convert enforcement labels you must have also selected the default rule labels option. If you did not, the Enforcement rules will be migrated without the label, and you will need to reconfigure the label if required
- Option 1: Proceed with Copy.
- Option 2: Go Back to Selection (to select Labels).

#### Convert Prisma Cloud developer suppressions as Cortex Cloud Application Security policies

When importing developer suppression settings from Prisma Cloud to Cortex Cloud, they are copied and adapted into the corresponding policy configuration, updating or modifying the policy's existing developer suppression settings as needed.

- **Global vs. per-policy configuration:** While this was a global setting in Prisma Cloud, on Cortex Cloud developer suppressions are configured per policy
- **Scope:** This setting only applies to custom policies created prior to the conversion. Any custom policy created after the conversion process will need to be configured manually
- **Conversion behavior:** Executing the process again will override the policies' developer suppressions settings
- **Multi-tenant use case:** Running the process from another tenant will override the previous tenants' settings

#### Copy Git History & Validate Secrets settings

Copy Prisma Cloud advanced secrets settings for Git History and Secrets Validation to Cortex Cloud.

- **Global vs. per-repository configuration:** While these were global settings in Prisma Cloud, on Cortex Cloud they are configured per repository
- **Scope:** These settings only apply to repositories that were onboarded prior to the migration. Any repositories onboarded after the migration will need to have these settings configured manually
- **Conversion behavior:** Executing the conversion process again will override the settings on all repositories
- **Multi-tenant use case:** Running this process from another tenant will override the previous tenants' settings

#### Copy non-default scanned branches

Copy your non-default Prisma Cloud scanned branches through the Scanned Branches setting.

- **Scope:** Prisma Cloud non-default scanned branches will be copied as scanned branches to the Cortex Cloud Set Scanned Branches configuration settings. Repositories must be onboarded prior to initiating the conversion. Any repositories onboarded after the migration will only be scanned on their default branch
- **Scan behavior:** If selected, the relevant repositories will be scanned only on these imported non-default branches. On Cortex Cloud you have the flexibility to scan up to ten different branches. This can be manually configured after the conversion is complete
- **Conversion behavior:** Executing the conversion again will override the settings on all repositories

#### Convert AppDNA Discovery Criteria to Cortex Cloud Application Criteria

Convert your Prisma Cloud Application Discovery criteria into Cortex Cloud Application Criteria.

Cortex Cloud Application Criteria correlates assets across both code and cloud environments. It uses code-to-cloud graph technology to automate application discovery, as opposed to the Prisma Cloud AppDNA functionality, which was limited to cloud-only discovery.

- **Tag logic:** While Prisma Cloud supported matching all possible combinations of multiple tags, Cortex Cloud uses a strict AND logic. Only assets that match all selected tags will be grouped into an application
- **Excluded Criteria:** Any manual applications or discovery criteria that include specific repositories will not be migrated. These will need to be recreated manually in Cortex Cloud if needed
- **Conversion behavior:** Executing the conversion again will override the converted criteria settings

#### 2.2.2.4 | Migrate Cortex CLI

To migrate from Prisma Cloud to Cortex Cloud, transition your workflows from your commercial version of **Checkov CLI**, which is used for SCA, Secrets, and IaC scanning in local or build environments, and the **TwistCLI**, which is used for container image scanning, to the Cortex CLI. The Cortex CLI provides a single, consistent command-line interface for scanning across Cloud Workload Protection (CWP), API Security, and Cortex Cloud Application Security.

##### **PREREQUISITE:**

Before you begin, ensure you have the following:



- **Cortex Cloud API key:** An active API key for your Cortex Cloud tenant with associated CLI role permissions. Refer to Manage API keys for more information

- **Install the Cortex CLI.** You can find the installation instructions [here](#)

#### Authentication

The Cortex CLI offers a consistent authentication method across all its supported modules (CWP, Application Security, and API Security). You can authenticate using one of two methods: environment variables or command-line flags.

##### Authenticate via environment variables

Setting environment variables is the recommended method for authentication as it prevents your API credentials from being exposed in your command history and codebase:

1. Create an environment configuration file named `cortex.env`.
2. Save the `cortex.env` file in your working directory and add your credentials to the file as variables.

The Cortex CLI uses the following environment variables:

- `CORTEX_API_KEY_ID`: Your unique API key ID
- `CORTEX_API_KEY`: Your API key
- `CORTEX_API_URL`: Your tenant URL (for example `https://api-tenantname.paloaltonetworks.com/`)

##### Authenticate via command-line flags

You can also authenticate by providing your API credentials and base URL directly in the command.

```
cortexcli code scan --api-base-url <CORTEX_API_BASE_URL> --api-key-id <YOUR_API_KEY_ID> --api-key <YOUR_API_KEY> --directory ./my-app
```

Replace these placeholders:

- `--api-key-id`: Your unique API key ID
- `--api-key`: Your API key
- `--api-base-url`: Your API base URL

##### Key changes: commands and functionality

The main change is the command you use to initiate a scan. Instead of the `checkov` or `twistcli` commands, you now use the `cortexcli` command with its subcommands.

Prisma Cloud Command	Cortex CLI Command	Description
<code>checkov</code>	<code>cortexcli code scan</code>	The base command for all code scanning operations
<code>twistcli images scan</code>	<code>cortexcli image scan</code>	The base command for all container image scanning operations

##### Migrate Checkov to the Cortex CLI

Migrate your existing Checkov workflows using the following resources to map your essential commands and flags.

##### Flag references

- For Cortex CLI flags applicable to all supported Cortex Cloud modules, refer to the Cortex CLI common command line reference guide documentation
- For specific Cortex Cloud Application Security flags, refer to Cortex CLI Cortex Cloud Application Security command line reference
- For `checkov` flags, refer to the CLI Command Reference

##### Cortex Cloud Application Security-specific flags

Here are some common Application Security flags to get you started:



- **--directory**: Specifies the directory path to be scanned. This is a required argument for most Application Security scan commands
- **--repo-id**: Identifies the repository being scanned. This command links the scan results to the correct repository within Cortex Cloud
- **--branch**: Specifies the branch of the repository being scanned
- **-upload-mode**: Determines the method for uploading data, with options for upload, no-upload, and no-code

#### Scan output and reporting

The output of a scan can be saved in various formats. The following table maps the output formats and commands.

	<b>Checkov</b>	<b>Cortex CLI</b>
Output formats	<ul style="list-style-type: none"> <li>• cli</li> <li>• sarif</li> <li>• json</li> <li>• spdx</li> <li>• Junitxml</li> <li>• Cyclonedx</li> <li>• cyclonedx_json</li> </ul>	<ul style="list-style-type: none"> <li>• CSV</li> <li>• sarif</li> <li>• Junitxml</li> <li>• GitLab SAST</li> <li>• Cyclonedx</li> </ul>
Output command	<code>-o [FORMAT]</code>	<code>--output [FORMAT]</code>

Use cases: migrate Checkov to Cortex CLI

Here are some common Checkov workflows and their equivalents using the Cortex CLI tool.

#### Case #1: Basic directory scan

To perform a basic scan on a local directory:

- Checkov: `checkov --directory`
- Cortex CLI: `cortexcli code scan --directory`

#### Case #2: Scan and upload to your tenant

- Checkov: By default, scan results are uploaded to your tenant if you have an API token. For example, `checkov -d . --repo-id my-org/my-repo` will upload scan results
- Cortex CLI: `cortexcli appsec scan [scan type] --directory . --repo-id my-org/my-repo --branch main --upload-mode upload`

#### Case #3: Scan without uploading output

Get scan results in your terminal without uploading them to your tenant.

- Checkov: `checkov -d --skip-results-upload`
- Cortex CLI: `cortexcli appsec scan --directory . --upload-mode no-upload`

#### Advanced use case: CI/CD Pipeline Integration

You can integrate the Cortex CLI directly into your CI/CD pipelines to enable automated code scans by adding code snippets to your build script or pipeline configuration, such as a YAML file (See here for Cortex CLI snippets (such as GitHub Actions, Jenkins and more)).

When updating your CI/CD pipeline, replace the legacy `checkov` step with the new `cortex scan` command.

Docker image limitation: The Cortex CLI does not support SCA scans. You must update your pipelines to download the `cortexcli` binary directly if your workflow relies on this functionality.

#### Example 1. Example: GitHub Actions workflow

These examples demonstrate a GitHub Actions workflow in both legacy and the new Cortex CLI environments.



- Checkov YAML step

This example shows a typical step using `checkov-action`.

```
- name: Run Checkov scan
  uses: bridgecrewio/checkov-action@v1
  with:
    directory: ./terraform
    framework: terraform
    quiet: true # Don't output results to stdout
```

- Cortex CLI YAML step

This new step calls the **Cortex CLI** directly. It uses GitHub secrets to securely provide API credentials. Note the prerequisites in the YAML (such as `Node.js v22`). For a list of requirements, refer to both the general requirements (Connect Cortex CLI) and Application Security specific requirements (Cortex CLI for Code Security).

```
name: Cortex CLI Code Scan
on:
  push:
    branches:
      - main
  workflow_dispatch:
env:
  CORTEX_API_KEY: ${secrets.CORTEX_API_KEY}
  CORTEX_API_KEY_ID: ${secrets.CORTEX_API_KEY_ID}
  CORTEX_API_URL: https://api-viso-cq3sdpg7uyd6vqk66ccjyv.xdr-ga2-uat.us.paloaltonetworks.com

jobs:
  cortex-code-scan:
    runs-on: ubuntu-latest
    steps:
      - name: Checkout Repository
        uses: actions/checkout@v2

      - name: Set up Node.js
        uses: actions/setup-node@v4
        with:
          node-version: 22
      - name: Verify Node.js Version
        run: node -v
      - name: Download cortexcli
        run: |
          set -x
          crtx_resp=$(curl "${CORTEX_API_URL}/public_api/v1/unified-cli/releases/download-link?os=linux&architecture=amd64" \
            -H "x-xdr-auth-id: ${CORTEX_API_KEY_ID}" \
            -H "Authorization: ${CORTEX_API_KEY}")
          crtx_url=$(echo $crtx_resp | jq -r ".signed_url")
          curl -o cortexcli $crtx_url
          chmod +x cortexcli
          ./cortexcli --version
      - name: Run Cortex CLI Code Scan
        run: |
          ./cortexcli \
            --api-base-url "${CORTEX_API_URL}" \
            --api-key "${CORTEX_API_KEY}" \
            --api-key-id "${CORTEX_API_KEY_ID}" \
            code scan \
            --directory "${{github.workspace}}" \
            --repo-id "${{github.repository}}" \
            --branch "${{github.ref_name}}" \
            --source "GITHUB_ACTIONS" \
            --create-repo-if-missing
```

Migrate TwistCLI to the Cortex CLI

To help you transition your TwistCLI workflows, this section provides both the necessary flag references and a practical example to guide you in implementing your most common use cases. You can use the following references to map your existing TwistCLI workflows to their Cortex CLI equivalents.

- For TwistCLI flags, refer to Scan Images with `twistcli`
- For `cortexcli` flags common to all supported Cortex Cloud modules, refer to Cortex CLI common command line reference guide
- For specific Cloud Workload Protection (CWP) flags, refer to Cloud Workload Protection command line reference

**Use case:** Scan a container image

Here is how you can map your TwistCLI image scan command to the Cortex CLI.



- Legacy Twistcli command

```
./twistcli images scan \
--address "your Prisma Cloud Console URL" \
--user "your_access_key_id" \
--password "your_secret_key" \
ubuntu:latest
```

- Cortex CLI command

```
cortexcli image scan <container image path>
```

### 2.2.3 | Set up users and roles

#### Abstract

Learn how to set up users and roles in Cortex Cloud.

Cortex Cloud uses both Role-Based Access Control (RBAC) and Scope-Based Access Control (SBAC) to manage roles with specific permissions for controlling user access.

RBAC helps manage access to Cortex Cloud components and Cortex Query Language (XQL) datasets, so that users, based on their roles, are granted minimal access required to accomplish their tasks.

SBAC refines the RBAC permissions by granting access only to the relevant data that the user requires for their designated role. Users with Access Management permission can apply scopes to limit the data and content that users can be granted access to in Cortex Cloud, which are divided into different scoping areas. The scoping areas include Assets, Cases and Issues, and Endpoints, which can be applied as relevant to the enforcement area or entity. For more information on user scopes, see [Manage user scope](#).

Cortex Gateway and the tenant have different options and requirements.

Location	Details
Cortex Gateway	<p>A centralized portal for managing roles, user groups, and users for all tenants. Any roles and user groups created in Cortex Gateway are available for all tenants.</p> <p>In Cortex Gateway, on the Permissions page, you can manage users that have been added to your Customer Support Portal account or view users that have been created in the tenant using SSO (you cannot edit SSO users in Cortex Gateway). All users must have at least one role or belong to at least one user group to be saved in the Cortex Gateway. You can exclude different tenants or different Cortex products. For more information, see <a href="#">Cortex Gateway Administrator Guide</a>.</p> <p>Only users with the Account Admin role can manage roles, tenants, and user groups in Cortex Gateway.</p>
Cortex Cloud tenant	<p>(Recommended) All permissions and roles are specific to the tenant and exist only at the tenant level. Advanced settings, such as SBAC and Dataset access management, can be defined at the tenant level.</p> <p>Managing users, roles, scopes, user groups, and authentication settings in Cortex Cloud requires View/Edit RBAC permissions for Access Management (under Configurations). Account Admin and Instance Administrator roles are granted this permission by default.</p> <p>For more information, see <a href="#">Manage user roles</a>.</p>

#### Predefined user roles

Role-based access control (RBAC) enables you to use predefined Palo Alto Networks roles to assign access rights to Cortex Cloud users. You can manage roles for all Cortex Cloud tenants and services in the Gateway or in the Cortex Cloud tenant. By assigning roles, you enforce the separation of access among functional or regional areas of your organization.

Each role extends specific privileges to users. The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access privileges to administrative user accounts.

You can manage role permissions in Cortex Cloud, which are listed by the various components according to the sidebar navigation in Cortex Cloud. Some components include additional action permissions, such as pivot (right-click) options, to which you can also assign access, but only when you've given the user View/Edit permissions to the applicable component.

The default Palo Alto Networks roles provide a specific set of access rights to each role. You cannot edit the default roles directly, but you can save them as new roles and edit the permissions of the new roles. To view the predefined permissions for each default role, go to Settings  $\rightarrow$  Configurations  $\rightarrow$  Access Management  $\rightarrow$  Roles.

**NOTE:**



Some features are license-dependent. Accordingly, users may not see a specific feature if the feature is not supported by the license type or if they do not have access based on their assigned role or scope.

Default Role	Description
Account Admin	<p>A Super User role that is assigned directly to the user in Cortex Gateway and has full access to all Cortex products in your account, including all tenants added in the future. The Account Admin can assign roles for Cortex instances and activate Cortex tenants specific to the product.</p> <p><b>NOTE:</b></p> <p>The user who activated the Cortex product is assigned the Account Admin role. You cannot create additional Account Admin roles in the Cortex Cloud tenant. If you do not want the user to have Account Admin permission, you must remove the Account Admin role in Cortex Gateway.</p>
Instance Administrator	<p>View and edit permissions for all components and access all pages in the Cortex Cloud tenant. The Instance Administrator can also make other users an Instance Administrator for the tenant. If the tenant has predefined or custom roles, the Instance Administrator can assign those roles to other users.</p>
Viewer	<p>View the majority of the features for this instance.</p>
Developer	<p>Have limited permissions primarily focused on viewing and monitoring security information. Access and analyze scan results, track progress, and collaborate with security teams. Does not include ability to modify detection rules, enforcements, or directly address security issues.</p>
CLI Read Only Role	<p>View scripts, playbooks, credentials, and CLI tool.</p>
CLI Role	<p>View scripts, playbooks, and credentials. View and edit permission for CLI tool.</p>
AppSec Admin	<p>Full permissions for all Cloud Application Security-related activities. Create and modify detection rules within the Code/Build domain, track progress, and adjust enforcements as needed. Additionally, triage and investigate findings, issues, and cases spanning from code to cloud. The role also includes complete visibility into all cloud assets.</p>
Security Admin	<p>Can triage and investigate issues and cases, respond (excluding Live Terminal), and edit profiles and policies.</p>
AI Security Administrator	<p>Manage all aspects of AI security in the organization.</p>
AI Security Viewer	<p>Views and investigates all issues and findings on AI security.</p>
Data Security Administrator	<p>View and manage all data security information, including objects and data patterns.</p>
Data Security Viewer	<p>View all data security information, including objects and data patterns.</p>
Identity Security Administrator	<p>The Identity Security Administrator has full access to all general Admin and Identity Security capabilities.</p>



<b>Default Role</b>	<b>Description</b>
Identity Security Viewer	The Identity Security Viewer can view the majority of the features for this Identity Security and can edit reports.

#### 2.2.3.1 | User group management

##### Abstract

Create user groups and assign roles and users to further refine your requirements.

Users are assigned roles and permissions either by being assigned a role directly or by being assigned membership in one or more user groups. A user group can only be assigned to a single role, but users can be added to multiple groups if they require multiple roles. You can also nest groups to achieve the same effect. Users who have multiple roles through either method will receive the highest level of access based on the combination of their roles. The same principle for users with multiple roles is followed for both the Role-Based Access Control (RBAC) access permissions and the Scope-Based Access Control (SBAC) granular scoping, so that users receive the highest level of access by combining their roles.

Example 2.

- Joe has an Analyst role and is a member of the Tier-1 Analyst user group, which is assigned the Triage role. Joe has the permissions of the Analyst role and the Triage role. Joe is assigned 2 roles, and has the highest permission based on the combination of both roles.
- John is a member of two user groups - Tier-1 Analyst and Tier-2 Analyst. One group is configured to use the Triage role and the other group is configured to use the Incident Response role. John is assigned both roles and has the highest permissions based on the combination of all roles.
- Jack is a member of the Tier-2 user group, which has an Incident response role. This user group is included in a Tier-3 user group (Threat Hunter role), added as a nested group. Jack is assigned both roles and has the highest permissions based on the combination of all roles.

On the User Groups page, you can create a new user group for several different system users or groups. You can see information including the details of all user groups, the roles, nested groups, IdP groups (SAML), and when the group was created/updated.

You can also right-click in the table to edit, save as a new group, remove (delete) a group, and copy text to the clipboard.

##### NOTE:

You can create user groups in the tenant or Cortex Gateway. User groups created in Cortex Gateway cannot be mapped to SAML groups. Only user groups created in the tenant support SAML group mapping and scoring. We recommend creating user groups in the Cortex tenant because:

- User groups are available for all tenants, and you may want different user groups in different tenants, such as dev/prod.
- You can apply granular scoping for a user role by granting access only to the relevant data that the user requires for their designated role in the tenant. You also need to enable scope-based access control in the Server Settings page. For more information, see [Manage user scope](#).

Before configuring SBAC, ensure that you review [Understand scoping](#) in the [Manage user scope](#) section.

How to create a user group

1. Go to Settings â€“ Configurations â€“ Access Management â€“ User Groups.

If creating in Cortex Gateway, go to Permission Management â€“ User Groups.

2. To create a new user group for several different system users or groups, click New Group, and add the following parameters:

<b>Parameter</b>	<b>Description</b>
Name	Name of the user group.
Description	Description of the user group.
Group for product	(Cortex Gateway only) If you have multiple products, select the relevant Cortex product.
Role	Select the group role associated with this user group. You can only have a single role designated per group.  In Cortex Gateway, you can only select either Instance Administrator or a custom role created in the Gateway.



Parameter	Description
Users	<p>Select the users you want to belong to this user group.</p> <p><b>NOTE:</b></p> <p>If users have been created in the CSP, but you want them to access the tenant through SSO only, skip this field and add only SAML group mapping after SSO is set up, otherwise, users can access the tenant through both the CSP and SSO.</p> <p>If you have not yet created any users, skip this field and add them later. See <a href="#">Set up authentication</a>.</p>
Nested Groups	<p>Lists any nested groups associated with this user group. If you have an existing group, you can add a nested group.</p> <p>User groups can include multiple users and nested groups, which inherit the permissions of parent user groups. The user group will have the highest level of permission.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Group A has Tier-1 Analyst permissions</li> <li>• Group B has Tier-2 Analyst permissions</li> </ul> <p>If you add Group A as a nested group in Group B, Group A inherits Group B's permissions (Tier-1 and Tier-2 permissions).</p> <p>In Cortex Gateway, you can only add user groups that are created in Cortex Gateway.</p>
SAML Group Mapping	<p>(Relevant when creating a user group in the Cortex tenant only.)</p> <p>Maps the SAML group membership to this user group. For example, you have defined a <code>Cortex Admins</code> group. You need to name this group exactly how it appears in Okta.</p> <p>You can add multiple groups by separating them with a comma.</p> <p><b>NOTE:</b></p> <p>When using Azure AD for SSO, the SAML group mapping needs to be provided using the group object ID (GUID) and not the group name.</p> <p>If you have not set up SSO in your tenant, skip this field and add it later. After you have added it, follow the procedure relevant to your IdP. For example, see <a href="#">Set up Okta as the identity using SAML 2.0</a>.</p>

3. (Optional) When creating the user group in the tenant, configure granular scoping for the user group.

If creating the user group in the Cortex Gateway, you can skip this step, as scoping is only supported in the tenant.

a. Click the Scope tab.

b. Expand the scoping areas that you want to grant the user role access to in the tenant by clicking the chevron icon (>) beside the scoping area title, and make any changes required. The following table explains the options available to configure:

Scoping Area	Granular Scoping Configurations
Assets	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• No assets: No asset is accessible.</li> <li>• All assets: Defines access to all assets.</li> <li>• Select asset groups: Defines access to the specific assets associated with the Asset Groups selected, and to view all their related cases, issues, and findings for these specific assets and Asset Groups. Under Select asset groups, define the specific asset groups that you want to grant access. Only Asset Groups relevant for scoping are listed, which are asset groups that are using only the asset attributes listed in Manage user scope (under Understand scoping &amp; Scoping Areas &amp; Assets).</li> </ul> <p>The scoping of assets also affects the scoping of cases, issues, and findings.</p> <p><b>NOTE:</b></p> <p>Visibility of Security domain Issues that refer to assets with agents is controlled by the Endpoints scoping configuration.</p>



Scoping Area    Granular Scoping Configurations	
Cases and Issues	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No cases and issues: Defines access to no cases and issues.</li> <li>All cases and issues: Defines access to all cases and issues. Users can view cases or issues referencing assets within their scope. Use the Assets section to define which assets are in scope.</li> <li>Select domains: Defines access to the domains selected to view their related cases and issues. Under Select domains, define the specific domains that you want to grant access.</li> </ul> <p>Users can only view cases or issues referencing assets and endpoints within their scope. Use the Assets section to define which assets are in scope.</p> <p>When selecting All cases and issues or Select domains, you can separately configure access to issues and cases that lack an asset reference or where the referenced asset is not in All Assets and All Endpoints inventories. To provide access, select the Allow access to cases and issues that are not referencing known assets or endpoints checkbox.</p>
Endpoints	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No endpoints: Defines access to no endpoints with no ability to view their related agent management and enterprise policies.</li> <li>All endpoints: Defines access to all endpoints with the ability to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> <li>Select specific (at least one required): Defines specific access to all endpoint groups by selecting Endpoint Groups or all endpoint tags by selecting Endpoint Tags to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> </ul>

#### **IMPORTANT:**

By default, Enable Scope Based Access Control is disabled in Settings → Configurations → General → Server Settings, and granular scoping is not enforced. Before enabling SBAC, we recommend that an administrator or a user with Access Management permissions first ensures that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes. For more information, see [Manage user scope](#).

4. Click Create to create the user group.

#### 2.2.3.2 | Assign user roles and groups

##### Abstract

Learn how to assign users to roles and user groups.

Assign roles directly to users or create user groups and assign roles to those groups. We recommend creating user groups (with a user role), and assigning users to those user groups rather than creating direct roles for each user.

##### **NOTE:**

If an existing user in the Cortex Gateway no longer has a role or a user group assigned, the user is revoked. Any roles, user groups, or egress configurations created by that user are shown as created by Revoked user instead of the user's email address.

Assign a user/user group to a role

Cortex Cloud provides predefined built-in user roles that provide specific access rights that cannot be modified. You can also create custom, editable user roles. If a user does not have any Cortex Cloud access permissions that are assigned specifically to them, the field displays No-Role.

1. Select Settings → Configurations → Access Management → Users.
2. Right-click the relevant user, and select Edit User Permissions.

#### **TIP:**

To apply the same settings to multiple users, select them, and then right-click and select Edit Users Permissions.

3. Ensure the Role tab is selected.
4. Under Role, select the default or custom role.
5. (Optional) Under User Groups, add the user to a group.



6. (Optional) Under Show Accumulated Permissions:

a. Do one of the following:

- Select all to view the combined permissions for every role and user group assigned to the user.
- Select a specific role assigned to the user to view the available permissions for that role.

b. Under Components, expand each list to view the permissions.

**IMPORTANT:**

Setting Cortex Query Language (XQL) dataset access permissions for a user role can only be performed from Cortex Cloud Access Management. For more information, see [Manage user roles](#).

7. (Optional) You can configure and manage granular scoping:

a. Click the Scope tab.

b. Under Scope Definition, expand the scoping areas that you want to grant the user role access to in the tenant by clicking the chevron icon (>) beside the scoping area title, and make any changes required. The following table explains the options available to configure:

**IMPORTANT:**

Before configuring, ensure that you review [Understand scoping](#) in the [Manage user scope](#) section.

Scoping Area	Granular Scoping Configurations
Assets	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"><li>• No assets: No asset is accessible.</li><li>• All assets: Defines access to all assets.</li><li>• Select asset groups: Defines access to the specific assets associated with the Asset Groups selected, and to view all their related cases, issues, and findings for these specific assets and Asset Groups. Under Select asset groups, define the specific asset groups that you want to grant access. Only Asset Groups relevant for scoping are listed, which are asset groups that are using only the asset attributes listed in <a href="#">Manage user scope</a> (under <a href="#">Understand scoping</a> â Scoping Areas â Assets).</li></ul> <p>The scoping of assets also affects the scoping of cases, issues, and findings.</p> <p><b>NOTE:</b></p> <p>Visibility of Security domain Issues that refer to assets with agents is controlled by the Endpoints scoping configuration.</p>
Cases and Issues	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"><li>• No cases and issues: Defines access to no cases and issues.</li><li>• All cases and issues: Defines access to all cases and issues. Users can view cases or issues referencing assets within their scope. Use the Assets section to define which assets are in scope.</li><li>• Select domains: Defines access to the domains selected to view their related cases and issues. Under Select domains, define the specific domains that you want to grant access.</li></ul> <p>Users can only view cases or issues referencing assets and endpoints within their scope. Use the Assets section to define which assets are in scope.</p> <p>When selecting All cases and issues or Select domains, you can separately configure access to issues and cases that lack an asset reference or where the referenced asset is not in All Assets and All Endpoints inventories. To provide access, select the Allow access to cases and issues that are not referencing known assets or endpoints checkbox.</p>



Scoping Area    Granular Scoping Configurations	
Endpoints	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No endpoints: Defines access to no endpoints with no ability to view their related agent management and enterprise policies.</li> <li>All endpoints: Defines access to all endpoints with the ability to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> <li>Select specific (at least one required): Defines specific access to all endpoint groups by selecting Endpoint Groups or all endpoint tags by selecting Endpoint Tags to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> </ul>

#### **IMPORTANT:**

By default, Enable Scope Based Access Control is disabled in Settings â Configurations â General â Server Settings, and granular scoping is not enforced. Before enabling SBAC, we recommend that an administrator or a user with Access Management permissions first ensures that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes. For more information, see [Manage user scope](#).

- Click Save.

#### Perform additional tasks

For more information about additional tasks such as creating a custom role, modifying a user's role, or removing a user's role, see [Manage user access](#) or [Cortex Gateway Administrator Guide](#).

### 2.2.4 | Manage API keys

API keys are used to manage and secure API interactions. An API key is essentially a unique string of alphanumeric characters that acts as a credential, allowing a specific user or application to access and interact with a particular API. When you request data or perform an action through an API call, you must include this API key in the header. Cortex Cloud then verifies the key's authenticity and, if valid, grants the requested access.

#### How to create an API key

- Select Settings â Configurations â Integrations â API Keys â New Key.
- In the Role tab, perform for the following:
  - Under Security Level, select the type of API Key you want to generate: Advanced or Standard. The Advanced API key hashes the key using a nonce, a random string, and a timestamp to prevent replay attacks. cURL does not support this but it is suitable with scripts.
  - Under Role, select the desired level of access for this key. You can select from predefined roles or custom roles. Roles are available according to what was defined in either the Cortex Gateway or Cortex Cloud Access Management. You can view the configuration of the role selected by expanding the sections under Components. For more information, see [Assign user roles and groups](#).
  - (Optional) Under Comment, provide a comment that describes the purpose of the API key.
  - (Optional) If you want to define a time limit on the API key authentication, select Enable Expiration Date, and select the expiration date and time. You can track the expiration date of each API key in the API Keys page. In addition, Cortex Cloud displays a API Key Expiration notification in the Notification Center one week and one day prior to the defined expiration date.
- (Optional) To configure and manage granular scoping for Scope-Based Access Control (SBAC), click the Scope tab, and under Scope Definition, expand the scoping areas that you want to grant the user role access to for this API by clicking the chevron icon (>) beside the scoping area title. The following table explains the options available to configure:

#### **IMPORTANT:**

Before configuring, ensure that you review [Understand scoping](#) in the [Manage user scope](#) section.



Scoping Area	Granular Scoping Configurations
Assets	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No assets: No asset is accessible.</li> <li>All assets: Defines access to all assets.</li> <li>Select asset groups: Defines access to the specific assets associated with the Asset Groups selected, and to view all their related cases, issues, and findings for these specific assets and Asset Groups. Under Select asset groups, define the specific asset groups that you want to grant access. Only Asset Groups relevant for scoping are listed, which are asset groups that are using only the asset attributes listed in Manage user scope (under Understand scoping â Scoping Areas â Assets).</li> </ul> <p>The scoping of assets also affects the scoping of cases, issues, and findings.</p> <p><b>NOTE:</b></p> <p>Visibility of Security domain Issues that refer to assets with agents is controlled by the Endpoints scoping configuration.</p>
Cases and Issues	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No cases and issues: Defines access to no cases and issues.</li> <li>All cases and issues: Defines access to all cases and issues. Users can view cases or issues referencing assets within their scope. Use the Assets section to define which assets are in scope.</li> <li>Select domains: Defines access to the domains selected to view their related cases and issues. Under Select domains, define the specific domains that you want to grant access.</li> </ul> <p>Users can only view cases or issues referencing assets and endpoints within their scope. Use the Assets section to define which assets are in scope.</p> <p>When selecting All cases and issues or Select domains, you can separately configure access to issues and cases that lack an asset reference or where the referenced asset is not in All Assets and All Endpoints inventories. To provide access, select the Allow access to cases and issues that are not referencing known assets or endpoints checkbox.</p>
Endpoints	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No endpoints: Defines access to no endpoints with no ability to view their related agent management and enterprise policies.</li> <li>All endpoints: Defines access to all endpoints with the ability to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> <li>Select specific (at least one required): Defines specific access to all endpoint groups by selecting Endpoint Groups or all endpoint tags by selecting Endpoint Tags to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> </ul>

**IMPORTANT:**

By default, Enable Scope Based Access Control is disabled in Settings â Configurations â General â Server Settings, and granular scoping is not enforced. Before enabling SBAC, we recommend that an administrator or a user with Access Management permissions first ensures that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes. For more information, see [Manage user scope](#).

4. Click Generate to generate the API key.

5. Copy the generated API key and click Done.

**IMPORTANT:**

You will not be able to view the API key again after you complete this step. Ensure that you copy the API key before closing the notification.

**Actions available on API Keys**

Below are some of the main pivot (right-click) options for actions available on each API key listed in the API Keys table. Only tasks that need further explanation are explained below.



Action	Description
View Examples	Copies the Python 3 example, so you can edit it to set up your own API calls.
Copy text to clipboard / Copy entire row	Copies the value of an API setting, such as the ID, to the clipboard by right-clicking the setting and selecting Copy text to clipboard. You can copy all the settings of an API key by right-clicking and selecting Copy entire row.
Filter API keys	Filters the API keys by selecting one of the filter options, such as Show rows 30 days prior to.... You can then adjust the filter options to filter the API keys according to all the available fields.

## 2.2.5 | Set up authentication

### Abstract

Authenticate Cortex Cloud users using SAML 2.0 or Cortex Gateway.

You can create users in the Customer Support Portal or by using SAML Single Sign-On (SSO) in the tenant. Users authenticate by doing the following:

- Authenticate through the Customer Support Portal

When users log into Cortex Gateway or the tenant (provided they are assigned a role) they are prompted to sign into the Customer Support Portal using their username and password or 2FA (if set up). This is the default method of authentication.

After you have created users, add them to user groups or assign roles directly.

- Authenticate using SAML single sign-on in the Cortex Cloud tenant

Users can be authenticated using your IdP provider such as Okta, Ping, or Azure AD. You can use any IdP that supports SAML 2.0. After you configure the SSO integration you need to map group SAML group membership to user groups in Cortex Cloud.

SSO authentication has the following advantages:

- Removes the administrative burden of requiring separate accounts to be configured through the Customer Support Portal.
- Enforces multi-factor authentication (MFA) and any conditional access policies on the user login at the IdP before granting a user access to Cortex Cloud.
- Maps SAML group memberships to user groups and roles, allowing you to manage role-based access control.
- Removes access to Cortex Cloud when a user is removed or disabled in the IdP.

Customer Support Portal authentication, by contrast, is useful if you have users who need the same permissions across multiple tenants. If you use SSO for multiple tenants, you must set up the SSO configuration separately for each tenant, both in the IdP and in Cortex Cloud.

If you want to restrict the user login through SSO only, remove any direct role and user group mapping for the user on Cortex Gateway or the Cortex Cloud tenant. This removes Customer Support Portal access for the user. You then need to ensure that you add the SAML group mapping. The user can access and acquire the user group and roles based on SAML group mapping. Once completed, the user is able to access Cortex Cloud using SSO only and will not be able to use Customer Support Portal login method.

### TIP:

You should have at least one user in the Customer Support Portal for backup, in case of any authentication issues with your IdP provider.

### 2.2.5.1 | Authenticate users through the Customer Support Portal

#### Abstract

Authenticate Cortex Cloud users when using the Customer Support Portal.

When you add users to your Customer Support Portal account, users are sent an invitation to join. After they accept, users can access Cortex Gateway and tenants, but they cannot view any tenants in the Gateway and cannot view any data in the tenant unless they are assigned a direct role or user group role. Only Account Admins can make any changes in Cortex Gateway.

### NOTE:

You must be assigned the Super User role in the Customer Support Portal to add users in the Customer Support Portal.



The first Super User who logs into Cortex Gateway is automatically assigned the Account Admin role and has access to the tenant. The user who activates the Cortex Cloud tenant will also be assigned the Account Admin role (if there is no current Account Admin role) or Instance Admin (if there is an existing Account Admin role) and will have access to the tenant. Any additional users including Super Users need to be assigned access to the tenant.

When users log into Cortex Gateway or the tenant they are prompted to sign into the Customer Support Portal using their username and password. This is the default method of authentication.

**NOTE:**

After users are added to the Customer Support Portal and they accept the invitation, you can manage them in Cortex Gateway or the Cortex Cloud tenant.

How to authenticate users through the Customer Support Portal

1. Add users to your Customer Support Portal account, by logging into <https://support.paloaltonetworks.com/> and doing one of the following:

- In your Customer Support User Account, create users.
  1. On the left-hand side menu, select Members → Create New User .
  2. Add the member details and click Submit.

An email is sent to the user which must be accepted within seven days.

For more detailed information including how to reset the invitation, see How a Super User Creates a New Customer Support Portal User Account.

- Send an Account Registration Link.

A registration link is generated by a Customer Support Portal account Super User and shared with users who need to create a login for access to the account.

1. On the left-hand side menu, select Account Management → Account Details, and click User Access.
2. In the Account Registration link, click Create.
3. Copy and send the link to the users you want to add.

When clicking the link, users are required to enter their registration details and submit them to the Customer Support Portal.

After users have submitted their details, the Super User receives a notification that a user has been created.

For more information about how to generate, regenerate, or disable a link, see How to Use the Account Registration Link.

2. Log in to Cortex Gateway .

After the user accepts the invitation, you see the added users. You must assign a role to the user directly or add them to user groups in Cortex Gateway or in the Cortex Cloud tenant.

## 2.2.5.2 | Authenticate users using SSO

Abstract

Set up authentication in the Cortex Cloud tenant using SSO.

Cortex Cloud enables you to authenticate system users securely across enterprise-wide applications and websites with one set of credentials using single sign-on (SSO) with SAML 2.0. System users can authenticate using your organization's Identity Provider (IdP), such as Okta or PingOne. You can integrate with any IdP that is supported by SAML 2.0.

Configuring SSO with SAML 2.0 is dependent on your organization's IdP. Some of the parameter values need to be supplied from your organization's IdP and some need to be added to your organization's IdP. You must have sufficient knowledge about IdPs, how to access your organization's IdP, which values to add to Cortex Cloud, and which values to add to your IdP fields.

**NOTE:**

- To set up SSO authentication in the tenant, you must be assigned an Instance Administrator or Account Admin role.
- SAML 2.0 users must log in to Cortex Cloud using the FQDN (full URL) of the tenant. To allow login directly from the IdP to , you must set the relay state on the IdP to the FQDN of the tenant.
- If you have multiple tenants, you must set up the SSO configuration separately for each tenant, both in the IdP and in Cortex Cloud.
- Create groups in Cortex Cloud that correspond to the groups in your IDP. Add the appropriate SAML group mapping from your IdP to each of the user groups in Cortex Cloud.
- When a user logs in for the first time, the user account is automatically created (JIT provisioning), provided you mapped groups. This process requires either using the default role option or ensuring that SSO groups are properly mapped to Cortex Cloud groups. If the user belongs to a group that has a mapping, the user will be granted access automatically upon login.
- If you are using AWS SSO, the Application ACS URL refers to the Single Sign-On URL and the Application SAML Audience refers to the Audience URL (SP Entity ID). Both values can be copied from the Authentication Settings in Cortex Cloud.



If you are configuring Okta or Azure, follow the procedure in Okta or Azure AD. You can also adapt these instructions for use with any similar SAML 2.0 IdP.

1. If you want to add another SSO connection to enable managing user groups with different roles and different IdPs, click Add SSO Connection.

Different SSO parameters for an SSO are displayed to configure according to your organization's additional IdP.

**NOTE:**

- The first SSO cannot be deleted, it can only be deactivated by toggling SSO Enabled to off.
- The Domain parameter is predefined for the first SSO.

If you add additional SSO providers, you must provide the email Domain in the SSO Integration settings for all providers except the first. Cortex Cloud uses this domain to determine to which identity provider to send the user for authentication.

- When mapping IdP user groups to Cortex Cloud user groups, you must include the group attribute for each IdP you want to use. For example, if you are using Microsoft Azure and Okta, your Cortex Cloud user group SAML Group Mapping field must include the IdP groups for each provider. Each group name is separated by a comma.

2. Set the following parameters using your organization's IdP.

- General parameters
- IdP Attribute Mapping
- Advanced Settings (optional)

3. Save your changes.

Whenever an SSO user logs in to Cortex Cloud, the following login options are available.

- Sign-in with SSO

If you have enabled more than one SSO provider, an optional email field appears. If the user does not enter an email address or if the email address does not match an existing domain, the user is automatically directed to the default IdP provider (the first in the list of SSO providers in the Authentication Settings). If the user enters an email address and it matches a domain listed in the Domain field in the SSO Integration settings for one of your IdPs, Sign-In with SSO sends the user to the IdP associated with that email domain.

General parameters

Parameter	Description
IdP SSO or Metadata URL	Select the option that meets your organization's requirements.  Indicates your SSO URL, which is a fixed, read-only value based on your tenant's URL using the format <code>https://&lt;name of tenant&gt;.crtx.paloaltonetworks.com/idp/saml</code> . For example, <code>https://tenant1.crtx.paloaltonetworks.com/idp/saml</code>  You need this value when configuring your IdP.
IdP SSO URL	Specify your organization's SSO URL, which is copied from your organization's IdP.
Metadata URL	
Audience URI (SP Entity ID)	Indicates your Service Provider Entity ID, also known as the ACS URL. It is a fixed, read-only value using the format, <code>https://&lt;name of tenant&gt;.paloaltonetworks.com</code> . For example <code>https://tenant1.crtx.paloaltonetworks.com</code> .  You need this value when configuring your organization's IdP.
Default Role	(Optional) Select the default role that you want any user to automatically receive when they are granted access to Cortex Cloud through SSO. This is an inherited role and is not the same as a direct role assigned to the user.



Parameter	Description
IdP Issuer ID	Specify your organization's IdP Issuer ID, which is copied from your organization's IdP.
X.509 Certificate	Specify your X.509 digital certificate, which is copied from your organization's IdP.
Domain	Relevant only for multiple SSOs. For one SSO, this is a fixed, read-only value. Associate this IdP with a specific email domain (user@<domain>). When logging in, users are redirected to the IdP associated with their email domain or to the default IdP if no association exists.

#### IdP attribute mapping

These IdP attribute mappings are dependent on your organization's IdP.

Parameter	Description
Email	Specify the email mapping according to your organization's IdP.
Group Membership	Specify the group membership mapping according to your organization's IdP. <b>NOTE:</b> Cortex Cloud requires the IdP to send the group membership as part of the SAML token. Some IdPs send values in a format that include a comma, which is not compatible with Cortex Cloud. In that case, you must configure your IdP to send a single value without a comma for each group membership. For example, if your IdP sends the Group DN (a comma-separated list), by default, you must configure IdP to send the Group CN (Common Name) instead.
First Name	Specify the first name mapping according to your organization's IdP.
Last Name	Specify the last name mapping according to your organization's IdP.

#### Advanced settings

The following advanced settings are optional to configure and some are specific for a particular IdP.

Parameter	Description
Relay State	(Optional) Specify the URL for a specific page that you want users to be directed to after they've been authenticated by your organization's IdP and log in to Cortex Cloud.
IdP Single logout URL	(Optional) Specify your IdP single logout URL provided by your organization's IdP to ensure that when a user initiates a logout from Cortex Cloud, the identity provider logs the user out of all applications in the current identity provider login session.



Parameter	Description
SP Logout URL	(Optional) Indicates the Service Provider logout URL that you need to provide when configuring a single logout from your organization's IdP to ensure that when a user initiates a logout from Cortex Cloud, the identity provider logs the user out of all applications in the current identity provider login session. This field is read-only and uses the following format <code>https://&lt;name of tenant&gt;.crtx.paloaltonetworks.com/idp/logout</code> , such as <code>https://tenant1.crtx.paloaltonetworks.com/idp/logout</code> .
Service Provider Public Certificate	(Optional) Specify your organization's IdP service provider public certificate.
Service Provider Private Key (Pem Format)	(Optional) Specify your organization's IdP service provider private key in Pem Format.
Remove SAML RequestedAuthnContext	(Optional) Requires users to log in to Cortex Cloud using additional authentication methods, such as biometric authentication.  Selecting this removes the error generated when the authentication method used for previous authentication is different from the one currently being requested. See here for more details about the <code>RequestedAuthnContext</code> authentication mismatch error.
Force Authentication	(Optional) Requires users to reauthenticate to access the Cortex Cloud tenant if requested by the IdP, even if they already authenticated to access other applications.

#### Troubleshoot SSO issues

The following list describes the common errors and issues when using SAML 2.0 authentication.

- Errors in your IdP could mean the Service Provider Entity ID and/or Service Identifier are not properly configured in the IdP or in the Cortex Cloud settings.
- SAML attributes from the IdP are not properly mapped in Cortex Cloud. The attributes are case sensitive and must exactly match in your IdP and in the Cortex Cloud IdP Attributes Mapping.
- Group memberships from the IdP have not been properly mapped to Cortex Cloud user groups. Verify the values your identity provider is sending, to properly map the groups in Cortex Cloud.
- The identity provider is not configured to sign both the SAML response and the assertion on the login token. Your IdP must be configured to sign both to ensure a secure login.
- If you require further troubleshooting, we recommend using your browser's built-in developer tools or additional browser plugins to capture the login request and SAML token.

#### 2.2.5.3 | Set up Okta as the Identity Provider Using SAML 2.0

This topic provides specific instructions for using Okta to authenticate your Cortex Cloud users. As Okta is a third-party software, specific procedures, and screenshots may change without notice. We encourage you to also review the Okta documentation for app integrations.

To configure SAML SSO in Cortex Cloud, you must be a user who can access the Cortex Cloud tenant and have either the Account Admin or Instance Administrator role assigned.

##### Task 1. Configure Okta Groups

Within Okta, assign users to groups that match the user groups they will belong to in Cortex Cloud. Users can be assigned to multiple Okta groups and receive permissions associated with multiple user groups in Cortex Cloud. Use an identifying word or phrase, such as Cortex Cloud, within the group names. For example, Cortex Cloud Analysts. This allows you to send only relevant group information to Cortex Cloud, based on a filter you will set in the group attribute statement.



Create a list of the Okta groups and their corresponding Cortex Cloud user groups (or the Cortex Cloud user groups you intend to create) and save this list for later use when configuring user groups in Cortex Cloud.

#### Task 2. Copy Single SSO and Audience URI Values from Cortex Cloud

1. Expand the SSO Integration settings.
2. Copy and save the values for Single Sign-On URL and Audience URI (SP Entity ID).

Both values are needed to configure your IdP settings.

You cannot save the enabled SSO Integration at this time, as it requires values from your IdP.

#### Task 3. Configure Cortex Cloud Application in Okta

1. In Okta, create a Cortex Cloud application and Edit the SAML Settings.
2. Paste the Single sign-on URL and the Audience URI (SP Entity ID) that you copied from the Cortex Cloud SSO settings. The Audience URI should also be pasted in the Default RelayState field, which allows users to log in to Cortex Cloud directly from the Okta dashboard.
3. Click Show Advanced Settings, verify that Okta is configured to sign both the response and the assertion signature for the SAML token, and then click Hide Advanced Settings.
4. Cortex Cloud requires the IdP to send four attributes in the SAML token for the authenticating user.
  - Email address
  - Group membership
  - First Name
  - Last Name

Configure Okta to send group memberships of the users using the `memberof` attribute. Use the word or phrase you selected when configuring Okta groups (such as Cortex Cloud) to create a filter for the relevant groups.

5. Copy the exact names of the attribute statements from Okta and save them, as they are required to configure the Cortex Cloud SSO integration. In the example above, the names are FirstName, LastName, Email, and memberOf. The attribute names are case-sensitive.

#### Task 4. Copy IdP SSO URL, Identity Provider Issuer, and X.509 Certificate Values

1. In Okta, from your Cortex Cloud application page, click View SAML setup instructions. If you do not see this button, verify you are on the Sign On tab of the application.
2. Copy and save the values for Identity Provider Single Sign-On URL, Identity Provider Issuer, and the X.509 Certificate. These values are needed to configure your Cortex Cloud SSO Integration.

#### Task 5. Configure the Cortex Cloud SSO Integration

1. Expand the SSO Integration settings.
2. Use the following table to complete the SSO Integration settings, based on the values you saved from Okta.

Okta	Cortex Cloud Field
Identity Provider Single Sign-On URL	IdP SSO URL
Identity Provider Issuer	IdP Issuer ID
X.509 Certificate	X.509 Certificate

3. In the IdP Attributes Mapping section, enter the attribute names from Okta. The names are case-sensitive and must match exactly.
4. Save your settings.

#### Task 6. Map SAML Group Memberships to Cortex Cloud User Groups

1. Right-click a user group and select Edit Group.



2. In the SAML Group Mapping field add the Okta group(s) that should be associated with this user group. Multiple groups should be separated with a comma. The Okta group name must match the exact value sent in the token.
3. Save your settings.
4. Repeat for each user group.

#### Task 7. Test SSO Login

1. Go to the Cortex Cloud tenant URL and Sign-In with SSO.

**NOTE:**

When using SAML 2.0, users are required to authenticate by logging in directly at the tenant URL. They cannot log in via Cortex Gateway.

2. After authentication to Okta, you are redirected again to the Cortex Cloud tenant.
3. When logged in, validate that you have been assigned the proper roles.

To view your role and any role assigned to a user group you are a member of, click your name in the bottom left-hand corner, and click About.

#### 2.2.5.4 | Set up Azure AD as the Identity Provider Using SAML 2.0

This topic provides specific instructions for using Azure AD to authenticate your Cortex Cloud users. As Azure AD is a third-party software, specific procedures, and screenshots may change without notice. We encourage you to also review the Azure AD documentation.

To configure SAML SSO in Cortex Cloud, you must be a user who can access the Cortex Cloud tenant and have either the Account Admin or Instance Administrator role assigned.

The following video is a step-by-step guide configuring SSO for Azure AD: Azure AD SSO.

#### Task 1. Configure Azure AD Security Groups

Within Azure AD, assign users to security groups that match the user groups they will belong to in Cortex Cloud. Users can be assigned to multiple Azure AD groups and receive permissions associated with multiple user groups in Cortex Cloud. Use an identifying word or phrase, such as Cortex Cloud, within the group names. For example, Cortex Cloud Analysts. This allows you to send only relevant group information to Cortex Cloud, based on a filter you will set in the group attribute statement.

#### Task 2. Copy Single SSO and Audience URI Values from Cortex Cloud

1. By default, SSO is disabled in Cortex Cloud.
2. Expand the SSO Integration settings.
3. Copy and save the values for Single Sign-On URL and Audience URI (SP Entity ID).

Both values are needed to configure your IdP settings.

**IMPORTANT:**

When copying the Single Sign-On URL value, remove `idp/saml` and leave the trailing `/`.

For example, if the Single Sign-On URL is `https://clientname.panproduct.region.paloaltonetworks.com/idp/saml`, just copy `https://clientname.panproduct.region.paloaltonetworks.com/`.

4. You cannot save the enabled SSO Integration at this time, as it requires values from your IdP.

#### Task 3. Configure Cortex Cloud Application in Azure AD

1. From within Azure AD, create a Cortex Cloud application and Edit the Basic SAML Configuration.



## Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Cortex XSOAR 8 Production.

The screenshot shows two configuration sections for SAML setup:

**1 Basic SAML Configuration**

Identifier (Entity ID)	<code>https://trainingxsoar.xsoarnetwork.com</code>
Reply URL (Assertion Consumer Service URL)	<code>https://trainingxsoar.xsoarnetwork.com/idp/saml</code>
Sign on URL	<code>https://trainingxsoar.xsoarnetwork.com</code>
Relay State (Optional)	<code>https://trainingxsoar.xsoarnetwork.com</code>
Logout Url (Optional)	<i>Optional</i>

**2 Attributes & Claims**

givenname	<code>user.givenname</code>
surname	<code>user.surname</code>
emailaddress	<code>user.mail</code>
name	<code>user.userprincipalname</code>
memberOf	<code>user.groups</code>
Unique User Identifier	<code>user.userprincipalname</code>

- Paste the Single sign-on URL and the Audience URI (SP Entity ID) that you copied from the Cortex Cloud SSO settings. The Single sign-on URL from Cortex Cloud should be pasted in the Reply URL and the Sign on URL fields. The Audience URI (SP Entity ID) value from Cortex Cloud should be pasted in the Identifier (Entity ID) and Relay State fields. This allows users to log in to Cortex Cloud directly from Azure AD.



**Basic SAML Configuration**

Save | Got feedback?

**Identifier (Entity ID) \*** ⓘ  
*The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.*

Default
https://[REDACTED].com

Add identifier  
**Patterns:** https://samitoolkit.azurewebsites.net

**Reply URL (Assertion Consumer Service URL) \*** ⓘ  
*The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.*

Index	Default
https://[REDACTED]	<input checked="" type="checkbox"/> ⓘ

Add reply URL  
**Patterns:** https://samitoolkit.azurewebsites.net/SAML/Consume

**Sign on URL \***  
*Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.*

https://[REDACTED].com/ ✓  
**Patterns:** https://samitoolkit.azurewebsites.net/

**Relay State (Optional) ⓘ**  
*The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.*

https://[REDACTED].com/

3. In the SAML Certificates section, click Edit and verify that Azure is configured to sign both the response and the assertion.

**SAML Signing Certificate**

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Save | New Certificate | Import Certificate | Got feedback?

Status	Expiration Date	Thumbprint
Active	8/30/2026, 4:03:21 PM	0120401318F5DC6F084CEFB1E70AD49FA97D276A

**Signing Option** Sign SAML response and assertion  
**Signing Algorithm** SHA-256

4. To have Azure AD send group membership for the user in the SAML token, you must + Add a group claim in the Attributes & Claims section. Send the Security groups, using the source attribute Group ID. Use the word or phrase you selected when configuring Azure AD security groups (such as Cortex Cloud) to create a filter. Customize the name of the group claim as memberOf.



**Group Claims**

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None  
 All groups  
 Security groups  
 Directory roles  
 Groups assigned to the application

**Source attribute \***

Group ID

Emit group name for cloud-only groups ⓘ

Advanced options

Filter groups

**Attribute to match \***

Display name

**Match with \***

Contains

**String \***

Cortex XSOAR

Customize the name of the group claim

**Name (required)**

memberOf

**Namespace (optional)**

Emit groups as role claims ⓘ

Apply regex replace to groups claim content

5. In addition to group membership, verify that there are also claims for:

- Email address
- First Name
- Last Name

#### Task 4. Copy Login URL, Azure ID Identifier, and Attribute Claims

1. In Azure, from the Single sign-on page, in the Set up Cortex Cloud Production section, copy the values for the Login URL and Azure AD Identifier. You need these values to configure the SSO Integration in Cortex Cloud.

**Set up Cortex XSOAR 8 Production**

You'll need to configure the application to link with Azure AD.

Login URL	<a href="https://login.microsoftonline.com/675675258000022525">https://login.microsoftonline.com/675675258000022525</a>
Azure AD Identifier	<a href="https://cortexxsoar.onmicrosoft.com/675675258000022525">https://cortexxsoar.onmicrosoft.com/675675258000022525</a>
Logout URL	<a href="https://login.microsoftonline.com/675675258000022525">https://login.microsoftonline.com/675675258000022525</a>

2. Edit Attributes & Claims and copy the values in the Claim name column. The claim name is case sensitive. You need these values to configure the SSO Integration in Cortex Cloud.



**NOTE:**

The default attributes shown on the main single sign-on page in Azure AD are not the values you need. You must click Edit next to Attributes and Claims to view and copy the actual values.

Required claim		
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]
Additional claims		
Claim name	Type	Value
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	SAML	user.mail
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	SAML	user.givenname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	SAML	user.userprincipalname
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>	SAML	user.surname
memberOf	SAML	user.groups

## Task 5. Download the Certificate

From the SAML Certificates section in Azure AD, Download the Certificate (Base64). You need the contents of this file to configure the Cortex Cloud SSO Integration.

SAML Certificates	
<b>Token signing certificate</b>	<a href="#"></a> Edit
Status	Active
Thumbprint	0120401318F5DC6F084CEFB1E70AD49FA97D276A
Expiration	8/30/2026, 4:03:21 PM
Notification Email	<a href="#">Send notification</a>
App Federation Metadata Url	<a href="https://login.microsoftonline.com/02525600-2525-4025-8225-000000000000">https://login.microsoftonline.com/02525600-2525-4025-8225-000000000000</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

## Task 6. Copy the Source IDs for Azure AD Security Groups

The claim for the membership attribute that is sent to Cortex Cloud uses the Object Id of the group. The Object Id is different from the Azure AD security group name. You can find the Object Id for each of your Azure AD security groups by navigating to Users and groups in Azure AD, clicking on the group name, and viewing the Object id. Create a list of the group names and corresponding Object Ids for every Azure AD security group you want to map to a Cortex Cloud user group.

## Task 7. Configure the Cortex Cloud SSO Integration

1. By default, SSO is disabled in Cortex Cloud.
2. Expand the SSO Integration settings.
3. Use the following table to complete the SSO Integration settings, based on the values you saved from Azure AD.

Azure AD	Cortex Cloud Field
Login URL	IdP SSO URL
Azure AD Identifier	IdP Issuer ID
Contents of the downloaded certificate file.	X.509 Certificate

4. In the IdP Attributes Mapping section, enter the attribute claim names from Azure AD. The names are case sensitive and must match exactly.



**NOTE:**

The attribute claim name must exactly match the value sent by your IdP. In some cases, this may be the full attribute name/namespace, depending on the configuration of our IdP

**IdP Attributes Mapping**

- Email  
[http://\*\*REDACTED\*\*/identity/claims/emailaddress](http://<b>REDACTED</b>/identity/claims/emailaddress)
- Group Membership  
[http://\*\*REDACTED\*\*/identity/claims/memberof](http://<b>REDACTED</b>/identity/claims/memberof)
- First Name  
[http://\*\*REDACTED\*\*/identity/claims/givenname](http://<b>REDACTED</b>/identity/claims/givenname)
- Last Name  
[http://\*\*REDACTED\*\*/identity/claims/surname](http://<b>REDACTED</b>/identity/claims/surname)

5. (Optional) Under Advanced Settings, select the checkboxes for ADFS and Compress encode URL (ADFS). In some circumstances, these fields may be required by your Azure AD configuration.

6. Save your settings.

**Task 8. Map SAML Group Memberships to Cortex Cloud User Groups**

1. Right-click a user group and select Edit Group.
2. In the SAML Group Mapping field add the Azure AD group(s) Object Ids that should be associated with this user group. Multiple Object Ids should be separated with a comma. The Azure AD group Object Id must match the exact value sent in the token.
3. Save your settings.
4. Repeat for each user group.

**Task 9. Test SSO Login**

1. Go to the Cortex Cloud tenant URL and Sign-In with SSO.

**NOTE:**

When using SAML 2.0, users are required to authenticate by logging in directly at the tenant URL. They cannot log in via Cortex Gateway.

2. After authentication to Azure AD, you are redirected again to the Cortex Cloud tenant.
3. When logged in, validate that you have been assigned the proper roles.

To view your role and any role assigned to a user group you are a member of, click your name in the bottom left-hand corner, and click About.

## 2.2.6 | Cloud service provider (CSP) onboarding

### Abstract

Learn about onboarding your cloud service provider to Cortex Cloud.

Onboard your cloud service provider (CSP) from the Data Source page.

### 2.2.6.1 | Ingest cloud assets

#### Abstract

Explains how to onboard cloud service providers from the Data Source page.

Cortex Cloud provides a unified, normalized asset inventory for cloud assets. This capability provides deeper visibility to all the assets and superior context for incident investigation.

The cloud service provider (CSP) onboarding wizard is designed to facilitate the seamless setup of CSP data into Cortex Cloud. The guided experience requires minimal user input; simply define the scope of your CSP accounts and specify the scan mode. For full control of the CSP setup, you can use the advanced settings. Based on the onboarding settings, Cortex Cloud generates an authentication template to establish trust to the CSP and grant permissions to Cortex Cloud. The template must be executed in the CSP to complete the onboarding process. Execution of the template grants the permissions and includes a component that notifies Cortex Cloud of the execution details and a new cloud instance is created.



#### **NOTE:**

The cloud accounts being onboarded must be owned by the customer performing the onboarding process.

You can leverage your CSP hierarchy and choose whether to onboard individual accounts one at a time or collection of accounts (such as organization in AWS and GCP or management group in Azure). Various options are available for each CSP to allow you to customize your data collection.

Cortex Cloud supports two scan modes:

- **Cloud scan:** (Recommended) The scanning takes place within the Cortex Cloud cloud environment. No additional setup is needed.
- **Outpost scan:** The scanning is performed on infrastructure deployed to a CSP account owned by you. The CSP account should be a dedicated account for the outpost, free from other resources. Each CSP account can host only one outpost. This mode requires additional cloud provider permissions and may incur additional cloud costs.

To allow you to fine tune your CSP data collection, you can modify the scope of data collection by including or excluding specific regions. If you selected to collect data from an organizational unit that is not the lowest on the CSP hierarchy (such as organization or organizational unit in AWS, organization or folder in GCP, and tenant or management group in Azure), you can also modify the scope by including or excluding specific accounts, projects, or subscriptions. If you choose to include specific accounts, only those specified accounts will be included, even if additional accounts are added to the CSP after onboarding. If you choose to exclude specific accounts, any new accounts added to the CSP after onboarding will be included in the scope. Excluded accounts are not visible in Cortex Cloud.

The advanced settings allow you to select which Cortex Cloud modules you want to enable for this CSP. By default, the following security capabilities are enabled:

- Discovery engine
- Cloud security posture management
- Cloud infrastructure entitlement management
- Agentless disk scanning
- AI security posture management

The additional security capabilities you can enable include:

- XSIAM analytics: Analyzes your endpoint data to develop a baseline and raise Analytics and Analytics BIOC alerts when anomalies and malicious behaviors are detected.
- Data security posture management: An agentless multi-cloud data security solution that discovers, classifies, protects, and governs sensitive data.
- Registry scanning: Scan container registry images for vulnerabilities, malware, and secrets. You can configure your initial preference for scanning your registry. Any newly discovered registry, repository or image in the account will be scanned by default.

#### **2.2.6.2 | Onboard Amazon Web Services**

Abstract

Follow the AWS onboarding wizard and Cortex Cloud creates a custom CloudFormation authentication template to be deployed in AWS CloudFormation.

Follow this wizard to onboard your Amazon Web Services (AWS) environment. The AWS onboarding wizard is designed to facilitate the seamless setup of AWS data into Cortex Cloud. The guided experience requires minimal user input; simply define the scope of your AWS accounts and specify the scan mode. For full control of the setup, you can use the advanced settings. Based on the onboarding settings, Cortex Cloud generates a CloudFormation authentication template to establish trust with AWS and grant permissions to Cortex Cloud. The template must be executed in AWS CloudFormation to complete the onboarding process. Execution of the template grants the permissions and includes a component that notifies Cortex Cloud of the execution details, and a new cloud instance is created.

#### **PREREQUISITE:**

- Ensure you have access to AWS Management Console.
- Ensure you have the Required AWS permissions.

To onboard AWS:

1. Select Settings → Data Sources & Integrations.
2. On the Data Sources & Integrations page, click + Add New.
3. On the Add Data Sources or Integrations page, search for Amazon Web Services (AWS), then hover over it and click Add.
4. In the AWS onboarding wizard, select the type of AWS environment:



- **Government:** AWS GovCloud environments for compatibility with FedRAMP-certified tenants.
- **Commercial:** (Default) Standard cloud deployment typically used for private and public sector organizations that do not require isolated government-specific infrastructure.

5. Select the scope for this data source:

- **Organization:** (Default) A collection of AWS accounts that are managed centrally.
- **Organizational Unit:** A group of AWS accounts within an organization. An organizational unit can also contain other organizational units.
- **Account:** A specific AWS member account.

6. Choose the Scan Mode:

- **Cloud Scan:** (Recommended) Security scanning is performed in the Cortex Cloud cloud environment.
- **Scan with Outpost:** Security scanning is performed on infrastructure deployed to a cloud account owned by you. If you select this option, choose the outpost account to use for this instance.

**NOTE:**

Scanning with an outpost may require additional CSP permissions and may incur additional CSP costs.

7. (Optional) Click Show advanced settings to define advanced settings:



- **Instance Name:** Enter a unique instance name or leave it empty to be automatically populated. The automatic naming convention is the CSP name followed by the ID of the scope unit selected in the onboarding wizard. For example, when onboarding an Amazon Web Services account, the automatic name would be `AWS-<accountID>` where `<accountID>` is the ID of the account onboarded.
- **Scope Modifications:** Use these settings to fine-tune your AWS scope, you can modify the scope by including or excluding specific regions. If you selected a Government environment, only AWS GovCloud regions are displayed. Additionally, if you selected an organization or organizational unit as the scope, you can modify the scope by including or excluding specific accounts. If you choose to include specific accounts, only those specified accounts will be included, even if additional accounts are added to your AWS environment after onboarding. If you choose to exclude specific accounts, any new accounts added to your AWS environment after onboarding will be included in the scope.

**NOTE:**

When onboarding an AWS organization or organizational unit (OU), Cortex Cloud creates IAM resources in every account within that organization or OU. This occurs even if you choose to exclude specific accounts from being scanned. While excluded accounts will not be scanned and will not appear in the asset inventory, the IAM resources may still be present.

- **Additional Security Capabilities:** Choose which security capabilities you want to benefit from. Some security capabilities are enabled by default and can be modified. Adding security capability typically requires additional cloud provider permissions. For detailed information on the permissions required, see Cloud service provider permissions. The additional security capabilities you can enable include:

- **XSIAM analytics:** Analyzes your endpoint data to develop a baseline and raise Analytics and Analytics BIOC alerts when anomalies and malicious behaviors are detected.
- **Data security posture management:** An agentless data security scanner that discovers, classifies, protects, and governs sensitive data. DSPM is not currently available in AWS GovCloud environments.
- **Registry scanning:** A container registry scanner that scans registry images for vulnerabilities, malware, and secrets. For more details, see Configure registry scanning for cloud accounts
- **Serverless functions scanning:** Implement serverless scanning to detect and remediate vulnerabilities within serverless functions during the development lifecycle. Seamless integration into CI/CD pipelines enables automated security scans for a continuously secure pre-production environment.

See Required AWS permissions for Cortex Cloud onboarding for the specific permissions you need to grant in your AWS account for scanning outposts and accessing logs.

- **Automation:** Use automation to pre-configure a list of integrations and associated commands to automate security issue responses. Commands can be utilized individually or as part of custom playbooks for issue remediation.

- **Log Level:** (Optional - for Automation only) Configure the automation integration logging level. Possible values are:

- Off (Default)
- Debug
- Verbose

- **Agentless disk scanning:** (Recommended) Implement agentless disk scanning to remotely detect and remediate vulnerabilities during the development lifecycle.

- **Cloud Tags:** Define tags and tag values to be added to any new resource created by Cortex Cloud in the cloud environment. Note: The `managed_by = paloaltonetworks` tag is automatically added to all resources. This tag is mandatory. You cannot edit or remove this tag.
- **Log Collection Configuration:** To maximize security coverage, include the collection of audit logs using CloudTrail. This may require additional cloud service provider permissions. For detailed information on the permissions required, see Log Collection. Select the collection method:

- **Automated collection:** Have Cortex Cloud collect audit logs using AWS resources in your AWS environment. You can also choose to Collect data events.

**Note:** For the purpose of collecting audit logs, Cortex Cloud automatically provisions dedicated AWS resources in your AWS environment, specifically an AWS CloudTrail trail, an Amazon SQS queue, and an Amazon S3 bucket. As a result, you may incur increased AWS costs, primarily due to CloudTrail event logging. While the trail defaults to capturing both read and write management events, the majority of these costs are typically associated specifically with read management events.

To help manage these costs, you may manually modify the trail (`cortex-trail-<aws_account_id>`) configuration in the AWS Management Console to disable read events. While this reduces detection coverage, it should significantly lower CloudTrail-related charges. It is important to note that these manual changes will be overwritten during future Cortex Cloud updates, but they can serve as a temporary measure for cost control.

- **Custom (user defined):** Select this option if you want to use an existing Amazon S3 bucket for storing your CloudTrail logs. When you select this option, you will need to enter the following details when manually executing the CloudFormation authentication template in CloudFormation: CloudTrail bucket name, CloudTrail SNS ARN, and if relevant, the CloudTrail KMS ARN.

You must ensure that the KMS key region and the SNS topic region are the exact same as the AWS region where you are deploying the CloudFormation stack.

8. Click Save. Cortex Cloud creates an instance in the pending state.



9. To complete the process, deploy the CloudFormation authentication template in AWS CloudFormation using one of the following methods:

- **Automated:** (Recommended) Click Execute in AWS to connect to AWS CloudFormation and create the stack. If you select Automated, you must already be logged in to AWS CloudFormation.
- **Manual:** Click Download CloudFormation to download the CloudFormation authentication template file.

The CloudFormation authentication template is reusable and can be executed as many times as you want to create new cloud instances with the settings you defined in the onboarding wizard.

10. Click Close.

Cortex Cloud generates a CloudFormation authentication template based on the settings you configured in the AWS onboarding wizard.

**Next step:** Follow the instructions to deploy the CloudFormation authentication template in AWS CloudFormation to create a stack.

Required AWS permissions for Cortex Cloud onboarding

Use the following template to create a dedicated role with the permissions required for onboarding AWS to Cortex Cloud:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CortexCloudOnboarding",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:UpdateRoleDescription",
        "iam:DeletePolicy",
        "iam>ListRoles",
        "iam>CreateRole",
        "iam>DeleteRole",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam>CreatePolicy",
        "iam:PassRole",
        "iam>CreateServiceLinkedRole",
        "iam:DetachRolePolicy",
        "iam>ListPolicyVersions",
        "iam>DeleteRolePolicy",
        "iam:UpdateRole",
        "iam>DeleteServiceLinkedRole",
        "iam>ListRolePolicies",
        "iam:GetRolePolicy",
        "iam>DeletePolicyVersion",
        "iam:SetDefaultPolicyVersion",
        "lambda:*",
        "kms:*",
        "s3:*",
        "sns:*",
        "cloudtrail:*",
        "cloudformation:/*"
      ],
      "Resource": "*"
    }
  ]
}
```

To enable serverless function scanning, grant the following permissions in your AWS account for scanning outposts and accessing logs:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:GetLayerVersion",
        "iam:GetRole"
      ],
      "Resource": "*"
    }
  ]
}
```

#### 2.2.6.2.1 | Manually upload template to AWS

Abstract

Learn how to manually create a stack in AWS Management Console using the CloudFormation file downloaded in the onboarding wizard.



When you have downloaded the CloudFormation template file in the onboarding wizard, you must connect to AWS Management Console to create a stack using the template file.

#### **PREREQUISITE:**

Before you begin, ensure you have:

- An AWS account
- Access to AWS Management Console
- Permission to create a stack and its resources in AWS CloudFormation

1. In AWS Management Console, navigate to CloudFormation.
2. On the Stacks page, click Create stack, and then select With new resources (standard).
3. On the Create stack page, in Prerequisite - Prepare template, select Choose an existing template.
4. In Specify template, select Upload a template file, then click Choose file and upload the template downloaded from your Cortex Platform. Click Next.
5. In the Specify stack details page, enter a Stack name.
6. In Parameters, enter a unique Amazon Resource Name (ARN) for the custom CortexPlatformRole role, and an ExternalID.
7. If you have enabled custom log collection, enter the following details:
  - CloudTrailKmsArn: (Optional) The ARN of the AWS KMS key used to encrypt the CloudTrail log files.
  - CloudTrailLogBucket: The name of the Amazon S3 bucket where CloudTrail stores the log files.
  - CloudTrailSnsArn: The ARN of the Amazon SNS topic that CloudTrail uses to send notifications when new log files are delivered.

#### **NOTE:**

You must ensure that the KMS key region and the SNS topic region are the exact same as the AWS region where you are deploying the CloudFormation stack.

Click Next and Next again.

8. In Review, acknowledge that CloudFormation might create IAM resources with custom names and click Submit. The stack is complete when it appears in the Stacks list with status of CREATE\_COMPLETE.

When the template is successfully uploaded to AWS and the stack creation is complete, the initial discovery scan is started. When the scan is complete, you can view the discovered assets in Asset Inventory.

#### 2.2.6.2.1 Configure AWS integration instances and monitor integration instance health

##### Abstract

Enable automations from Data Sources & Integrations and monitor AWS integration instance health.

You can streamline and simplify configuring AWS integration instances within the Data Sources & Integrations page. This includes granting the necessary permissions for the platform to execute commands, scripts, and playbooks as part of issue response. All automation permissions are added to the Terraform as part of the setup process.

Configure a new or existing AWS integration instance

#### **NOTE:**

If you have not yet onboarded your cloud integration, see [Ingest cloud assets](#).

You can configure a new AWS integration instance or edit an existing AWS integration instance, for example to enable automations.

1. Navigate to Settings â Data Sources & Integrations.
2. Select the AWS integration row.
  - To configure a new AWS integration instance: Click Add Instance.
  - To edit an existing AWS integration instance:
3. (Optional) Under Show advanced settings, select Automation and select a log level for the automation integration logs.
4. If the instance is not enabled, in the row for the AWS integration instance, right-click and select Enable. Alternatively, click the more options icon and select Enable.
5. Manually upload the template (Terraform) to the relevant cloud provider.

An automation integration instance with the same name as the cloud integration instance is automatically created and automation permissions are automatically updated in the system. For more information, see [Ingest cloud assets](#).



## Monitor AWS integration instance health

Monitoring AWS integration instance health ensures continuous, reliable operation, facilitating issue response and improving overall security posture.

1. Navigate to Settings â Data Sources & Integrations.
2. In the AWS integration instance row, click the View Details link and then click a specific Instance Name.

From the list of health statuses, you can click the following to see automation instance health status:

- Permissions: Shows any permission issues or missing permissions for the instance.
- Automation: Indicates any errors during automation instance creation or configuration.

### **NOTE:**

Currently, automation permission errors or missing automation permissions do not affect the Automation health status. You can view any permission errors or missing permissions in the the Permissions health status.

## 2.2.6.3 | Onboard Google Cloud Platform

### Abstract

Follow the GCP onboarding wizard, and Cortex Cloud creates a custom authentication template to be applied in GCP.

Follow this wizard to onboard your Google Cloud Platform (GCP) environment. The GCP onboarding wizard is designed to facilitate the seamless setup of GCP data into Cortex Cloud. The guided experience requires minimal user input; simply define the scope of your GCP accounts and specify the scan mode. For full control of the setup, you can use the advanced settings. Based on the onboarding settings, Cortex Cloud generates an authentication template to establish trust to GCP and grant permissions to Cortex Cloud. The template must be applied in GCP to complete the onboarding process. Application of the template grants the permissions and includes a component that notifies Cortex Cloud of the execution details, and a new cloud instance is created.

### **PREREQUISITE:**

- Ensure you have access to Google Cloud Console.
- Ensure you have an admin user with the required admin GCP permissions.
- Ensure you have the following APIs in the GCP project you are onboarding:
  - Cloud Resource Manager API
  - Identity and Access Management (IAM) API
  - Cloud Pub/Sub API (if audit logs are enabled)
  - If you plan on enabling Automation as an additional security capability, enable the following APIs:
    - Kubernetes Engine API
    - Compute Engine API
    - Service Usage API
    - Cloud Storage API

To onboard GCP:

1. Select Settings â Data Sources & Integrations.
2. On the Data Sources & Integrations page, click + Add New.
3. On the Add Data Sources or Integrations page, search for Google Cloud Platform (GCP), then hover over it and click Add.
4. In the GCP onboarding wizard, choose the scope for this data source:
  - Organization: (Default) A collection of GCP projects that are managed centrally.
  - Folder: A GCP folder can contain projects, folders, or a combination of both projects and folders.
  - Project: A specific GCP project.
5. Choose the Scan Mode:
  - Cloud Scan: (Recommended) Security scanning is performed in the Cortex Cloud cloud environment.
  - Scan with Outpost: Security scanning is performed on infrastructure deployed to a cloud account owned by you. If you select this option, choose the outpost account to use for this instance.

### **NOTE:**

Scanning with an outpost may require additional CSP permissions and may incur additional CSP costs.



6. If you selected Organization or Project as the scope, enter its ID.

7. (Optional) Click Show advanced settings to define advanced settings:

- **Instance Name:** Enter a unique instance name or leave it empty to be automatically populated. The automatic naming convention is the CSP name followed by the ID of the scope unit selected in the onboarding wizard. For example, when onboarding a Google Cloud Platform project, the automatic name would be GCP-<projectId> where <projectId> is the ID of the project onboarded.
- **Scope Modifications:** To allow you to fine-tune your GCP data collection, you can modify the scope by including or excluding specific regions. Additionally, if you selected an organization or folder as the scope, you can modify the scope by including or excluding specific projects. If you choose to include specific projects, only those specified projects will be included, even if additional projects are added to your GCP environment after onboarding. If you choose to exclude specific projects, any new projects added to your GCP environment after onboarding will be included in the scope. Excluded projects are not visible in Cortex Cloud.
- **Additional Security Capabilities:** Enable additional Cortex security add-ons, if available. This may require additional cloud provider permissions. For detailed information on the permissions required, see Cloud service provider permissions. The additional security capabilities you can enable include:
  - **XSIAM analytics:** Analyzes your endpoint data to develop a baseline and raise Analytics and Analytics BIOC alerts when anomalies and malicious behaviors are detected.
  - **Data security posture management:** An agentless multi-cloud data security solution that discovers, classifies, protects, and governs sensitive data.
  - **Registry scanning:** Scan container registry images for vulnerabilities, malware, and secrets. You can configure your initial preference for scanning your registry. Any newly discovered registry, repository, or image in the account will be scanned by default. For more details, see Configure registry scanning for cloud accounts
  - **Serverless functions scanning (Gen 1 only):** Implement serverless scanning to detect and remediate vulnerabilities within serverless functions during the development lifecycle. Seamless integration into CI/CD pipelines enables automated security scans for a continuously secure pre-production environment.
  - **Automation:** Use automation to pre-configure a list of integrations and associated commands to automate security issue responses. Commands can be utilized individually or as part of custom playbooks for issue remediation.
  - **Agentless disk scanning:** (Recommended) Implement agentless disk scanning to remotely detect and remediate vulnerabilities during the development lifecycle.
- **Log Level:** (Optional - for Automation only) Configure the automation integration logging level. Possible values are:
  - Off (Default)
  - Debug
  - Verbose
- **Cloud Tags:** Define tags and tag values to be added to any new resource created by Cortex Cloud in the cloud environment. Note: The `managed_by = paloaltonetworks` tag is automatically added to all resources. This tag is mandatory. You cannot edit or remove this tag.
- **Log Collection Configuration:** To maximize security coverage, include collection of audit logs (GCP Pub/Sub). This may require additional cloud service provider permissions. For detailed information on the permissions required, see Cloud service provider permissions.
- **Connect to GCP Workspace:** Gain a comprehensive view of your Google Workspace identities and security. This provides you with detailed information on your users, groups, and organizational units, and collects security event logs to help you detect threats, improve your security posture, and meet compliance requirements.

#### **NOTE:**

If you want to connect to your GCP Workspace, you must first complete onboarding with the option disabled. Once the GCP cloud instance is created, perform the steps detailed in Connect Google Workspace with your GCP cloud instance.

8. Click Save.

9. Download the template file by clicking Download Terraform and then click Close.

The Terraform authentication template is reusable and can be applied as many times as you want to create new instances with the settings you defined in the GCP onboarding wizard. The Terraform authentication template is valid for seven days from when it was created.

Cortex Cloud generates a Terraform authentication template based on the settings you configured in the GCP onboarding wizard.

**Next step:** Apply the Terraform authentication template in GCP.

Required admin GCP permissions for Cortex Cloud onboarding

Use the following template to create a dedicated role with the permissions required for onboarding GCP to Cortex Cloud.

```
{  
  "title": "CortexCloudOnboarding",  
  "permissions": [
```



```

"description": "Custom role with permissions required for onboarding Cortex Cloud",
"stage": "GA",
"includedPermissions": [
  "iam.roles.create",
  "iam.roles.delete",
  "iam.roles.get",
  "iam.roles.list",
  "iam.roles.update",
  "iam.serviceAccounts.create",
  "iam.serviceAccounts.delete",
  "iam.serviceAccounts.get",
  "iam.serviceAccounts.getIamPolicy",
  "iam.serviceAccounts.list",
  "iam.serviceAccounts.setIamPolicy",
  "iam.serviceAccounts.update",
  "logging.sinks.create",
  "logging.sinks.delete",
  "logging.sinks.get",
  "logging.sinks.update",
  "pubsub.subscriptions.create",
  "pubsub.subscriptions.delete",
  "pubsub.subscriptions.getIamPolicy",
  "pubsub.subscriptions.setIamPolicy",
  "pubsub.subscriptions.update",
  "pubsub.topics.create",
  "pubsub.topics.delete",
  "pubsub.topics.getIamPolicy",
  "pubsub.topics.setIamPolicy",
  "pubsub.topics.update",
  "resourcemanager.folders.get",
  "resourcemanager.folders.getIamPolicy",
  "resourcemanager.folders.list",
  "resourcemanager.folders.setIamPolicy",
  "resourcemanager.organizations.get",
  "resourcemanager.organizations.getIamPolicy",
  "resourcemanager.organizations.setIamPolicy",
  "resourcemanager.projects.get",
  "resourcemanager.projects.getIamPolicy",
  "resourcemanager.projects.list",
  "resourcemanager.projects.setIamPolicy"
]
}

```

#### 2.2.6.3.1 | Manually upload template to GCP

##### Abstract

Learn how to manually deploy the Terraform template file in Google Cloud Console.

When you have downloaded the Terraform template file in the onboarding wizard, you must connect to Google Cloud Console to create a stack using the template file.

##### **PREREQUISITE:**

Before you begin, ensure you have:

- A GCP account.
- Permission to create the required resources in Google Cloud Deployment Manager.
- Installed Terraform on your local machine. You can download Terraform from the official Terraform website and follow the installation instructions for your operating system.
- Installed the GCP gcloud CLI tool.
- Reviewed the introduction to Terraform for Cloud service provider (CSP) onboarding to understand the underlying logic of how Terraform interacts with your cloud environment.

1. Open your local terminal (Command prompt, PowerShell, or Terminal).

2. Log in to your GCP account using the gcloud CLI:

```
gcloud auth login
```

3. Create a directory on your local machine to store and run the Terraform code. If you have more than one GCP connector, you need a separate directory for each one:

##### **NOTE:**

The directory you create must be a subdirectory of the home directory.

```
mkdir -p ~/terraform/gcp-connector-1
```

4. Navigate to the directory you created and extract the Terraform files. Ensure all necessary Terraform files are present (`main.tf`, `template_params.tfvars`, etc).

##### **IMPORTANT:**

You must not delete or move the Terraform files from this folder. It will prevent you from being able to edit your cloud instance in the future.



```
cd ~/terraform/gcp-connector-1  
tar -xzvf <your_template>.tar.gz
```

5. Initialize Terraform in your project directory:

```
terraform init
```

6. Apply your Terraform configuration using the downloaded parameter file. When prompted, enter the project ID if you configured one in the onboarding wizard:

```
terraform apply --var-file=template_params.tfvars
```

The Terraform template is deployed.

When the template is successfully uploaded to GCP, the initial discovery scan is started. When the scan is complete, you can view your cloud assets in Asset Inventory.

#### 2.2.6.3.2 | Connect Google Workspace with your GCP cloud instance

To gain full visibility into GCP permissions and identity relationships, highlight risks, and offer proper remediation, Cortex Cloud must ingest user, group, and group membership data from your Google Workspace. You need to create a custom role in Google Workspace, assign it specific privileges, and then assign your Cortex Cloud service account to this newly created role.

##### **PREREQUISITE:**

Ensure you have the Super Admin role in Google Workspace.

1. Create a Cortex Cloud role in Google Workspace

1. Log in to your Google Admin Console.
2. In the left menu, select Account → Admin roles.
3. Click Create new role.
4. In the Role info page, enter a name for the role, such as **cortex-cloud-security-role**.
5. (Optional) Enter a description.
6. Click Continue.

7. In the Select Privileges page, in the Privilege Name list, under Admin API, select the following privileges:

- Organization Units > Read (This automatically selects the Organizational Units > Read permission. Leave it selected.)
- Users > Read
- Groups > Read

8. Click Continue and then click Create Role.

2. Assign the Cortex Cloud service account to the created role

1. In Cortex Cloud, navigate to Settings → Data Sources & Integrations and select Google Cloud Platform (GCP) → View details.
2. Identify the GCP cloud instance and click the instance name to open the details pane for that instance.
3. In the details pane, click the more options icon at the top right corner and then select Authorization Details.
4. Copy the value of Cortex discovery role.
5. Log in to your Google Admin Console.
6. In the left menu, select Account → Admin roles.
7. Select the role created previously and click Assign role.
8. Click Assign service accounts and paste the value of the Cortex discovery role. Click Add.
9. Click Assign role.

Your Cortex Cloud service account has been successfully granted the necessary permissions in Google Workspace to ingest user, group, and group membership data. It may take several hours for the results to appear in Cortex Cloud, depending on the size of your cloud estate.

3. Enable Google Workspace in your GCP cloud instance

##### **PREREQUISITE:**



- Ensure you have the organization ID of the Google Workspace you want to connect:
  - Log in to your Google Admin Console, and navigate to Account → Account settings → Profile. Next to Customer ID is your organization ID.
- Ensure the organization ID you want to connect meets one of the following requirements:
  - It must already be defined within your Domain Restricted Principles policy.
  - It is the Workspace organization ID to which the GCP organization you have onboarded in this cloud instance belongs.

1. In Cortex Cloud, navigate to Settings → Data Sources & Integrations and select Google Cloud Platform (GCP) → View details.
2. Identify the GCP cloud instance and click Configuration at the right end of the cloud instance row.
3. In the Google Cloud Provider (GCP) onboarding wizard, click Show advanced settings.
4. Under Discovery Enhancements, select Connect to GCP Workspace.
5. Enter the organization ID of your Google Workspace. You can enter more than one organization ID.
6. Click Save.

You have successfully enabled the Google Workspace in your GCP cloud instance.

#### 2.2.6.3.1 | Configure GCP integration instances and monitor integration instance health

##### Abstract

Enable automations from Data Sources & Integrations and monitor GCP integration instance health.

You can streamline and simplify configuring GCP integration instances within the Data Sources & Integrations page. This includes granting the necessary permissions for the platform to execute commands, scripts, and playbooks as part of issue response. All automation permissions are added to the Terraform as part of the setup process.

Configure a new or existing GCP integration instance

##### **NOTE:**

If you have not yet onboarded your cloud integration, see Ingest cloud assets.

You can configure a new GCP integration instance or edit an existing GCP integration instance, for example to enable automations.

1. Navigate to Settings → Data Sources & Integrations.
2. In the GCP integration row:
  - To configure a new GCP integration instance: Click  and then click Add New Instance or click View Details and from the New Instance dropdown select the GCP cloud service provider.
  - To edit an existing GCP integration instance: Click View Details and then click the configuration pencil icon.
3. (Optional) Under Show advanced settings, select Automation and select a log level for the automation integration logs.
4. If the instance is not enabled, in the row for the GCP integration instance, right-click and select Enable. Alternatively, click the more options icon and select Enable.
5. Manually upload the template (Terraform) to the relevant cloud provider.

An automation integration instance with the same name as the cloud integration instance is automatically created and automation permissions are automatically updated in the system. For more information, see Ingest cloud assets.

##### Monitor GCP integration instance health

Monitoring GCP integration instance health ensures continuous, reliable operation, facilitating issue response and improving overall security posture.

1. Navigate to Settings → Data Sources & Integrations.
2. In the GCP integration instance row, click the View Details link and then click a specific Instance Name.

From the list of health statuses, you can click the following to see automation instance health status:

- Permissions: Shows any permission issues or missing permissions for the instance.
- Automation: Indicates any errors during automation instance creation or configuration.

##### **NOTE:**

Currently, automation permission errors or missing automation permissions do not affect the Automation health status. You can view any permission errors or missing permissions in the the Permissions health status.



## Abstract

Learn how to grant authorization to Cortex Cloud to scan within your GCP service perimeter.

A service perimeter can provide an additional layer of security for your GCP projects. It serves as a fortified boundary around your Google Cloud resources. While resources inside the perimeter can communicate freely, the perimeter is designed to prevent unauthorized communication to Google Cloud services beyond its confines.

To enable Cortex Cloud to scan assets and resources within your GCP perimeter, you must authorize Cortex Cloud's identities to access the perimeter from within GCP. If you have a perimeter set up in your GCP project and you have not authorized Cortex Cloud's identities to scan the perimeter, you will receive the following error:

```
Request is prohibited by organization's policy. vpcServiceControlsUniqueIdentifier: {{<GCP-perimeter-ID>}}
```

### **NOTE:**

Each GCP cloud instance is assigned a scope within GCP. If the scope, whether it be organization, folder, or project, includes any projects with a service perimeter, this procedure must be performed for that cloud instance to authorize Cortex Cloud to scan the resources in the perimeter.

#### Obtain Cortex Cloud identity details

1. In your Cortex Cloud tenant, select Settings â Data Sources & Integrations.
2. Hover over the Google Cloud Platform (GCP) row and select View Details.
3. In the Cloud Instances page, identify the GCP instance with the perimeter, right-click it and select Details.
4. In the details pane, click the more options icon and select Authorization Details.
5. The authorization values that you need to add as approved identities in GCP are listed in the Authorization Details dialog box.

#### Add Cortex Cloud authorization values to GCP perimeter

1. Log into Google Cloud Platform Console.
2. Navigate to VPC Service Controls.
3. In the list of perimeters, select the perimeter to which you want to grant access to Cortex Cloud.
4. In the Service perimeter details screen, click Edit.
5. In the Edit service perimeter screen, select Ingress policy.
6. In the Ingress rules pane, click Add an ingress rule.
7. Enter a Title for the ingress rule.
8. In the From section, under Identities, select Select identities & groups.
9. Click Add identities. In the Add identities pane, under Search identities, paste Cortex discovery role from Cortex Cloud's Authorization Details dialog box. If there are more authorized values, paste each of them under Search identities. Click Add identities.
10. In the To section, under Resources, select Select projects.
11. Click Add projects. In the Add projects pane, select the relevant projects.
12. Under Operations or IAM roles, select All operations.
13. Click Next to add an egress rule.
14. In the Egress rules pane, click Add an egress rule.
15. Enter a Title for the egress rule.
16. In the From section, under Identities, select Select identities & groups.
17. Click Add identities. In the Add identities pane, under Search identities, paste Cortex discovery role from Cortex Cloud's Authorization Details dialog box. If there are more authorized values, paste each of them under Search identities. Click Add identities.
18. In the To section, under Resources, select Select projects.
19. Click Add projects. In the Add projects pane, select the relevant projects.
20. Click Save. Confirm the changes and click Confirm.

The Cortex Cloud authorization values have been added as approved identities in GCP.



## Abstract

Follow the Azure onboarding wizard, and Cortex creates a custom authentication template to be executed in Azure.

Follow this wizard to onboard your Microsoft Azure environment. The Microsoft Azure onboarding wizard is designed to facilitate the seamless setup of Microsoft Azure data into Cortex Cloud. The guided experience requires minimal user input; simply define the scope of your Microsoft Azure accounts and specify the scan mode. For full control of the setup, you can use the advanced settings. Based on the onboarding settings, Cortex Cloud generates an authentication template to establish trust with Microsoft Azure and grant permissions to Cortex Cloud. The template must be applied to complete the onboarding process. Application of the authentication template grants the permissions and includes a component that notifies Cortex Cloud of the execution details, and a new cloud instance is created.

Microsoft Azure private resources are not currently discoverable.

### **PREREQUISITE:**

- Ensure you have a Microsoft Azure subscription.
- Ensure you have the admin permissions required to onboard Microsoft Azure or the built-in Security Administrator role.
- Obtain the tenant ID and subscription ID. You can view these in the Microsoft Azure Portal in Management groups.

How to onboard Azure:

1. Select Settings → Data Sources & Integrations.
2. On the Data Sources & Integrations page, click + Add New.
3. On the Add Data Sources or Integrations page, search for Microsoft Azure, then hover over it and click Add.
4. In the onboarding wizard, select the type of Microsoft Azure environment:
  - **Government:** Microsoft Azure Government environments for compatibility with FedRAMP-certified tenants.
  - **Commercial:** (Default) Standard cloud deployment typically used for private and public sector organizations that do not require isolated government-specific infrastructure.
5. Select the scope for this data source.
  - **Tenant:** (Default) A specific instance of Azure Active Directory, which can contain several subscriptions.
  - **Management Group:** A collection of Microsoft Azure subscriptions.
  - **Subscription:** A collection of Microsoft Azure resources associated with a specific Microsoft Azure tenant.
6. Choose the Scan Mode:
  - **Cloud Scan:** (Recommended) Security scanning is performed in the Cortex Cloud cloud environment.
  - **Scan with Outpost:** Security scanning is performed on infrastructure deployed to a cloud account owned by you. If you select this option, choose the outpost account to use for this instance or create a new outpost. For more information on outposts, see Outposts.

Scanning with an outpost may require additional CSP permissions and may incur additional CSP costs.
7. Select an approved tenant ID from the Tenant ID list. If no tenant IDs have been approved, enter the tenant ID. Click Approve in Azure to add Cortex Cloud as an approved application on this tenant. When the tenant ID is approved, it appears with a green check next to it.
8. (Optional) Click Show advanced settings to define advanced settings:



- **Instance Name:** Enter a unique instance name or leave it empty to be automatically populated. The automatic naming convention is the CSP name followed by the ID of the scope unit selected in the onboarding wizard. For example, when onboarding an Azure tenant, the automatic name would be `AZURE-<tenantID>` where `<tenantID>` is the ID of the tenant onboarded.
- **Scope Modifications:** To fine-tune your Microsoft Azure data collection, you can modify the scope by including or excluding specific regions. If you selected a Government environment, only Microsoft Azure Government regions are displayed. Additionally, if you selected a tenant or management group as the scope, you can modify the scope by including or excluding specific subscriptions. If you choose to include specific subscriptions, only those specified subscriptions will be included, even if additional subscriptions are added to your Microsoft Azure environment after onboarding. If you choose to exclude specific subscriptions, any new subscriptions added to your Microsoft Azure environment after onboarding will be included in the scope. Excluded subscriptions are not visible in Cortex Cloud.
- **Additional Security Capabilities:** Choose which security capabilities you want to benefit from. Some security capabilities are enabled by default and can be modified. Adding security capability typically requires additional cloud provider permissions. For detailed information on the permissions required, see Cloud service provider permissions. The additional security capabilities you can enable include:
  - **XSIAM analytics:** Analyzes your endpoint data to develop a baseline and raise Analytics and Analytics BIOC alerts when anomalies and malicious behaviors are detected.
  - **Data security posture management:** An agentless multi-cloud data security solution that discovers, classifies, protects, and governs sensitive data. DSPM is not currently available in Microsoft Azure Government environments.
  - **Registry scanning:** Scan container registry images for vulnerabilities, malware, and secrets. You can configure your initial preference for scanning your registry. Any newly discovered registry, repository or image in the account will be scanned by default. For more details, see Configure registry scanning for cloud accounts
  - **Serverless functions scanning:** Implement serverless scanning to detect and remediate vulnerabilities within serverless functions during the development lifecycle. Seamless integration into CI/CD pipelines enables automated security scans for a continuously secure pre-production environment.
  - **Automation:** Use automation to pre-configure a list of integrations and associated commands to automate security issue responses. Commands can be utilized individually or as part of custom playbooks for issue remediation.
    - **Log Level:** (Optional - for Automation only) Configure the automation integration logging level. Possible values are:
      - Off (Default)
      - Debug
      - Verbose
  - **Agentless disk scanning:** (Recommended) Implement agentless disk scanning to remotely detect and remediate vulnerabilities during the development lifecycle.
- **Cloud Tags:** Define tags and tag values to be added to any new resource created by Cortex Cloud in the cloud environment. Note: The `managed_by = paloaltonetworks` tag is automatically added to all resources. This tag is mandatory. You cannot edit or remove this tag.
- **Log Collection Configuration:** To maximize security coverage, include the collection of audit logs (Event Hub). This may require additional cloud service provider permissions. For detailed information on the permissions required, see Cloud service provider permissions.

9. Click Save.

10. To complete the process, download the authentication template:

- For onboarding Azure tenants and management groups, click one of the following:
  - Download Terraform to download a Terraform file and proceed to Finalize onboarding by applying the Terraform template's configuration.  
To onboard all subscriptions within a management group or tenant, our authentication template uses Azure Resource Management (ARM) templates internally. The ARM templates are encoded with base64 and located inside the `template_params.tfvars` file as the `policy_template` variable.
  - Azure Resource Manager to download a `.tar.gz` file and proceed to Finalize onboarding of tenants and management groups by deploying the Microsoft Azure Resource Manager (ARM) template.
- For onboarding Azure subscriptions, click one of the following:
  - Download Terraform to download a Terraform file and proceed to Finalize onboarding by applying the Terraform template's configuration.
  - Azure Resource Manager to download a JSON file and proceed to Finalize onboarding of subscriptions by deploying the Microsoft Azure Resource Manager (ARM) template.

The authentication template is reusable and can be executed as many times as you want to create new cloud instances with the settings you defined in the onboarding wizard.

11. Click Close.

Cortex Cloud generates an authentication template based on the settings you configured in the Microsoft Azure onboarding wizard.



Use the following template to create a dedicated role with the permissions required for onboarding Microsoft Azure to Cortex Cloud.

```
{
  "Name": "CortexCloudOnboarding",
  "IsCustom": true,
  "Description": "Custom role with permissions for Cortex Cloud onboarding",
  "Actions": [
    "Microsoft.Authorization/roleAssignments/delete",
    "Microsoft.Authorization/roleAssignments/read",
    "Microsoft.Authorization/roleAssignments/write",
    "Microsoft.Authorization/roleDefinitions/delete",
    "Microsoft.Authorization/roleDefinitions/read",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleManagementPolicies/read",
    "Microsoft.Authorization/roleManagementPolicies/write",
    "Microsoft.Authorization/roleManagementPolicyAssignments/read",
    "Microsoft.Insights/diagnosticSettings/write",
    "Microsoft.PolicyInsights/remediations/cancel/action",
    "Microsoft.PolicyInsights/remediations/delete",
    "Microsoft.PolicyInsights/remediations/listDeployments/read",
    "Microsoft.PolicyInsights/remediations/read",
    "Microsoft.PolicyInsights/remediations/write",
    "Microsoft.Resources/deploymentScripts/delete",
    "Microsoft.Resources/deploymentScripts/logs/read",
    "Microsoft.Resources/deploymentScripts/read",
    "Microsoft.Resources/deploymentScripts/write",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/exportTemplate/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/deployments/whatIf/action",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/moveResources/action",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourceGroups/validateMoveResources/action",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Resources/subscriptions/resourceGroups/deployments/operations/read",
    "Microsoft.Resources/subscriptions/resourceGroups/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/deployments/read",
    "Microsoft.Resources/subscriptions/resourceGroups/deployments/write",
    "Microsoft.Resources/subscriptions/resourceGroups/resources/read",
    "Microsoft.aadiam/diagnosticsettings/delete",
    "Microsoft.aadiam/diagnosticsettings/read",
    "Microsoft.aadiam/diagnosticsettings/write",
    "microsoft.azureADMetrics/providers/Microsoft.Insights/diagnosticSettings/write",
    "microsoft.aadiam/tenants/providers/Microsoft.Insights/diagnosticSettings/write"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    <SUBSCRIPTION_ID> or <MANAGEMENT_GROUP_ID> or <TENANT_ID>
  ]
}
```

Where <SUBSCRIPTION\_ID>, <MANAGEMENT\_GROUP\_ID>, or <TENANT\_ID> is replaced with the ID of the scope you are onboarding.

#### 2.2.6.4.1 | Finalize Microsoft Azure onboarding by executing the authentication template

##### Abstract

Learn how to execute the authentication template file in Microsoft Azure for subscriptions, tenants, and management groups. We provide instructions both for applying the Terraform template's configuration and for deploying the Microsoft Azure Resource Manager (ARM) template.

While onboarding Microsoft Azure with the onboarding wizard, you have to choose one of the following options for executing an authentication template:  
Download Terraform or Azure Resource Manager.

After running the wizard, you finalize the onboarding by executing the template to provision the resources for subscriptions, management groups, and tenants in your cloud environment.

After the template is successfully executed, the initial discovery scan starts. When the scan completes, view your cloud assets in Asset Inventory.

##### Finalize onboarding by applying the Terraform template's configuration

If you selected the Download Terraform option in the Microsoft Azure onboarding wizard, execute the template with the CLI. You decide, based on your own use case, how you would like to perform the CLI commands, for example, locally or in CloudShell.

#### PREREQUISITE:

Before you begin, ensure you have:



- An Azure subscription.
- A user with the required permissions for the relevant scope (subscription, management group, tenant). We recommend you create a dedicated role.
- Tenant ID and subscription ID. You can view these in Microsoft Azure Portal in Management groups.
- Installed Terraform on your local machine. You can download Terraform from the official Terraform website and follow the installation instructions for your operating system.

**TIP:**

Review the Introduction to Terraform for Cloud service provider (CSP) onboarding to get familiar with how Cortex works with Terraform for cloud onboarding.

- Installed the Azure CLI tool.

1. In your local terminal, log in to your Azure account using the Azure CLI:

```
az login
```

2. Create a directory on your local machine to store and run the Terraform code. If you have more than one Azure connector, you need a separate directory for each one:

```
mkdir -p ~/terraform/azure-connector-1
```

3. Navigate to the directory you created and extract the Terraform files. Ensure all necessary Terraform files are present (`main.tf`, `template_params.tfvars`, and so on).

**IMPORTANT:**

Do not delete or move the Terraform files from this folder. It will prevent you from being able to edit your cloud instance in the future.

```
cd ~/terraform/azure-connector-1
tar -xvf <your_template>.tar.gz.
```

4. Initialize Terraform in your project directory:

```
terraform init
```

5. Apply your Terraform configuration using the downloaded parameter file. When prompted, enter the subscription, management group, or tenant ID:

```
terraform apply --var-file=template_params.tfvars
```

6. When prompted, review the actions the Terraform will perform and approve them by entering `yes`.

The Terraform template is executed.

Finalize onboarding of subscriptions by deploying the Microsoft Azure Resource Manager (ARM) template

If you selected the Azure Resource Manager option in the Microsoft Azure onboarding wizard to onboard subscriptions, deploy the template with the CLI. You decide, based on your use case, how you would like to perform the CLI commands, for example, locally or in CloudShell.

**PREREQUISITE:**

Before you begin, ensure you have:

- An Azure subscription.
- A user with the required permissions for the relevant scope (subscription, management group, tenant). We recommend you create a dedicated role.
- Tenant ID and subscription ID. You can view these in Microsoft Azure Portal in Management groups.
- Installed the Azure CLI tool.
- Authorization to create management group policies.

1. In your local terminal or CloudShell, log in to your Azure account using the Azure CLI:

```
az login
```

2. Deploy the template file.

```
az deployment sub create \
--location <LOCATION> \
--subscription <SUBSCRIPTION_ID> \
--template-file <JSON_TEMPLATE>
```

where:

- `<LOCATION>` is the location of the management group, such as `eastus` or `westus`.
- `<SUBSCRIPTION_ID>` is the ID of the subscription you want to onboard.
- `<JSON_TEMPLATE>` is the JSON template file that you downloaded at the end of the onboarding wizard.

To verify the deployment was successful, check the Azure Portal under the "Deployments" section of the targeted subscription.



If you selected the Azure Resource Manager option in the Microsoft Azure onboarding wizard to onboard tenants or management groups, deploy the template with the CLI using Bash in CloudShell.

#### PREREQUISITE:

Before you begin, ensure you have:

- An Azure subscription.
- A user with the required permissions for the relevant scope (subscription, management group, tenant). We recommend you create a dedicated role.
- Tenant ID and subscription ID. You can view these in Microsoft Azure Portal in Management groups.
- Installed the Azure CLI tool.
- Authorization to create management group policies.

1. To prepare for deployment, execute the following commands in a Bash-compliant terminal, such as the Bash environment in Azure Cloud Shell:

Step	Command
Create a folder on your local machine to store the <code>tar</code> file. If you have more than one Azure connector, you need a separate directory for each one.	<code>mkdir -p ~/azure-connector-1</code>
Navigate to the directory you created and extract the files.	<code>cd ~/azure-connector-1 tar -xzvf &lt;your_template&gt;.tar.gz.</code>

2. Deploy the template file: `bash onboard.sh`

When prompted, enter the following values:

- The Azure region where you want the resources to be created, such as `eastus` or `westus`.
- The ID of the management group or tenant that you want to onboard.
- The ID of the subscription where the deployment script will run.

To verify the deployment was successful, check the Azure Portal under the "Deployments" section of the targeted management group, or tenant.

See also

- Introduction to Terraform for Cloud service provider (CSP) onboarding

#### 2.2.6.4.2 | Configure Azure integration instances and monitor integration instance health

Abstract

Enable automations from Data Sources & Integrations and monitor Azure integration instance health.

You can streamline and simplify configuring Azure integration instances within the Data Sources & Integrations page. This includes granting the necessary permissions for the platform to execute commands, scripts, and playbooks as part of issue response. All automation permissions are added to the Terraform as part of the setup process.

Configure a new or existing Azure integration instance

#### NOTE:

If you have not yet onboarded your cloud integration, see Ingest cloud assets.

You can configure a new Azure integration instance or edit an existing Azure integration instance, for example to enable automations.

1. Navigate to Settings â Data Sources & Integrations.

2. In the Azure integration row:

- To configure a new Azure integration instance: Click  and then click Add New Instance or click View Details and from the New Instance drop down select the Azure cloud service provider.
- To edit an existing Azure integration instance: Click View Details and then click the configuration pencil icon.



3. (Optional) Under Show advanced settings, select Automation and select a log level for the automation integration logs.
4. If the instance is not enabled, in the row for the Azure integration instance, right-click and select Enable. Alternatively, click the more options icon and select Enable.
5. Manually upload the template (Terraform) to the relevant cloud provider.

An automation integration instance with the same name as the cloud integration instance is automatically created and automation permissions are automatically updated in the system. For more information, see Ingest cloud assets.

#### Monitor Azure integration instance health

Monitoring Azure integration instance health ensures continuous, reliable operation, facilitating issue response and improving overall security posture.

1. Navigate to Settings → Data Sources & Integrations.
2. In the Azure integration instance row, click the View Details link and then click a specific Instance Name.

From the list of health statuses, you can click the following to see automation instance health status:

- Permissions: Shows any permission issues or missing permissions for the instance.
- Automation: Indicates any errors during automation instance creation or configuration.

#### **NOTE:**

Currently, automation permission errors or missing automation permissions do not affect the Automation health status. You can view any permission errors or missing permissions in the the Permissions health status.

#### 2.2.6.5 | Onboard Oracle Cloud Infrastructure

##### Abstract

Follow the OCI onboarding wizard, and Cortex Cloud creates a custom authentication template to be applied in OCI.

Follow this wizard to onboard your Oracle Cloud Infrastructure (OCI) environment. The OCI onboarding wizard is designed to facilitate the seamless setup of OCI data into Cortex Cloud. This guided experience requires minimal user input. For full control of the setup, you can use the advanced settings. Based on the onboarding settings, Cortex Cloud generates a Terraform authentication template to establish trust with OCI and grant permissions to Cortex Cloud.

Application of the Terraform authentication template completes the onboarding process. The Terraform authentication template grants the permissions, includes a component that notifies Cortex Cloud of the execution details, and a new cloud instance is created.

#### **PREREQUISITE:**

- Ensure you have access to the Oracle Cloud Infrastructure console
- Permissions for all of the following are required:
  - Creation of identity groups (for more information, refer to Managing Groups)
  - Policies (for more information, refer to How Policies Work)
  - Tag namespaces in the root compartment (for more information, refer to Tags and Tag Namespace Concepts)
- If you enable audit log collection, you must first Configure the OCI connector for log collection. If you want to use bucket replication, see Object Storage Replication.

To onboard OCI:

1. Select Settings → Data Sources & Integrations.
2. On the Data Sources & Integrations page, click + Add New.
3. On the Add Data Sources or Integrations page, search for Oracle Cloud Infrastructure, then hover over it and click Add.
4. (Optional) Enter a unique instance name.

If you don't enter a name, the wizard will apply the default name, `OCI-<TENANCY_OCID>`.

5. (Optional) Click Show advanced settings to define advanced settings:



- Scope Modifications: You can modify the scope by including or excluding specific Compartments. If you choose to include specific compartments, only the specified compartments and their sub-compartments will be included. This setting will affect future sub-compartments added to your OCI environment after onboarding. If you choose to exclude specific compartments, this setting will also affect their sub-compartments.
- Note:** The root compartment is always onboarded, and only the sub-compartment scope can be modified.
- Excluded compartments are not visible in Cortex Cloud.
- Additional Security Capabilities: Enable additional Cortex Cloud security add-ons, if available. This may require additional cloud provider permissions. For detailed information on the permissions required, see Cloud service provider permissions. The additional security capabilities you can enable include:
    - **Data security posture management:** An agentless multi-cloud data security solution that discovers, classifies, protects, and governs sensitive data.
    - **Serverless functions scanning (Gen 1 only):** Implement serverless scanning to detect and remediate vulnerabilities within serverless functions during the development lifecycle. Seamless integration into CI/CD pipelines enables automated security scans for a continuously secure pre-production environment.
    - **Registry scanning:** Scan container registry images for vulnerabilities, malware, and secrets. You can configure your initial preference for scanning your registry. Any newly discovered registry, repository, or image in the account will be scanned by default. For more details, see Configure registry scanning for cloud accounts
    - **Agentless disk scanning:** (Recommended) Implement agentless disk scanning to remotely detect and remediate vulnerabilities during the development lifecycle.
  - **Cloud Tags:** Define tags and tag values to be added to any new resource created by Cortex Cloud in the cloud environment. Note: The `managed_by = paloaltonetworks` tag is automatically added to all resources. This tag is mandatory. You cannot edit or remove this tag.
  - **Log Collection Configuration:** To maximize security coverage, enable the collection of audit logs. This may require additional cloud service provider permissions. For detailed information on the permissions required, see Cloud service provider permissions. Enter the following details for each preexisting OCI storage bucket that you intend to use for log collection:
    - Region: The geographic OCI region where the bucket is located. For example, "us-phoenix-1".
    - Bucket Name: The name of the OCI storage bucket.
    - Compartment OCID: The Oracle Cloud Identifier (OCID) of the compartment that contains the bucket.

6. Click Save.

7. Download the OCI authentication template by clicking Download Terraform.

The Terraform authentication template is reusable and can be executed as many times as you want to create new instances with the settings you defined in the wizard. The Terraform authentication template is valid for seven days from when it was created.

8. Click Close.

Cortex Cloud generates a Terraform authentication template based on the settings you configured in the OCI onboarding wizard.

**Next step:** Apply the Terraform authentication template in OCI.

#### 2.2.6.5.1 | Manually upload template to OCI

**Abstract**

Learn how to manually deploy the Terraform template files in Oracle Cloud Infrastructure (OCI).

When you have downloaded the Terraform template files in the onboarding wizard, you must log in to the Oracle Cloud Infrastructure (OCI) CLI tool to deploy the template file. For more information about the OCI CLI tool, refer Oracle documentation.

#### PREREQUISITE:

Before you begin, ensure you have:

- An Oracle Cloud Infrastructure account and the tenancy OCID.
- Permission to deploy a custom template and create its resources in OCI.
- Installed Terraform on your local machine. You can download Terraform from the official Terraform website and follow the installation instructions for your operating system.
- Installed the OCI CLI tool, and authenticated with a key pair or token-based credentials.

1. Log in to OCI and open Cloud Shell.

2. Create a directory on your local machine to store and run the Terraform code. If you have more than one OCI connector, you need a separate directory for each one. For example:



```
mkdir -p ~/terraform/oci-connector-1
```

3. Navigate to the directory you created and extract the Terraform files. Ensure all necessary Terraform files are present (`main.tf`, `template_params.tfvars`, and so on). For example:

```
cd ~/terraform/oci-connector-1  
tar -xzvf <your_template>.tar.gz.
```

4. Initialize Terraform in your project directory:

```
terraform init
```

It might take several seconds until the initialization is complete.

5. Apply your Terraform configuration using the downloaded parameter file. When prompted to enter a value, enter the tenancy OCID.

```
terraform apply --var-file=template_params.tfvars
```

6. When prompted, review the actions the Terraform will perform, and approve them by entering `yes`.

The Terraform template is deployed.

When the template is successfully uploaded to OCI, the initial discovery scan starts. When the scan is complete, you can view your cloud assets in Asset Inventory. You can also view details about the instance by hovering over the instance on the Data Sources & Integrations page, and then clicking View Details.

#### 2.2.6.5.2 | Configure the OCI connector for log collection

##### Abstract

Create an OCI service connector and define the log source within OCI and the connector's target as the OCI bucket you want to use for audit log collection.

In order to enable audit log collection in Cortex Cloud, you must first create an OCI service connector. For more details, see [Creating a Connector with a Logging Source](#). After you have created the OCI service connector, you can proceed to [Onboard Oracle Cloud Infrastructure](#) and enable collection of audit logs.

1. Log in to the OCI Console. Open the navigation menu and go to Analytics and AI → Connector Hub.
2. On the Connectors page, click Create connector.
3. On the Create Connector page, enter a descriptive name for the new connector (for example, `CortexCloud_Log_Exporter`). Click Create connector.
4. Select the Compartment where you want to store the new connector resource.
5. Set the Source service to Logging.
6. Set the Target service to Object Storage. This is the storage bucket that Cortex Cloud will read from.
7. Under Configure target, configure the storage bucket to send the log data to:
  - Compartment: Select the compartment that contains the bucket that you want to use.
  - Bucket: Select the name of the bucket that you want to send the data to.
  - Object Name Prefix: (Optional) Enter a prefix value.
  - Show additional options: (Optional) Click this link to enter values for batch size (in MBs) and batch time (in milliseconds).
8. (Optional) Add one or more tags to the connector. Select Show Advanced Options to show the Add Tags section.
9. Click Create. When the connector is ready, the connector's details page opens.

When you onboard your OCI environment and select to Collect Audit Logs, enter the OCI region, the bucket name, and the compartment OCID.

#### 2.2.6.6 | Manually connect a cloud instance

When onboarding your cloud instance using the onboarding wizard, after you download the authentication template and execute it in your cloud environment, notification is sent to Cortex Cloud and a cloud instance is created. This connection between your cloud environment and the Cortex Cloud cloud instance typically occurs automatically.

There are several scenarios when the instance should be connected manually:

- You executed the template in your cloud environment and your environment is an air-gapped network. In this case, the notification to create the instance in Cortex Cloud does not happen.
- You have executed the template, but the instance has not appeared in Cloud Instances. This is often due to connectivity or firewall issues.
- You have a specific need to connect the instance manually.



To manually connect a cloud instance, you need to identify the pending instance you want to connect. In Cloud Instances, remove the default filter that excludes pending instances. Right-click on a pending instance and select View Details to see the configuration details of that specific pending instance. After you have identified the pending instance you want to connect manually, right-click and select Manually connect an instance. For more information on pending instances, see Pending cloud instances.

## AWS

In AWS Management Console, navigate to CloudFormation. Use the following table to guide you on where to obtain the necessary input for the manual onboarding. Not every field appears in every manual onboarding instance.

Connect Instance Input Field	Value
Organization ID	Onboarded organization ID.
Organizational Unit ID	Onboarded organizational unit ID.
Account ID	Onboarded account ID.
Role ARN	The value of Outputs → CORTEXXDRARN.
External ID	The value of Parameters → ExternalID.
Audit Logs SQS URL	The value of Resources → CloudTrailLogsQueue.
Audit Logs Role ARN	The value of Resources → CloudTrailReadRole → ARN.
Audit Logs Audience	Automatically populated.
Outpost Scanner Role ARN	The value of Resources → CortexPlatformScannerRole → ARN.

## GCP

1. Open your local terminal (Command prompt, PowerShell, or Terminal).

2. Log in to your GCP account using the gcloud CLI:

```
gcloud auth login
```

3. Display the values of all defined output variables in your Terraform configuration, formatted as a JSON object:

```
terraform output -json
```

Use the following table to guide you on which values in the output map to the necessary input for the manual onboarding. Not every field appears in every manual onboarding instance.

Connect Instance Input Field	Value
Organization ID	organization_id.value
Project ID	project_id.value
Folder ID	folder_id.value
Service Account Email	service_account_email.value



Connect Instance Input Field	Value
Audit Logs Audit Pubsub Subscription ID	resources_data.value.AUDIT_LOGS.audit_pubsub_subscription_id
Audit Logs Service Account Email	resources_data.value.AUDIT_LOGS.audit_service_account_email
Outpost Scanner Service Account Email	resources_data.value.OUTPOST_SCANNER.outpost_scanner_service_account_email

#### Azure with Terraform

1. Open your local terminal (Command prompt, PowerShell, or Terminal).

2. Log in to your Azure account using the Azure CLI:

```
az login
```

3. Display the values of all defined output variables in your Terraform configuration, formatted as a JSON object:

```
terraform output -json
```

Use the following table to guide you on which values in the output map to the necessary input for the manual onboarding. Not every field appears in every manual onboarding instance.

Connect Instance Input Field	Value
Resource Group Location (only for subscription scope)	Onboarded resource group location
Resource Group Name	Automatically populated
Audit Logs Audience	Automatically populated
Audit Logs Storage Account Name	resources_data.value.AUDIT_LOGS.storage_account_name
Audit Logs Tenant ID	Automatically populated
Audit Logs Client ID	resources_data.value.AUDIT_LOGS.client_id
Audit Logs Namespace	resources_data.value.AUDIT_LOGS.namespace
Audit Logs Eventhub Name	resources_data.value.AUDIT_LOGS.eventhub_name
Audit Logs Azure Audit Eventhub Consumer Group Name	resources_data.value.AUDIT_LOGS.azure_audit_eventhub_consumer_group_name

#### Azure Portal

- Navigate to the Microsoft Azure Portal and log in.

Use the following table to guide you on which values in the output map to the necessary input for the manual onboarding. Not every field appears in every manual onboarding instance.



Connect Instance Input Field	Value
Resource Group Location (only for subscription scope)	Onboarded resource group location
Resource Group Name	Automatically populated
Audit Logs Audience	Automatically populated
Audit Logs Storage Account Name	Navigate to Storage accounts and filter by resource group.
Audit Logs Tenant ID	Automatically populated
Audit Logs Client ID	Navigate to App registrations and sort by time. The default name starts with "auditlogsapp".
Audit Logs Namespace	Navigate to Event Hubs and filter by resource group.
Audit Logs Eventhub Name	Navigate to Event Hubs and select the Event Hub Namespace. Under Event Hubs, take the value in the Name column.
Audit Logs Azure Audit Eventhub Consumer Group Name	Navigate to Event Hubs -and select the Event Hub Namespace and then the Event Hub. Under Consumer Groups, use the value in the Name column, but not \$Default .

#### 2.2.6.7 | Edit your onboarded CSP configuration

In order to make changes to your onboarded CSP configuration, you first modify the cloud instance settings in Cortex Cloud and download an updated authentication template. After uploading the updated template to the CSP environment, you execute the template and then the changes take affect.

1. Navigate to Settings → Data Sources & Integrations.
2. Identify the Cloud Service Provider you want to update and click View Details.
3. In the Cloud Instances page, identify the cloud instance you want to edit and click the Configuration pencil to edit the instance.
4. Make changes to the configuration settings. Click Save.

If the changes you made require reexecuting the authentication template, you will be prompted to download the file. Click Download CloudFormation or Download Terraform as relevant to your CSP type.

**IMPORTANT:**

When using Terraform authentication templates, you must execute the updated Terraform template from the same folder where the original Terraform template was executed.

5. In the Cloud Instances page, a notification appears stating that there are pending changes for the cloud instance you updated. These changes are not applied until you execute the updated template in the CSP environment.
6. Execute the updated authentication template in your CSP environment by selecting the appropriate procedure below.

#### Amazon Web Services

After you have downloaded the updated CloudFormation authentication template, connect to AWS Management Console to perform a direct update to the stack using the updated template file. With a direct update, you submit a template or input parameters that specify updates to the resources in the stack, and CloudFormation immediately deploys them.

1. Log in to the AWS Management Console and open the CloudFormation console.
2. On the Stacks page, select the existing stack that you want to update.



3. In the stack details pane, select Update stack → Make a direct update.
4. On the Update stack page, select Replace existing template.
5. Under Specify template, select Upload a template file. Select the updated authentication template you downloaded from Cortex Cloud.
6. Click Next and Next again.
7. Select to acknowledge that AWS CloudFormation might create IAM resources with custom names. Click Next.
8. Click Submit. The stack update is complete when it appears in the Stacks list with status of UPDATE\_COMPLETE.

#### Google Cloud Platform

After you have downloaded the updated Terraform template file, connect to Google Cloud Console to update the stack using the updated template file.

1. Open your local terminal (Command prompt, PowerShell, or Terminal).

2. Log in to your GCP account using the gcloud CLI:

```
gcloud auth login
```

3. Navigate to the directory you originally used for the Terraform template when onboarding your CSP and extract the Terraform files.

```
cd ~/terraform/gcp-connector-1
tar -xzvf <your_template>.tar.gz
```

4. Initialize the upgrade of the Terraform in your project directory:

```
terraform init -upgrade
```

5. Apply your Terraform configuration using the downloaded parameter file. When prompted, enter the project ID if you configured one in the onboarding wizard:

```
terraform apply --var-file=template_params.tfvars
```

The updated Terraform template is deployed.

#### Microsoft Azure Resource Manager using the CLI

After you have downloaded the updated authentication template file, log in to Azure portal to update the stack using the updated template file.

1. Log in to the Azure portal. Select Cloud Shell from the top navigation and then select Bash.

2. Navigate to the directory you originally used for the authentication template when onboarding your CSP and extract the files.

```
cd ~/azure-connector-1
tar -xzvf <your_template>.tar.gz
```

3. In Cloud Shell, run the onboard.sh file:

```
bash onboard.sh
```

The updated authentication template is deployed.

#### Microsoft Azure subscriptions

After you have downloaded the updated authentication template file, use the same method you used initially to execute the template in Microsoft Azure:

##### Execute the Terraform authentication template

1. Open your local terminal (Command prompt, PowerShell, or Terminal).

2. Log in to your Azure account using the Azure CLI:

```
az login
```

3. Navigate to the directory you originally used for the Terraform template when onboarding your CSP and extract the Terraform files.

```
cd ~/terraform/azure-connector-1
tar -xzvf <your_template>.tar.gz
```

4. Initialize the upgrade of the Terraform in your project directory:

```
terraform init -upgrade
```

5. Apply your Terraform configuration using the downloaded parameter file. :

```
terraform apply --var-file=template_params.tfvars
```

The updated Terraform template is deployed.

##### Deploy the authentication template in Azure Resource Manager



1. Open your local terminal.
2. Log in to your Azure account using the Azure CLI:

```
az login
```

3. Deploy the updated template file:

```
az deployment sub create --location <LOCATION> --subscription <SUBSCRIPTION_ID> --template-file <JSON_TEMPLATE>
```

where:

- <LOCATION> is the location of the resource group. (For example, eastus or westus.)
- <SUBSCRIPTION\_ID> is the ID of the subscription you want to onboard.
- <JSON\_TEMPLATE> is the JSON template file that you downloaded at the end of the onboarding wizard.

The updated template is deployed.

#### 2.2.6.8 | Outposts

##### Abstract

An outpost enables you to have security scans performed on infrastructure in a cloud account owned by you.

An outpost is a dedicated set of infrastructure resources that extends the reach of Cortex Cloud into your environment. It serves as a secure, localized point for scanning assets across cloud providers and on-premises workloads.

By establishing a trusted relationship between Palo Alto Networks and your environment, the outpost allows for deep security analysis—such as identifying vulnerabilities or classifying sensitive data—while ensuring that your live workloads remain unaffected. This architecture helps you maintain strict data residency and compliance by performing scans locally within a demarcated area of your network.

##### **IMPORTANT:**

Outpost scan is an alternative to the recommended standard cloud scan. Cloud scan is recommended because it is fully managed by Palo Alto Networks and incurs no compute costs for your organization. Outpost scan is an advanced deployment model reserved for specific data residency or architectural requirements.

##### What's Next?

- Review outpost fundamentals
- Plan your outpost
- Create your outpost

#### 2.2.6.8.1 | Outpost fundamentals and planning

##### Abstract

An outpost enables you to have security scans performed on infrastructure in a cloud account owned by you. Learn about outpost fundamentals and what to consider when planning your outpost.

This topic explains the basic fundamentals for planning and deploying outpost infrastructure.

##### **IMPORTANT:**

While outposts provide maximum control over the scanning environment, cloud scan mode is the recommended default for most organizations.

##### When to choose outpost scan

Cloud scan offers lower operational overhead, faster onboarding, and Palo Alto Networks assumes the associated cloud compute costs.

Outpost scan mode should typically only be reserved for specific architectural requirements or strict data residency constraints.

If you determine you do need outpost scanning, consider the following differences between the scan modes, which might impact your decision.



Cloud Scan (Recommended)	Outpost Scan
<p>Configure a managed outpost when there is sufficient trust between you and Cortex Cloud. Cortex accesses your environment more extensively and with less mediation.</p>	<p>Choose to deploy and manage your own outpost if:</p> <ul style="list-style-type: none"> <li>• If you operate in a high-regulated market with a healthy mistrust of vendors.</li> <li>• For compliance with certain regulations for which Cortex is not compliant out of the box.</li> </ul> <p>In these cases, you might prefer to keep your data within your own network boundary.</p>
<p>The cloud resources involved are charged to Palo Alto Networks instead of to you.</p>	<p>This mode requires additional cloud provider permissions and may incur additional cloud costs.</p>
<p>Cortex-managed outposts require zero management from you.</p>	<p>Outposts incur some additional maintenance overhead. This includes securing the outpost, managing the necessary IAM roles and permissions, upgrading versions, and adjusting cloud provider quotas to meet workload demands. Actively manage your capacity and quotas to meet the workload requirements.</p>
<p>For DSPM, your actual data is accessible to Palo Alto Networks— not just metadata. Rest assured, your data are deleted after scanners have completed. Zero trust security is used to secure your data in Palo Alto Networks-owned accounts.</p>	<p>For DSPM, only metadata is accessible to Palo Alto Networks—not your actual data.</p>
<p>DSPM on SaaS (such as for Snowflake and Office 365) is currently supported only for cloud scan.</p>	<p>DSPM on SaaS (such as for Snowflake and Office 365) is not supported for outpost scan.</p>

#### Outpost security concepts and component handling

This section presents outpost-related concepts and a high-level overview of how outposts perform scanning on your resources and data without putting them at risk. For a deeper understanding, contact your Palo Alto Networks representative.

Concept	Description
<p>Trust model</p>	<p>Cortex Cloud interacts with your environment via dedicated IAM roles within the outpost. This establishes a secure trust relationship that adheres to the principle of least privilege.</p>
<p>Data security and residency</p>	<p>Outposts utilize a regionally symmetric architecture, processing data locally within the same cloud region and provider where it resides. Only metadata is ever sent back to Cortex Cloud.</p>
<p>Scan operations</p>	<p>Scanning is performed by task-specific, ephemeral VMs built from hardened and continuously patched images. These instances are automatically terminated and all temporary resources are purged immediately after a scan completes.</p>
<p>Secure orchestration storage (such as buckets)</p>	<p>Scanner VMs operate in isolated private subnets without direct internet or Cortex Cloud access. They communicate exclusively through encrypted, cloud-native storage used for operational data and scan results— never raw customer data.</p>



Concept	Description
Temporary processing storage (such as artifact buckets)	For specific scans where direct data sharing is restricted, data is temporarily placed in encrypted regional storage for analysis. Cortex Cloud has no read permissions on this storage, and all data is deleted immediately after the job finishes.
Scanner isolation	Each scanner VM is purpose-built with a strictly defined set of permissions and network access tailored to its specific job. This ensures complete compartmentalization between different scan types.
Data encryption	Security is enforced through universal encryption at rest and in transit. Advanced egress filtering locks down external traffic to verified destinations, and secrets are managed via your own cloud-native secret management service.

#### Outpost planning

Before creating outposts, we recommend you become familiar with how outposts work and then plan accordingly. For example, some points to consider include:

- A dedicated account is required for the outpost account. Make sure the dedicated account is free from other resources.
- Each cloud account (AWS account, Azure subscription, GCP project) can host only one outpost.
- An individual outpost instance is strictly bound to a single Cortex Cloud tenant and cannot be used to scan resources belonging to a different tenant or organization.
- Using an outpost requires additional cloud provider permissions and may incur additional cloud costs.
- Familiarize yourself with the needed permissions and resources expected to be added to the outpost during creation.

For exact implementation details, contact your Palo Alto Networks representative.

#### About outpost creation

After planning, you can create and configure your outpost in the following ways:

- Before onboarding your Cortex Cloud with the cloud service provider (CSP) onboarding wizard, create an outpost by navigating to Settings → Data Sources & Integrations → Outposts.
- Alternatively, while onboarding your Cortex Cloud with the cloud service provider (CSP) onboarding wizard, the wizard prompts you to choose a scan mode: Cloud scan or Outpost scan. When choosing Outpost scan, you have the opportunity to create your outpost. To start the cloud service provider (CSP) onboarding wizard, navigate to Settings → Data Sources & Integrations → Add New.

#### NOTE:

Before you create your outpost, verify that your internet connection is active. An active internet connection is necessary for the notification to be sent to Cortex Cloud to create the new outpost.

For details, see Create an outpost.

#### What's next?

- Create your outpost
- View and manage existing outposts by navigating to Settings → Data Sources & Integrations → Outposts

#### 2.2.6.8.2 | Create an outpost

##### Abstract

Create an outpost for security scanning performed on infrastructure in a cloud account owned by you.

This topic provides instructions for creating an outpost for different CSPs.

#### IMPORTANT:



While outposts provide maximum control over the scanning environment, cloud scan mode is the recommended default for most organizations. For details, see [When to choose outpost scan](#).

Creating an outpost comprises the following phases:

1. Planning
2. Running the outpost creation wizard in Cortex Cloud to generate an outpost authentication template for the relevant CSP. This template establishes trust with the CSP and grant the necessary permissions to Cortex Cloud. Described below.
3. Executing the template in the CSP to create the outpost, initially in pending status. Described below.
4. Running the CSP onboarding wizard Cortex Cloud to generate an authentication template for the relevant CSP (AWS, GCP, Azure).
5. Executing the authentication template in the CSP to onboard the CSP and ingest its data sources.

Run the outpost creation wizard to generate a template

Start the outpost creation wizard by navigating to Settings â Data Sources & Integrations â Outposts and clicking New Outpost.

**NOTE:**

Verify that your internet connection is active. An active internet connection is necessary for notifications to be sent to Cortex Cloud for creating the new outpost. If you are unable to establish an internet connection, contact customer support for a manual workaround.

Perform the steps according to your CSP.

AWS

1. In Create AWS Outpost, select the type of AWS environment:
  - **Commercial:** (Default) Standard cloud deployment typically used for private and public sector organizations that do not require isolated government-specific infrastructure.
  - **Government:** AWS GovCloud environments for compatibility with FedRAMP-certified tenants.
2. (Optional) Define tags and tag values to be added to any new resource created by Cortex in the cloud environment. Click Next.
3. Click Download Terraform to download the Terraform template file.

Execute the Terraform template in the CSP to create the outpost.

GCP

1. In Create GCP Outpost, select the type of GCP environment:
  - **Commercial:** (Default) Standard cloud deployment typically used for private and public sector organizations that do not require isolated government-specific infrastructure.
  - **Government:** GCP Assured Workloads for compatibility with FedRAMP-certified tenants.
2. Enter the project ID of the GCP project.
3. (Optional) Define tags and tag values to be added to any new resource created by Cortex in the cloud environment. Click Next.
4. Click Download Terraform to download the Terraform template file.

Execute the Terraform template in the CSP to create the outpost.

Azure

**NOTE:**

When creating an outpost for a specific Azure subscription, the outpost account must be in the same Azure organization as the monitored subscriptions.

1. In Create Azure Outpost, select the type of Microsoft Azure environment:
  - **Commercial:** (Default) Standard cloud deployment typically used for private and public sector organizations that do not require isolated government-specific infrastructure.
  - **Government:** Microsoft Azure Government environments for compatibility with FedRAMP-certified tenants.
2. Enter the tenant ID of the Azure tenant in which you want to establish the outpost.
3. (Optional) Define tags and tag values to be added to any new resource created by Cortex in the cloud environment. Click Next.
4. Click Download Terraform to download the Terraform template file.

Execute the Terraform template in the CSP to create the outpost.



Execute the template in the CSP to finalize the outpost

When you have downloaded the Terraform template file in the onboarding wizard, log in to the CSP and execute the template file.

Perform the steps according to your CSP.

AWS

#### **PREREQUISITE:**

Before you begin, ensure you have:

- An AWS account
- Permission to create a stack and its resources in AWS
- Installed Terraform on your local machine. You can download Terraform from the official Terraform website and follow the installation instructions for your operating system.
- Installed the AWS CLI tool and configured your profile with the `aws configure sso` wizard.

1. Open your local terminal (Command prompt, PowerShell, or Terminal).

2. Log in to your AWS account using the AWS CLI:

```
aws sso login --profile <my-profile>
```

Where `<my-profile>` is the profile you configured with the `aws configure sso` wizard.

3. Create a directory on your local machine to store and run the Terraform code. If you are creating more than one outpost, you need a separate directory for each one:

```
mkdir -p ~/terraform/aws-outpost-1
```

4. Navigate to the directory you created and extract the Terraform files.

```
cd ~/terraform/aws-outpost-1  
tar -xvf <your_template>.tar.gz
```

5. Initialize Terraform in your project directory:

```
terraform init
```

6. Apply your Terraform configuration using the downloaded parameter file. When prompted, enter the subscription ID:

```
terraform apply --var-file=template_params.tfvars
```

7. When prompted, review the actions Terraform will perform and approve them by entering `yes`.

The Terraform template is deployed, and your outpost is created. To view all outposts and their details, navigate to Settings → Data Data Sources & Integrations → Outposts.

GCP

#### **PREREQUISITE:**

Before you begin, ensure you have:

- A GCP account
- Permission to create the required resources in Google Cloud Deployment Manager
- Installed Terraform on your local machine. You can download Terraform from the official Terraform website and follow the installation instructions for your operating system.
- Installed the GCP gcloud CLI tool

1. Open your local terminal (Command Prompt, PowerShell, or Terminal).

2. Log in to your GCP account using the gcloud CLI:

```
gcloud auth login
```

3. Create a directory on your local machine to store and run the Terraform code. If you are creating more than one outpost, you need a separate directory for each one:

```
mkdir -p ~/terraform/gcp-outpost-1
```

4. Navigate to the directory you created and extract the Terraform files.

```
cd ~/terraform/gcp-outpost-1  
tar -xvf <your_template>.tar.gz
```

5. Initialize Terraform in your project directory:

```
terraform init
```



6. Apply your Terraform configuration using the downloaded parameter file. When prompted, enter the project ID:

```
terraform apply --var-file=template_params.tfvars
```

7. When prompted, review the actions Terraform will perform and approve them by entering **yes**.

The Terraform template is deployed, and your outpost is created. To view all outposts and their details, navigate to Settings  $\rightarrow$  Data Sources & Integrations  $\rightarrow$  Outposts.

Azure

#### PREREQUISITE:

Before you begin, ensure you have:

- An active Azure subscription.
- Installed the Azure CLI tool.
- Permission to deploy a custom template and create its resources in Microsoft Azure ("Owner" or "Contributor" on the designated outpost subscription scope, and Active Directory "Cloud Application Administrator" or "Application Administrator" privileged roles).
- Installed Terraform 1.9.4 or above on your local machine. You can download Terraform from the official Terraform website and follow the installation instructions for your operating system.
- A static egress IP assigned to the machine running this Terraform. This is used to configure the Azure Storage IP whitelist (Recommended). Without this, future runs of this Terraform may fail on Azure storage configurations.

1. Open your local terminal (Command Prompt, PowerShell, or Terminal).

2. Log in to your Azure account using the Azure CLI:

```
az login
```

3. If prompted, select the `subscription_id` of the designated subscription, or run:

```
az account set --subscription <subscription_id>
```

Where `<subscription_id>` is the subscription ID of the designated subscription.

4. Create a directory on your local machine to store and run the Terraform code. If you are creating more than one outpost, you need a separate directory for each one:

```
mkdir -p ~/terraform/azure-outpost-1
```

5. Navigate to the directory you created and extract the Terraform files.

```
cd ~/terraform/azure-outpost-1  
tar -xzvf <your_template>.tar.gz
```

6. Initialize Terraform in your project directory:

```
terraform init
```

7. Apply your Terraform configuration using the downloaded parameter file. When prompted, enter the subscription ID:

```
terraform apply --var-file=template_params.tfvars
```

8. When prompted for `var.storage_account_ip_whitelist`, you can leave it empty to enable access from any public IP to the storage accounts. We recommend you to limit access to selected IPs. To limit access, enter a comma-separated list of public IP addresses, including your local machine's egress IP (to enable the completion of the Terraform run). For example: `8.8.8.8, 8.8.4.4`

9. Review the actions Terraform will perform and approve them by entering **yes**.

10. It is important to create a backup of the Terraform state file using one of the following methods:

Back up the `terraform.tfstate` and `terraform.tfstate.backup` files or use Terraform backend to save the state.

- Create copies of the `terraform.tfstate` and `terraform.tfstate.backup` files. These can then be moved to the working folder to allow Terraform to upgrade or destroy the created resources as necessary.
- Ensure you're using a backend block in your Terraform configuration. For more information, see Backend block configuration overview.

The Terraform template is deployed, and your outpost is created. To view all outposts and their details, navigate to Settings  $\rightarrow$  Data Sources & Integrations  $\rightarrow$  Outposts.

What's next?

After you have executed the template in your CSP:

- The necessary permissions are granted and a notification is sent to Cortex Cloud with the execution details.
- A new outpost is created in pending status and can be viewed in the Outpost page at Settings  $\rightarrow$  Data Sources & Integrations  $\rightarrow$  Outposts.



Continue the CSP onboarding by running and executing the CSP onboarding wizard to generate an authentication template for the relevant CSP (AWS, GCP, Azure).

## Troubleshooting

If you have successfully executed the template in your cloud service provider and no new outpost has been created, verify that your internet connection is active. An active internet connection is necessary for the notification to be sent to Cortex Cloud to create the new outpost. If you are unable to establish an internet connection, contact customer support for a manual workaround.

### 2.2.6.9 | Introduction to Terraform for Cloud service provider (CSP) onboarding

#### Abstract

Introductory concepts for working with Terraform to facilitate cloud onboarding.

Terraform is an open-source Infrastructure as Code (IaC) tool that allows you to define and provision cloud infrastructure using declarative configuration files. Instead of manually creating resources in a cloud console, you use Terraform templates to automate the setup required for Cortex Cloud.

#### Key Terraform concepts

These concepts explain the underlying logic of how Terraform interacts with your cloud environment.

##### Infrastructure as Code (IaC)

Infrastructure as Code allows you to manage your network and security settings through declarative configuration (text) files. Terraform reads these files and compares them to your actual cloud environment to determine which resources need to be created, updated, or deleted to match the template.

##### The Terraform state file (.tfstate)

The `.tfstate` state file is a local record that maps your template configuration to the real resources in your cloud. The state file acts as a database that maps your configuration to real-world resources.

Each time you execute a Terraform template (such as by using plan or apply commands), Terraform compares the state file with the actual cloud environment to ensure everything is in sync. If there are differences, Terraform attempts to sync between the template and the cloud. Any resources that differ from the template are synced to match the template definition.

It is critical that you follow the following rules:

- Never delete the `.tfstate` file. If this file is lost, Terraform loses its "memory" of what it created, making it difficult to update or offboard (delete) those resources later.
- Always run Terraform commands from the original folder where you initialized the template to ensure access to the `.tfstate` file.
- If using a cloud-based terminal (like Azure Cloud Shell), ensure your files are saved to a persistent directory so the `.tfstate` file is not lost when the session ends.

#### Authentication and CLI prerequisites

Terraform does not have its own login; it uses the credentials for each cloud service provider. Before executing Terraform templates provided by Cortex Cloud, configure and authenticate using your cloud provider's Command Line Interface (CLI):

- AWS: Configure the AWS CLI.
- Azure: Log in to the Azure CLI (`az`).
- GCP: Initialize the Google Cloud CLI (`gcloud`).
- OCI: Configure the OCI CLI. We recommend you use token based authentication.

#### Core Terraform commands

While Terraform has many features, the Cortex Cloud onboarding process typically only uses the following core commands.

#### **IMPORTANT:**

Always run these commands in the same folder where the original `.tf` files and `.terraform` folder live – this is where the state is stored.

The `terraform init` command

The `terraform init` command prepares Terraform for the actual actions it will perform, such as downloading any required modules and cloud provider plugins.

Command: `terraform init`

Run this command when:



- It is the first time the template is going to be executed.
- There are changes to the template that necessitate updates to modules that have changed.

The `terraform apply` command

The `terraform apply` command previews the changes and executes the template to create or update the cloud resources.

Command: `terraform apply --var-file=template_params.tfvars [-auto-approve]`

When running the command, you must pass the template parameter file as an argument.

This command requests confirmation before making any changes. Type `yes` for the changes to be made. You can bypass the confirmation by passing `-auto-approve` to the `apply` command.

The first time this command is run, this command also creates the `.tfstate` state file. This file stores the state of the cloud resources at the time the command is executed.

#### **IMPORTANT:**

This `.tfstate` state file is critical because it is needed by the `terraform destroy` command to clean up created resources. It is critical that you never delete this file.

The `terraform destroy` command

The `terraform destroy` command removes all resources created by the `terraform apply` command. This is the standard way to offboard the CSP.

Command: `terraform destroy --var-file=template_params.tfvars [-auto-approve]`

Run this command:

- To off-board.
- To re-onboard. Before re-onboarding, clean up existing resources before re-onboarding.

When running the command, you must pass the template parameter file as an argument.

This command requests confirmation before making any changes. Type `yes` for the changes to be made. You can bypass the confirmation by passing `-auto-approve` to the `apply` command.

Standard Terraform deployment workflows

The lifecycle of a Cortex Cloud resource involves the following primary workflows:

- The initial provisioning of resources.
- The subsequent updating of those resources as requirements change, or as Cortex releases new updates and features.

Initial template onboarding

The onboarding process involves the initial translation of your cloud configuration into live cloud resources.

- **Preparation:** Download the necessary provider plugins, and then download and extract the Terraform template configuration files, such as `.tf` and `.tfvars`, into the working directory.
- **Initialization:** Prepare the local environment for a specific template by executing this command from inside the template folder:

`terraform init`

- **Application:** Apply the configuration to the cloud provider using the specific variable file (such as `template_params.tfvars`) to define your unique environment settings. Execute this command from inside the template folder:

`terraform apply --var-file=template_params.tfvars`

Upgrades

As Cortex releases new features or updates, or you have changes to your own cloud infrastructure, you must update the existing template. This workflow involves merging new configuration files into your existing local directory while strictly maintaining the original state file.

This "upgrade" scenario relies on the state file to identify what has changed. By reconfiguring the initialization and applying the new files, Terraform identifies the differences and modifies the existing resources rather than recreating them from scratch.



- **Reconfiguration:** Updates the existing working template folder to account for changes in the underlying template structure, such as by copying new files into the folder. You can replace existing files but do not delete any files.
- **Synchronization:** Updates the live cloud resources to align with the new template definition while preserving your existing variables. Execute the following commands:

```
terraform init -reconfigure
terraform apply --var-file=template_params.tfvars
```

Working in Cloud Shell environments

If you are onboarding using a browser-based terminal (like Azure Cloud Shell or GCP Cloud Shell) instead of locally, make sure to adhere to the following:

- **Keep the original folder:** You must always run commands from the original folder where you initialized Terraform.
- **Persistence:** Ensure your session is saved to a persistent home folder (such as `~/.`). If the session ends and the folder is deleted, your `.tfstate` file will be lost, which prevents easy cleanup or resource management.

CSP	Folder For Persistence
Azure	See Persist files in Azure Cloud Shell
AWS	<code>~/</code>
GCP	<code>~/</code>
OCI	<code>~/</code>

## 2.2.6.10 | Container Registry Scanning

### 2.2.6.10.1 | Overview of container registry scanning

Container Registry Scanning identifies vulnerabilities, malware, and secrets, providing comprehensive protection for containerized applications across various cloud environments without manual intervention.

Cortex Cloud supports scanning of registries through the following methods:

- **Managed Cloud Registries:** The container registry scanner automatically detects and scans container registries and images within your onboarded cloud accounts. Supported registries include Amazon Elastic Container Registry (ECR), Azure Container Registry (ACR), Google Artifact Registry (GAR), and Oracle Cloud Infrastructure (OCI) Artifact Registry.
- **Third-Party Integrations:** The container registry scanner supports agentless scanning of container images by direct integration with various third-party registries, independent of the cloud account onboarding process. These integrations include a streamlined, user-friendly connector configuration experience for the following:
  - Docker Hub
  - Docker V2 compliant registries
  - GitLab Container Registry
  - Harbor Registry
  - JFrog Container Registry
  - Sonatype Nexus Repository Manager

After you onboard your container registries, Runtime Security ensures that all containers and images are scanned at regular intervals and that you are notified about any deviation from your security policies and best practices.

### 2.2.6.10.1.1 | Registry Components

To understand how container registry scanning works, it's essential to understand its core components:



- **Container registry:** A container registry is a service for publishing, maintaining, and securely distributing container images, providing a centralized hub for managing and accessing containerized application components across your organization. This scanning helps to enable proactive identification and remediation of security risks before deployment which means you will be using only trusted and compliant images in production environments.
- **Container image repository:** Within a container registry, container images are organized into multiple repositories to improve management, access control, collaboration, and security isolation. Each repository should ideally contain images related to a specific application, service, or project, allowing for granular permissioning and security policies. Images within a repository often share a common base image or purpose, making it easier to apply consistent security controls across related components.
- **Image Tags:** Image tags are essential for identifying and managing container image versions within a repository, enabling the selection and deployment of appropriate builds. From a security perspective, tags facilitate tracking vulnerable images, deploying patched versions, and maintaining image provenance for auditing. There are two common formats for referencing image tags:
  - image:tag – A human-readable label that can be reassigned to different versions. For example, myapp:latest or myapp:v1.0.0.
  - image@sha – A cryptographic hash that provides an immutable reference to a specific image version. For example, myapp@sha256:abc123.

While human-readable tags like myapp:latest (reassignable) and myapp:v1.0.0 are common, using immutable tags such as myapp@sha256:abc123 provides a cryptographically secure and verifiable reference, crucial for ensuring the integrity and trustworthiness of deployed images.

- **Image Digest:** A cryptographic digest (SHA-256 hash) uniquely identifies a container image's content, providing a strong guarantee of immutability. Unlike user-defined image tags, which can be reassigned, using the digest as a tag ensures that even if an image is renamed or retagged, its content remains verifiably identical, making it a critical element for security auditing and ensuring the integrity of deployed applications. Relying on image digests helps prevent potential supply chain attacks where malicious actors might attempt to replace images with compromised versions.

#### 2.2.6.10.1.1 | How Container Registry Scanning Works

The process of container registry scanning consists of three key phases: discovery, scanning, and evaluation.

1. **Discovery:** The connector discovers all registries, repositories, and tags within the account.
2. **Scanning:** The connector extracts software bills of materials (SBOMs), malware indicators, and secrets from each image.
3. **Evaluation:** Scan results are evaluated for vulnerabilities, malware, and secrets, and asset findings are created accordingly.

#### 2.2.6.10.2 | Configure registry scanning for cloud accounts

Configuring registry scanning ensures that only verified and compliant images are deployed across your cloud environments. You can configure container registry scanning during the onboarding process for managed registries such as Amazon Elastic Container Registry (ECR), Azure Container Registry (ACR), Google Artifact Registry (GAR), and Oracle Cloud Infrastructure (OCI) Artifact Registry.

If an account is already onboarded, you can modify its configuration to enable registry scanning as an Additional Security Capability to scan images for vulnerabilities, malware, and secrets.

#### **PREREQUISITE:**

Ensure that you have performed the all steps till Additional Security Capabilities as listed in the onboarding wizard for the required CSP:

- Onboard Amazon Web Services
- Onboard Google Cloud Platform
- Onboard Microsoft Azure
- Onboard Oracle Cloud Infrastructure

To configure registry scanning, do the following:

1. Under Additional Security Capabilities, select Registry Scanning, then click Edit Preferences.



## Additional Security Capabilities i

Enable additional security add-ons. This may require additional cloud provider permissions

XSIAM analytics i

Data security posture management i

Registry scanning i [Edit Preferences](#)

Serverless functions scanning i

2. In Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tags: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images created or modified in the last few days. You can select a range of up to 90 days for the scan.

3. Select Save.

After you configure your container registries, the system automatically starts a new scan. The connection process can take up to 15 minutes. To check the status of the data connector and view the registry scan results, go to the Cloud Instances page and select the relevant Instance Name from the list.

4. Next Steps.

- After the scan completes, you can view the scanned images in the Container Image page. For more details, see Container Image assets.
- You can also modify your cloud instances to manage them effectively. For more details, see Managing Cloud Instances.

### 2.2.6.10.3 | Modify the container registry scanning scope

Using the Modify Scanning Scope option, you can define conditions to automatically exclude selected scopes from scanning. These conditions can be based on the registry, repository, or tag. After you set the scope, the exclusion conditions are automatically applied to newly discovered images in the account.

To modify the scanning scope, do the following:

1. Navigate to Settings â Data Sources.
2. In the Cloud Provider section, locate the provider where your assets are stored and click View Details.
3. On the Cloud Instances page, click the instance name for which you want to modify the scope.
4. Under the Accounts section, select the account, right-click, and choose Edit.
5. Under the Registry Scanning Scope, enable Modify Scanning Scope.
6. From the list of images, select the image you want to modify.
7. Alternatively, you can also filter for a specific image by clicking the Filter icon and selecting Registry, Repository ,or Tags option and then adding the desired value to refine your search.

The search results are applied automatically, even if you do not select Save.

8. Click Save to confirm your modifications.

This ensures that the specified scanning scope is customized based on your needs.

### 2.2.6.10.4 | Scan re-evaluation process

After the initial scan has been completed, the scan re-evaluation process ensures that container images remain secure over time without requiring a full re-scan.



Instead of manually triggering new scans, the scan re-evaluation process automatically reassesses existing scan results every **24 hours** using the latest threat intelligence feeds. This approach reduces the need for resource-intensive re-scans, while maintaining up-to-date security assessments.

By continuously monitoring container images for emerging threats, you can proactively mitigate risks and ensure compliance with security best practices.

#### 2.2.6.10.5 | Connect Docker Hub registry

Cortex Cloud allows you to scan and secure your container images from vulnerabilities, malware, and secrets after you authenticate and connect your public or private Docker Hub account.

How to connect Docker Hub registry

Follow the wizard to connect your Docker Hub registry with Cortex Cloud.

1. Navigate to Settings → Data Sources & Integrations.
2. On the Add Data Source or Integrations page, click + Add New, search for Docker Hub, then hover over it and click Add.
3. The Instance Name is automatically populated. You can change it to a more meaningful name.
4. Choose the Scan Mode, and then follow the steps for that mode to configure the connection.

##### Cloud Scan

Security scanning is performed in the Cortex cloud environment when you select this mode.

1. Select the appropriate Cloud Provider and Region for the Cortex environment to use for registry scanning.

As a best practice, choose the region closest to your registry deployment to achieve the best scanning throughput and potentially reduce cloud costs.

2. (Optional) Enable Allow access by IPs to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so the scanner can access the registry during the scanning process.

3. Choose the relevant Repository Access for scanning:

##### Authenticated access

Discover and scan private and public repositories within the given account.

- a. Under Authentication Method, enter your private Docker Hub account credentials (Username and Password) for authentication.

##### Public access only

Discover and scan images within a specific public repository.

- a. Enter your public Docker Hub Repository Name.

To specify an official Docker Hub repository, enter `library/`, followed by the short string used to designate the repo. For example, to scan the images in the official Alpine Linux repository, enter `library/alpine`.

- b. Under Authentication Method, enter your public Docker Hub account user credentials (Username and Password) for authentication.

4. Select Next.

##### Scan with Outpost

Security scanning is performed on infrastructure deployed to a cloud account that you own. This mode requires additional cloud provider permissions and may incur extra costs.

#### PREREQUISITE:

Ensure an Outpost is connected to your tenant.

1. Choose a Cloud Provider to initialize registry scanning.

#### NOTE:

If you choose Azure as the Cloud Provider, you must also select the Tenant Id. The Tenant Id is required to approve Cortex as an enterprise application in your Azure tenant.

2. Choose Outpost account to use for this instance. If no Outposts are shown, you can Create a new one. For more details, see Outposts.

#### NOTE:

If you choose Azure as the cloud provider, only Outposts associated with the selected tenant ID are displayed.

3. Select the Region where the registry is hosted.



4. (Optional) Enable Allow access by IPs if you want to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so that the scanner can access the registry during the scanning process.

5. Choose the relevant Repository Access for scanning:

Authenticated access

Discover and scan private and public repositories within the given account.

a. Under Authentication Method, enter your private Docker Hub account credentials (Username and Password) for authentication.

Public access only

Discover and scan images within a specific public repository.

a. Enter your public Docker Hub Repository Name.

To specify an official Docker Hub repository, enter `library/`, followed by the short string used to designate the repo. For example, to scan the images in the official Alpine Linux repository, enter `library/alpine`.

b. Under Authentication Method, enter your public Docker Hub account user credentials (Username and Password) for authentication.

6. Select Next.

#### Scan with Broker VM

Security scanning in private networks is done using broker VM infrastructure when you select this mode.

##### **PREREQUISITE:**

- Set up and configure Broker VM
- Configure High Availability Cluster

1. Choose a Scan with Broker VM mode to initiate registry scanning. You can select either a standalone Broker VM or a High Availability (HA) Cluster.

2. Select Applicable Broker VMs.

Choose the appropriate Broker VM or Cluster from the list configured in your tenant.

##### **NOTE:**

- The list of Broker VMs displays only VMs that support registry scanning.
- The list of high-availability Clusters displays only clusters that contain at least one VM supporting registry scanning.
- The registry scanning status for each VM appears in brackets if it was previously activated for that specific VM.

If the list does not display any Broker VMs or Clusters, Add New Broker VM or Add New Cluster. For more details, see Set up and configure Broker VM.

3. Choose the relevant Repository Access for scanning:

Authenticated access

Discover and scan private and public repositories within the given account.

a. Under Authentication Method, enter your private Docker Hub account credentials (Username and Password) for authentication.

Public access only

Discover and scan images within a specific public repository.

a. Enter your public Docker Hub Repository Name.

To specify an official Docker Hub repository, enter `library/`, followed by the short string used to designate the repo. For example, to scan the images in the official Alpine Linux repository, enter `library/alpine`.

b. Under the Authentication Method, enter your public Docker Hub account user credentials (Username and Password) for authentication.

4. Select Next.

5. In Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tag: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images created or modified in the last few days. You can select a range of up to 90 days for the scan.

6. Select Save.



When the Docker Hub data source is saved, a new data connector is created, and the initial discovery scan begins. The connection process may take up to 15 minutes.

#### 7. To check the connector status and scan results, follow these steps:

- a. Navigate to Settings → Data Sources & Integrations.
- b. Find the Docker Hub instance from the list of 3rd Party Data Sources connectors, or use Search.
- c. In the Docker Hub instance row, select View Details. The Docker Hub Instances page appears.
- d. On the Docker Hub Instances page, you can filter results by any heading and value.
- e. Select an Instance Name to open the details pane. The details pane contains the following granular information:

Instance Details	Description
Status	Shows the status of the connector: Connected, Error, Warning, Disabled, or Pending.
Applet Status on Broker VM	Shows the status of the Registry Scanner applet on the Broker VM page. This status is visible only when the Scan with Broker VM mode is selected.
Repositories	Shows the number of scanned repositories in the registry.
Scan Mode	Shows the selected scan mode for the data connector, such as Cloud Scan, Scan with Outpost, or Scan with Broker VM.
Security Capabilities	Shows a breakdown of the security capabilities enabled on the instance and their individual statuses. For example, select Registry Scanning when it shows a warning or error status to see the open errors and issues that contributed to the status.

#### 8. Next Steps

After the scan is complete, you can view the scanned images on the Container Images Inventory page. For more details, see Container Image assets.

If you have selected the Scan with Broker VM option, then a Registry Scanner applet is created on the selected Broker VM or Cluster. For details, see Verify Registry Scanner connection.

DEVICE NAME	STATUS	CLUSTER NAME	VERSION	CONFIGURATION STATUS	APPS	CPU USAGE	MEMORY USAGE	DISK USAGE
8T	Connected		28.0.96	Up to date	Registry Scanner	31%	47%	0% (2.7GB/346.2GB)

2.2.6.10.5.1 | Manage a Docker Hub connector

After you add a Docker Hub connector, you can modify the connector settings and configure the scanning scope to control which images are scanned in the connected registry.

To manage the connector, follow these steps:

1. Select Settings → Data Sources.
2. Find the Docker Hub instance from the list of 3rd Party Data Sources connectors, or use Search.
3. In the Docker Hub instance row, select View Details. The Docker Hub Instances page appears.
4. On the Docker Hub Instances page, you can filter the results by any heading and value. You can also create a new instance by selecting + Add Instance and following the onboarding wizard to define the settings.





5. You can perform actions on each Docker Hub instance: For example, select the (three dots) icon to Exclude/Include image, Delete, or Disable the instance as follows:

Action	Instructions
Edit	<p>Edit the Docker V2 instance.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>If you selected Scan with Broker VM mode, you can't change to a different scan mode (such as Cloud Discovery or Scan with Outpost) when you edit the instance.</li> <li>When editing an instance configured for Scan with Broker VM, you must re-enter your authentication credentials, including Username, Password, and CA certificate.</li> </ul>
Exclude/Include images	Define conditions to automatically exclude or include specific images in scanning. Conditions can be based on Repository or Tags. These conditions apply automatically to newly discovered images in the account.
Delete	Removes the connector.
Disable	Stops image scanning for the connector without deleting it.

#### 2.2.6.10.6 | Connect Docker V2 compliant container registry

A Docker V2-compliant registry is a registry service that complies with the specifications and requirements outlined in the Docker Registry HTTP API V2. This API defines the protocol for interacting with a Docker registry, a repository where Docker images are stored and from which they can be pulled or pushed.

To scan public and private repositories on Docker Hub, use the Docker Hub registry connector.

##### How to connect Docker V2

Follow the wizard to use the Docker V2 connector in Cortex Cloud to scan and secure container images from any container registry that supports the Docker V2 protocol, ensuring comprehensive security.

1. Navigate to Settings → Data Sources & Integrations.
2. On the Add Data Source or Integrations page, click + Add New, search for Docker V2, then hover over it and click Add.
3. The Instance Name is automatically populated. You can change it to a more meaningful name.
4. Choose the Scan Mode, and then follow the steps for that mode to configure the connection.

##### Cloud Scan

Security scanning is performed in the Cortex cloud environment when you select this mode.

1. Select the appropriate Cloud Provider and Region for the Cortex environment to use for registry scanning.

As a best practice, choose the region closest to your registry deployment to achieve the best scanning throughput and potentially reduce cloud costs.

2. (Optional) Enable Allow access by IP's to specify a static IP address for the scanner to use. Ensure the static IP is allowed through your firewall so the scanner can access the registry during the scanning process.

3. Enter the Registry URL. This must match the URL you use with the docker login command.

Equivalent URL: <https://docker.io/>

If you are using a CA certificate for authentication, enter the server IP address instead of the Registry URL.

4. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

Use your Docker ID as the username (for example, john0907) and **not** your email address.

5. (Optional) Expand Show Advanced Settings, and then enter the CA certificate in PEM format for Cortex to validate the Docker registry v2.



Ensure that the Custom CA certificate that you use is not revoked by the issuing authority.

6. Select Next.

Scan with Outpost

Security scanning is performed on infrastructure deployed to a cloud account that you own. This mode requires additional cloud provider permissions and may incur extra costs.

#### **PREREQUISITE:**

Ensure an Outpost is connected to your tenant. Outposts

1. Choose a Cloud Provider to initialize registry scanning.

#### **NOTE:**

If you choose Azure as the Cloud Provider, you must also select the Tenant Id. The Tenant Id is required to approve Cortex as an enterprise application in your Azure tenant.

2. Choose Outpost account to use for this instance. If no Outposts are shown, you can Create a new one. For more details, see Outposts.

#### **NOTE:**

If you choose Azure as the cloud provider, only Outposts associated with the selected tenant ID are displayed.

3. Select the Region where the registry is hosted.

4. (Optional) Enable Allow access by IPâ€ s if you want to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so that the scanner can access the registry during the scanning process.

5. Enter the Registry URL. This must match the URL you use with the docker login command.

Equivalent URL: <https://docker.io/>

If you are using a CA certificate for authentication, enter the server IP address instead of the Registry URL.

6. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

Use your Docker ID as the username (for example, john0907) and not your email address.

7. (Optional) Expand Show advanced settings, and then enter the CA certificate in PEM format for Cortex to validate the Docker registry v2.

Ensure that the Custom CA certificate that you use is not revoked by the issuing authority.

8. Select Next.

Scan with Broker VM

Security scanning in private networks is performed using broker VM infrastructure when you select this mode.

#### **PREREQUISITE:**

Ensure one of the following is configured:

- Set up and configure Broker VM.
- Configure High Availability Cluster.

1. Choose a Scan with Broker VM mode to initiate registry scanning. You can select either a standalone Broker VM or a High Availability (HA) Cluster.

2. Select Applicable Broker VMs.

Choose the appropriate Broker VM or Cluster from the list configured in your tenant.

#### **NOTE:**

- The list of Broker VMs displays only VMs that support registry scanning.
- The list of high-availability Clusters displays only clusters that contain at least one VM supporting registry scanning.
- The registry scanning status for each VM appears in brackets if it was previously activated for that specific VM.

If the list does not display any Broker VMs or clusters, Add New Broker VM or Add New Cluster. For more details, see Set up and configure Broker VM.

3. Enter the Registry URL. This must match the URL you use with the docker login command.

Equivalent URL: <https://docker.io/>

If you are using a CA certificate for authentication, enter the server IP address instead of the Registry URL.

4. Under Authentication Method, enter the Username and Password of the registry that you want to connect.



Use your Docker ID as the username (for example, john0907) and not your email address.

5. (Optional) Expand Show advanced settings, and then enter the CA certificate in PEM format for Cortex to validate the Docker registry v2.

Ensure that the Custom CA certificate that you use is not revoked by the issuing authority.

6. Select Next.

5. In the Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tag: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images that have been created in the last few days. You can select a range of up to 90 days for the scan.

6. Select Save.

When the Docker V2 data source is saved successfully, a new data connector is created, and the initial discovery scan begins. The connection process can take up to 15 minutes.

7. To check the connector status and scan results, follow these steps:

- Select Settings → Data Sources.
- Find the Docker V2 instance from the list of 3rd Party Data Sources connectors, or use Search.
- In the Docker V2 instance row, select View Details. The Docker V2 Instances page appears.
- On the Docker V2 Instances page, you can filter results by any heading and value.
- Select an Instance Name to open the details pane. The details pane contains the following granular information:

Instance Details	Description
Status	Shows the status of the connector: Connected, Error, Warning, Disabled, or Pending.
Applet Status on Broker VM	Shows the status of the Registry Scanner applet on the Broker VM page. This status is visible only when the Scan with Broker VM mode is selected.
Repositories	Shows the number of scanned repositories in the registry.
Scan Mode	Shows the selected scan mode for the data connector, such as Cloud Scan, Scan with Outpost, or Scan with Broker VM.
Security Capabilities	Shows a breakdown of the security capabilities enabled on the instance and their individual statuses. For example, select Registry Scanning when it shows a warning or error status to see the open errors and issues that contributed to the status.

8. Next Steps

After the scan is complete, you can view the scanned images on the Container Images Inventory page. For more details, see Container Images assets.

If you have selected the Scan with Broker VM option, then a Registry Scanner applet is created on the selected Broker VM or Cluster. For details, see Verify Registry Scanner connection.



After you add a Docker V2 connector, you can modify the connector settings and configure the scanning scope to control which images are scanned in the connected registry.

To manage the connector, follow these steps:

1. Select Settings → Data Sources.
2. Find the Docker V2 instance from the list of 3rd Party Data Sources connectors, or use Search.
3. In the Docker V2 instance row, select View Details. The Docker V2 Instances page appears.
4. On the Docker V2 Instances page, you can filter the results by any heading and value. You can also create a new instance by selecting + Add Instance and following the onboarding wizard to define the settings.



5. You can also perform actions on each Docker V2 instance: for example, select the (pencil) icon to Edit the instance, or select the (three dots) icon to Exclude/Include images, Delete, or Disable the instance as follows:

Action	Instructions
Edit	<p>Edit the Docker V2 instance.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• If you selected Scan with Broker VM mode, you can't change to a different scan mode (such as Cloud Discovery or Scan with Outpost) when you edit the instance.</li> <li>• When editing an instance configured for Scan with Broker VM, you must re-enter your authentication credentials, including Username, Password, and CA certificate.</li> </ul>
Exclude/Include images	Define conditions to automatically exclude or include specific images while scanning. Conditions can be based on Repository or Tags. These conditions apply automatically to newly discovered images in the account.
Delete	Removes the connector.
Disable	Stops image scanning for the connector without deleting it.

Configure Cortex Cloud to scan your GitLab Container Registry without using administrator credentials. Use a GitLab Personal Access Token (PAT) to authenticate Cortex to access the GitLab Container Registry. This allows Cortex to list all container registries or images, and secure them from vulnerabilities, malware, and secrets.

How to connect GitLab registry

Follow the wizard to connect the GitLab Container Registry connector in Cortex Cloud.

1. Navigate to Settings → Data Sources & Integrations.
2. On the Add Data Source or Integrations page, click + Add New, search for GitLab Container Registry, then hover over it and click Add.
3. The Instance Name is automatically populated. You can change it to a more meaningful name.
4. Choose the Scan Mode, and then follow the steps provided for that mode to configure the connection.

#### Cloud Scan

Security scanning is done in the Cortex cloud environment when you select this mode.

1. Select the appropriate Cloud Provider and Region for the Cortex environment to use for registry scanning.

As a best practice, choose the region closest to your registry deployment to achieve the best scanning throughput and potentially reduce cloud costs.



2. (Optional) Enable Allow access by IPs to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so the scanner can access the registry during the scanning process.

3. Choose the relevant Account Type for Gitlab deployments:

Gitlab Cloud (Saas)

a. (Optional) Enter the Group Id.

You can enter a single group ID or a list of group IDs separated by a comma. The group ID is used to locate all the registries within a specific group.

b. (Optional) Enter the Project Id.

You can enter a Gitlab Project ID or a list of project IDs separated by a comma. The project ID is used to locate all the registries located within a specific project.

**NOTE:**

When both the group ID and project ID are provided, the system retrieves container images from all projects within the specified group as well as from the specified project.

If neither the group ID nor the project ID is provided, the system retrieves container images from all registries (across all groups and projects) accessible to the authenticated user or token in GitLab.

c. Under Authentication Method, enter your Gitlab Access Token.

Gitlab Self-Hosted

a. Enter the Registry URL.

If you are using a CA certificate, enter the server IP address instead of the registry url.

b. (Optional) Enter the Group id.

You can enter a single group ID or a list of group IDs separated by a comma. The group ID is used to locate all the registries within a specific group.

c. (Optional) Enter the Project Id.

You can enter a Gitlab Project ID or a list of project IDs separated by a comma. The project ID is used to locate all the registries located within a specific project.

**NOTE:**

When both the group ID and project ID are provided, the system retrieves container images from all projects within the specified group as well as from the specified project.

If neither the group ID nor the project ID is provided, the system retrieves container images from all registries (across all groups and projects) accessible to the authenticated user or token in GitLab.

d. Enter the Api Domain. You must enter the base URL for the Gitlab API.

e. Under Authentication Method, enter your Gitlab Access Token.

f. (Optional) Expand Show Advanced Settings, and then enter the CA certificate in PEM format for Cortex to validate the Gitlab registry.

4. Select Next.

Scan with Outpost

Security scanning is done on infrastructure deployed to a cloud account that you own. This mode requires additional cloud provider permissions and may incur extra costs.

**PREREQUISITE:**

Ensure an Outpost is connected to your tenant.

1. Choose a Cloud Provider to initialize registry scanning.

**NOTE:**

If you choose Azure as the Cloud Provider, you must also select the Tenant Id. The Tenant Id is required to approve Cortex as an enterprise application in your Azure tenant.

2. Choose Outpost account to use for this instance. If no Outposts are shown, you can Create a new one. For more details, see Outposts.

**NOTE:**

If you choose Azure as the cloud provider, only Outposts associated with the selected tenant ID are displayed.

3. Select the Region where the registry is hosted.



4. (Optional) Enable Allow access by IPs if you want to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so that the scanner can access the registry during the scanning process.

5. Choose the relevant Account Type for Gitlab deployments:

Gitlab Cloud (Saas)

a. (Optional) Enter the Group Id.

You can enter a single group ID or a list of group IDs separated by a comma. The group ID is used to locate all the registries within a specific group.

b. (Optional) Enter the Project Id.

You can enter a Gitlab Project ID or a list of project IDs separated by a comma. The project ID is used to locate all the registries located within a specific project.

**NOTE:**

When both the group ID and project ID are provided, the system retrieves container images from all projects within the specified group as well as from the specified project.

If neither the group ID nor the project ID is provided, the system retrieves container images from all registries (across all groups and projects) accessible to the authenticated user or token in GitLab.

c. Under Authentication Method, enter your Gitlab Access Token.

Gitlab Self-Hosted

a. Enter the Registry URL.

If you are using a CA certificate, enter the server IP address instead of the registry url.

b. (Optional) Enter the Group Id. You can enter a single group ID or a list of group IDs separated by a comma. The group ID is used to locate all the registries within a specific group.

c. (Optional) Enter the Project Id. You can enter a Gitlab Project ID or a list of project IDs separated by a comma. The project ID is used to locate all the registries located within a specific project.

**NOTE:**

When both the group ID and project ID are provided, the system retrieves container images from all projects within the specified group as well as from the specified project.

If neither the group ID nor the project ID is provided, the system retrieves container images from all registries (across all groups and projects) accessible to the authenticated user or token in GitLab.

d. Enter the Api Domain. You must enter the base URL for the Gitlab API.

e. Under Authentication Method, enter your Gitlab Access Token.

f. (Optional) Expand Show Advanced Settings, and then enter the custom CA certificate in PEM format for Cortex to validate the Gitlab registry.

6. Select Next.

Scan with Broker VM

Security scanning in private networks is done using broker VM infrastructure when you select this mode.

**PREREQUISITE:**

- Set up and configure Broker VM
- Configure High Availability Cluster

1. Choose a Scan with Broker VM mode to initiate registry scanning. You can select either a standalone Broker VM or a High Availability (HA) Cluster.

2. Select Applicable Broker VMs.

Choose the appropriate Broker VM or Cluster from the list configured in your tenant.

**NOTE:**

- The list of Broker VMs displays only VMs that support registry scanning.
- The list of high-availability Clusters displays only clusters that contain at least one VM supporting registry scanning.
- The registry scanning status for each VM appears in brackets if it was previously activated for that specific VM.

If the list does not display any Broker VMs or Clusters, Add New Broker VM or Add New Cluster. For more details, see Set up and configure Broker VM.

3. Choose the relevant Account Type for Gitlab deployments:



## Gitlab Cloud (Saas)

- a. (Optional) Enter the Group Id. You can enter a single group ID or a list of group IDs separated by a comma. The group ID is used to locate all the registries within a specific group.
- b. (Optional) Enter the Project Id. You can enter a Gitlab Project ID or a list of project IDs separated by a comma. The project ID is used to locate all the registries located within a specific project.

### **NOTE:**

When both the group ID and project ID are provided, the system retrieves container images from all projects within the specified group as well as from the specified project.

If neither the group ID nor the project ID is provided, the system retrieves container images from all registries (across all groups and projects) accessible to the authenticated user or token in GitLab.

- c. Under Authentication Method, enter your Gitlab Access Token.

## Gitlab Self-Hosted

- a. Enter the Gitlab Registry URL.

If you are using a CA certificate, enter the server IP address instead of the registry url.

- b. (Optional) Enter the Group Id. You can enter a single group ID or a list of group IDs separated by a comma. The group ID is used to locate all the registries within a specific group.
- c. (Optional) Enter the Project Id. You can enter a Gitlab Project ID or a list of project IDs separated by a comma. The project ID is used to locate all the registries located within a specific project.

### **NOTE:**

When both the group ID and project ID are provided, the system retrieves container images from all projects within the specified group as well as from the specified project.

If neither the group ID nor the project ID is provided, the system retrieves container images from all registries (across all groups and projects) accessible to the authenticated user or token in GitLab.

- d. Enter the Api Domain. You must enter the base URL for the Gitlab API.

- e. Under Authentication Method, enter your Gitlab Access Token.

- f. (Optional) Expand Show Advanced Settings, and then enter the CA certificate in PEM format for Cortex to validate the Gitlab registry.

## 4. Select Next.

## 5. In Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tag: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images created or modified in the last few days. You can select a range of up to **90** days for the scan.

## 6. Select Save.

When the Gitlab data source is saved successfully, a new data connector is created, and the initial discovery scan is started. The connection process may take up to 15 minutes.

## 7. To check connector status and scan results, follow these steps:

- a. Navigate to Settings â Data Sources & Integrations.
- b. Find the Gitlab Container Registry instance from the list of 3rd Party Data Sources connectors, or use Search.
- c. In the Gitlab Container Registry instance row, select View Details. The Gitlab Instances page appears.
- d. On the Gitlab Instances page, you can filter results by any heading and value.
- e. Select an instance name to open the details pane. The details pane contains the following granular information:

Instance Details	Description
Status	Shows the status of the connector: Connected, Error, Warning, Disabled, or Pending.



Instance Details	Description
Applet Status on Broker VM	Shows the status of the Registry Scanner applet on the Broker VM page. This status is visible only when the Scan with Broker VM mode is selected.
Repositories	Shows the number of scanned repositories in the registry.
Scan Mode	Shows the selected scan mode for the data connector, such as Cloud Scan, Scan with Outpost, or Scan with Broker VM.
Security Capabilities	Shows a breakdown of the security capabilities enabled on the instance and their individual statuses. For example, select Registry Scanning when it shows a warning or error status to see the open errors and issues that contributed to the status.

## 8. Next Steps.

- After the scan is complete, you can view the list of scanned images on the Container Images Inventory page. For more details, see Container Image assets.
- If you have selected the Scan with Broker VM option, then a Registry Scanner applet is created on the selected Broker VM or Cluster. For details, see Verify Registry Scanner connection.

The screenshot shows the 'Broker VMs' section of the Data Connector interface. On the left, there's a sidebar with various configuration options like Upgrade Helper, General, Server Settings, Security Settings, Agent Configurations, Remote Repository Settings, Notifications, Cortex - Analytics, Data Broker, and Broker VMs. The 'Broker VMs' option is highlighted. The main area displays a table with columns: DEVICE NAME, STATUS, CLUSTER NAME, VERSION, CONFIGURATION STATUS, APPS, CPU USAGE, MEMORY USAGE, and DISK USAGE. One row is present, showing '81' as the device name, 'Connected' as the status, '28.0.96' as the version, 'Up to date' as the configuration status, and 'Registry Scanner' as the app. Resource usage at the bottom indicates 31% CPU, 47% Memory, and 0% Disk usage.

2.2.6.10.7.1 | Manage a Gitlab Container Registry connector

After you add a Gitlab Container Registry connector, you can modify the connector settings and configure the scanning scope to control which images are scanned in the connected registry.

To manage the connector, follow these steps:

- Select Settings → Data Sources.
- Find the Gitlab Container Registry instance from the list of 3rd Party Data Sources connectors, or use Search.
- In the Gitlab Container Registry instance row, select View Details. The Gitlab Instances page appears.
- On the Gitlab Instances page, you can filter the results by any heading and value. You can also create a new instance by selecting + Add Instance and following the onboarding wizard to define the settings.



5. You can perform actions on each Gitlab instance: For example, select the (pencil) icon to Edit the instance, or select the (three dots) icon to Exclude/Include image, Delete, or Disable the instance as follows:



(three



Action	Instructions
Edit	<p>Edit the Gitlab instance.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>If you selected Scan with Broker VM mode, you can't change to a different scan mode (such as Cloud Discovery or Scan with Outpost) when you edit the instance.</li> <li>When editing an instance configured for Scan with Broker VM, you must re-enter your authentication credentials, including Username, Password, and CA certificate.</li> </ul>
Exclude/Include images	Define conditions to automatically exclude or include specific images in scanning. Conditions can be based on Repository or Tags. These conditions apply automatically to newly discovered images in the account.
Delete	Removes the connector.
Disable	Stops image scanning for the connector without deleting it.

#### 2.2.6.10.8 | Connect Harbor registry

Cortex Cloud allows you to scan and secure your container images from vulnerabilities, malware, and secrets after you authenticate and connect your Harbor registry account.

##### How to connect Harbor

Follow the wizard to use the Harbor connector in Cortex Cloud to scan and secure container images.

1. Navigate to Settings â Data Sources & Integrations.
2. On the Add Data Source or Integrations page, click + Add New, search for Harbor, then hover over it and click Add.
3. The Instance Name is automatically populated. You can change it to a more meaningful name.
4. Choose the Scan Mode, and then follow the steps for that mode to configure the connection.

##### Cloud Scan

Security scanning is performed in the Cortex cloud environment when you select this mode.

1. Select the appropriate Cloud Provider and Region for the Cortex environment to use for registry scanning.  
As a best practice, choose the region closest to your registry deployment to achieve the best scanning throughput and potentially reduce cloud costs.
2. (Optional) Enable Allow access by IPâ€¢ s to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so the scanner can access the registry during the scanning process.
3. Enter the Registry URL.

Use the base URL of the Harbor registry. For example:

`https://harbor.yourdomain.com`

`https://harbor.yourdomain.com:8443` (with a specific port)

Alternatively, if you are using a CA certificate, enter the server IP address instead of the registry URL. For example:

`https://35.209.190.220`

`https://35.210.190.225:8084` (with a custom port)

4. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

If you have configured a robot account for automated access, use the robot accountâ€¢ s username and secret/token as authentication credentials.

For example: `docker login harbor.example.com -u 'robot$<your-robot-account-name>' -p '<your-robot-token>'`



5. (Optional) Expand Show advanced settings and then enter a custom CA certificate in PEM format for Cortex to validate the Harbor registry. Ensure that the Custom CA certificate that you use is not revoked by the issuing authority.

6. Select Next.

Scan with Outpost

Security scanning is done on infrastructure deployed to a cloud account that you own. This mode requires additional cloud provider permissions and may incur extra costs.

#### PREREQUISITE:

Ensure an Outpost is connected to your tenant.

1. Choose a Cloud Provider to initialize registry scanning.

#### NOTE:

If you choose Azure as the Cloud Provider, you must also select the Tenant Id. The Tenant Id is required to approve Cortex as an enterprise application in your Azure tenant.

2. Choose Outpost account to use for this instance. If no Outposts are shown, you can Create a new one. For more details, see Outposts.

#### NOTE:

If you choose Azure as the cloud provider, only Outposts associated with the selected tenant ID are displayed.

3. Select the Region where the registry is hosted.

4. (Optional) Enable Allow access by IPâ€ s if you want to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so that the scanner can access the registry during the scanning process.

5. Enter the Registry URL.

Use the base URL of the Harbor registry. For example:

`https://harbor.yourdomain.com`

`https://harbor.yourdomain.com:8443` (with a specific port)

Alternatively, if you are using a CA certificate, enter the server IP address instead of the registry URL. For example:

`https://35.209.190.220`

`https://35.209.190.220:8084` (with a custom port)

6. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

If you have configured a robot account for automated access, use the robot accountâ€ s username and secret/token as authentication credentials.

For example: `docker login harbor.example.com -u 'robot$<your-robot-account-name>' -p '<your-robot-token>'`

7. (Optional) Expand Show advanced settings and then enter a custom CA certificate in PEM format for Cortex to validate the Harbor registry. Ensure that the Custom CA certificate that you use is not revoked by the issuing authority.

8. Select Next.

Scan with Broker VM

Security scanning in private networks is performed using broker VM infrastructure when you select this mode.

#### PREREQUISITE:

Ensure one of the following is configured:

- Set up and configure Broker VM.
- Configure High Availability Cluster.

1. Choose a Scan with Broker VM mode to initiate registry scanning. You can select either a standalone Broker VM or a High Availability (HA) Cluster.

2. Select Applicable Broker VMs.

Choose the appropriate Broker VM or Cluster from the list configured in your tenant.

#### NOTE:

- The list of Broker VMs displays only VMs that support registry scanning.
- The list of high-availability Clusters displays only clusters that contain at least one VM supporting registry scanning.
- The registry scanning status for each VM appears in brackets if it was previously activated for that specific VM.



If the list does not display any Broker VMs or clusters, Add New Broker VM or Add New Cluster. For more details, see Set up and configure Broker VM.

3. Enter the Registry URL.

Use the base URL of the Harbor registry. For example:

`https://harbor.yourdomain.com`

`https://harbor.yourdomain.com:8443` (with a specific port)

Alternatively, if you are using a CA certificate, enter the server IP address instead of the registry URL. For example:

`https://35.209.190.220`

`https://35.210.190.225:8443` (with a custom port)

4. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

If you have configured a robot account for automated access, use the robot account's username and secret/token as authentication credentials.

For example: `docker login harbor.example.com -u 'robot$<your-robot-account-name>' -p '<your-robot-token>'`

5. (Optional) Expand Show advanced settings and then enter a custom CA certificate in PEM format for Cortex to validate the Harbor registry. Ensure that the Custom CA certificate that you use is not revoked by the issuing authority.

6. Select Next.

5. In the Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tag: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images that have been created in the last few days. You can select a range of up to 90 days for the scan.

6. Select Save.

When the Harbor data source is saved successfully, a new data connector is created, and the initial discovery scan begins. The connection process may take up to 15 minutes.

7. To check connector status and scan results, follow these steps:

- a. Navigate to Settings → Data Sources & Integrations.
- b. Find the Harbor instance from the list of 3rd Party Data Sources connectors, or use Search.
- c. In the Harbor instance row, select View Details. The Harbor Instances page appears.
- d. On the Harbor Instances page, you can filter results by any heading and value.
- e. Select an instance name to open the details pane. The details pane contains the following granular information:

Instance Details	Description
Status	Shows the status of the connector: Connected, Error, Warning, Disabled, or Pending.
Applet Status on Broker VM	Shows the status of the Registry Scanner applet on the Broker VM page. This status is visible only when the Scan with Broker VM mode is selected.
Repositories	Shows the number of scanned repositories in the registry.
Scan Mode	Shows the selected scan mode for the data connector, such as Cloud Scan, Scan with Outpost, or Scan with Broker VM.



Instance Details	Description
Security Capabilities	Shows a breakdown of the security capabilities enabled on the instance and their individual statuses. For example, select Registry Scanning when it shows a <b>warning</b> or <b>error</b> status to see the open errors and issues that contributed to the status.

## 8. Next Steps.

After the scan is complete, you can view the scanned details on the Container Images Inventory page. For more details, see Container Images assets.

If you have selected the Scan with Broker VM option, then a Registry Scanner applet is created on the selected Broker VM or Cluster. For details, see Verify Registry Scanner connection.

2.2.6.10.8.1 | Manage a Harbor connector

After successfully adding a connector, you can modify the connector settings and configure the scanning scope to control which images are scanned in the connected registry.

To manage the connector, follow these steps:

1. Select Settings → Data Sources.
2. Find the Harbor instance from the list of 3rd Party Data Sources connectors, or use Search.
3. In the Harbor instance row, select View Details. The Harbor Instances page appears.
4. On the Harbor Instances page, you can filter the results by any heading and value. You can also create a new instance by selecting + Add Instance and following the onboarding wizard to define the settings.



(pencil) icon to Edit the instance, or select the



5. You can also perform actions on each Harbor instance: for example, select the (three dots) icon to Exclude/Include images, Delete, or Disable the instance as follows:

Action	Instructions
Edit	<p>Edit the Harbor instance.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>If you selected Scan with Broker VM mode, you can't change to a different scan mode (such as Cloud Discovery or Scan with Outpost) when you edit the instance.</li> <li>When editing an instance configured for Scan with Broker VM, you must re-enter your authentication credentials, including Username, Password, and CA certificate.</li> </ul>
Exclude/Include images	Define conditions to automatically exclude or include specific images while scanning. Conditions can be based on Repository or Tags. These conditions apply automatically to newly discovered images in the account.
Delete	Removes the connector.
Disable	Stops image scanning for the connector without deleting it.



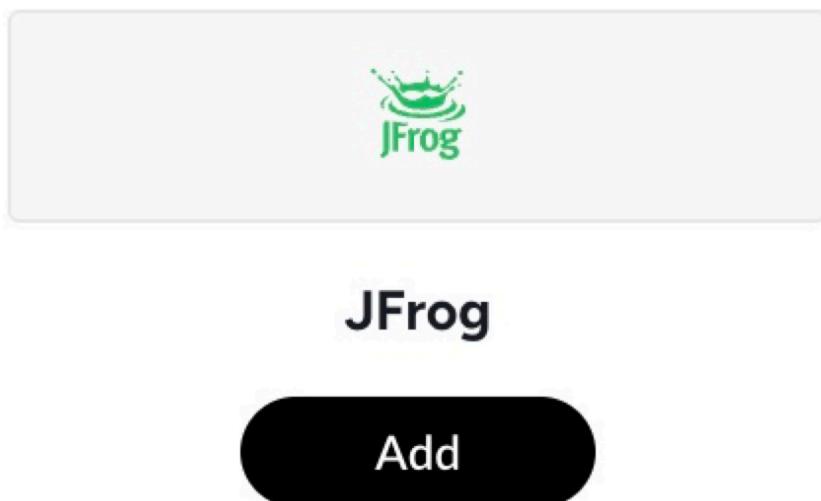
## 2.2.6.10.9 | Connect JFrog container registry

Cortex Cloud allows you to scan and secure your container images from vulnerabilities, malware, and secrets after you authenticate and connect your JFrog account. This process ensures robust artifact management and enhanced security.

### How to connect JFrog

Follow the wizard to connect your JFrog Container Registry with Cortex Cloud.

1. Navigate to Settings → Data Sources & Integrations.
2. On the Add Data Source or Integrations page, click + Add New, search for JFrog, then hover over it and click Add.



3. Select Image scanning to continue scanning your container images.

If you want to enable Software Composition Analysis (SCA) scanning for your private packages, then select Package resolution for code scanning and refer to JFrog Artifactory for more details.

4. The Instance Name is automatically populated. You can change it to a more meaningful name.
5. Choose the Scan Mode, and then follow the steps provided for that mode to configure the connection.

#### Cloud Scan

Security scanning is done in the Cortex cloud environment when you select this mode.

1. Select the appropriate Cloud Provider and Region for the Cortex environment to use for registry scanning.

As a best practice, choose the region closest to your registry deployment to achieve the best scanning throughput and potentially reduce cloud costs.

2. (Optional) Enable Allow access by IPs to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so the scanner can access the registry during the scanning process.

3. Choose the relevant Account Type for JFrog deployments:

#### JFrog Cloud (SaaS)

- a. Enter your JFrog Account Name.

For example, the scanner connects to <https://myaccount.jfrog.io>, where <myaccount> is your actual account name.

- b. Under Authentication Method, enter your JFrog account credentials (Username and Password) for authentication.

#### JFrog Self-Hosted



- a. Enter the JFrog Artifactory URL as the Registry URL.

For example, `https://artifactory.example.com/artifactory`, where `<artifactory.example.com>` is your server's domain or IP address.

- b. Under Authentication Method, enter your JFrog user credentials (Username and Password) for authentication.

- c. (Optional) Expand Show Advanced Settings, and then enter the CA certificate in PEM format for Cortex to validate the JFrog Artifactory registry.

4. Select Next.

#### Scan with Outpost

Security scanning is done on infrastructure deployed to a cloud account that you own. This mode requires additional cloud provider permissions and may incur extra costs.

#### **PREREQUISITE:**

Ensure an Outpost is connected to your tenant.

1. Choose a Cloud Provider to initialize registry scanning.

#### **NOTE:**

If you choose Azure as the Cloud Provider, you must also select the Tenant Id. The Tenant Id is required to approve Cortex as an enterprise application in your Azure tenant.

2. Choose Outpost account to use for this instance. If no Outposts are shown, you can Create a new one. For more details, see Outposts.

#### **NOTE:**

If you choose Azure as the cloud provider, only Outposts associated with the selected tenant ID are displayed.

3. Select the Region where the registry is hosted.

4. (Optional) Enable Allow access by IPs if you want to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so that the scanner can access the registry during the scanning process.

5. Choose the relevant Account Type for JFrog deployments:

#### JFrog Cloud (SaaS)

- a. Enter your JFrog Account Name.

For example, the scanner connects to `https://myaccount.jfrog.io`, where `<myaccount>` is your actual account name.

- b. Under Authentication Method, enter your JFrog account credentials (Username and Password) for authentication.

#### JFrog Self-Hosted

- a. Enter the JFrog Artifactory URL as the Registry URL.

For example, `https://artifactory.example.com/artifactory`, where `<artifactory.example.com>` is your server's domain or IP address.

- b. Under Authentication Method, enter your JFrog user credentials (Username and Password) for authentication.

- c. (Optional) Expand Show Advanced Settings, and then enter the custom CA certificate in PEM format for Cortex to validate the JFrog Artifactory registry.

6. Select Next.

#### Scan with Broker VM

Security scanning in private networks is done using broker VM infrastructure when you select this mode.

#### **PREREQUISITE:**

- Set up and configure Broker VM
- Configure High Availability Cluster

1. Choose a Scan with Broker VM mode to initiate registry scanning. You can select either a standalone Broker VM or a High Availability (HA) Cluster.

2. Select Applicable Broker VMs.

Choose the appropriate Broker VM or Cluster from the list configured in your tenant.

#### **NOTE:**



- The list of Broker VMs displays only VMs that support registry scanning.
- The list of high-availability Clusters displays only clusters that contain at least one VM supporting registry scanning.
- The registry scanning status for each VM appears in brackets if it was previously activated for that specific VM.

If the list does not display any Broker VMs or Clusters, Add New Broker VM or Add New Cluster. For more details, see Set up and configure Broker VM.

### 3. Choose the relevant Account Type for JFrog deployments:

JFrog Cloud (SaaS)

- Enter your JFrog Account Name.

For example, the scanner connects to <https://myaccount.jfrog.io>, where <myaccount> is your actual account name.

- Under Authentication Method, enter your JFrog account credentials (Username and Password) for authentication.

JFrog Self-Hosted

- Enter the JFrog Artifactory URL as the Registry URL.

For example, <https://artifactory.example.com/artifactory>, where <artifactory.example.com> is your server's domain or IP address.

- Under Authentication Method, enter your JFrog user credentials (Username and Password) for authentication.

- (Optional) Expand Show Advanced Settings.

- Select Use insecure connection to pull images if you want to allow image pull from the registry over an HTTP connection instead of HTTPS.

- Enter the CA certificate in PEM format for Cortex to validate the JFrog Artifactory registry.

### 4. Select Next.

### 6. In Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tag: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images created or modified in the last few days. You can select a range of up to 90 days for the scan.

### 7. Select Save.

When the JFrog data source is saved successfully, a new data connector is created, and the initial discovery scan is started. The connection process may take up to 15 minutes.

### 8. To check connector status and scan results, follow these steps:

- Navigate to Settings â— Data Sources & Integrations.
- Find the JFrog Artifactory instance from the list of 3rd Party Data Sources connectors, or use Search.
- In the JFrog Artifactory instance row, select View Details. The JFrog Artifactory Instances page appears.
- On the JFrog Artifactory Instances page, you can filter results by any heading and value.
- Select an instance name to open the details pane. The details pane contains the following granular information:

Instance Details	Description
Status	Shows the status of the connector: Connected, Error, Warning, Disabled, or Pending.
Applet Status on Broker VM	Shows the status of the Registry Scanner applet on the Broker VM page. This status is visible only when the Scan with Broker VM mode is selected.
Repositories	Shows the number of scanned repositories in the registry.



Instance Details	Description
Scan Mode	Shows the selected scan mode for the data connector, such as Cloud Scan, Scan with Outpost, or Scan with Broker VM.
Security Capabilities	Shows a breakdown of the security capabilities enabled on the instance and their individual statuses. For example, select Registry Scanning when it shows a warning or error status to see the open errors and issues that contributed to the status.

## 9. Next Steps.

- After the scan is complete, you can view the list of scanned images on the Container Images Inventory page. For more details, see Container Image assets.
- If you have selected the Scan with Broker VM option, then a Registry Scanner applet is created on the selected Broker VM or Cluster. For details, see Verify Registry Scanner connection.

DEVICE NAME	STATUS	CLUSTER NAME	VERSION	CONFIGURATION STATUS	APPS	CPU USAGE	MEMORY USAGE	DISK USAGE
B1	Connected		28.0.96	Up to date	Registry Scanner	31%	47%	0% (2.7GB/346.2GB)

2.2.6.10.9.1 | Manage a JFrog connector

After you add a JFrog connector, you can modify the connector settings and configure the scanning scope to control which images are scanned in the connected registry.

To manage the connector, follow these steps:

- Select Settings → Data Sources.
- Find the JFrog instance from the list of 3rd Party Data Sources connectors, or use Search.
- In the JFrog instance row, select View Details. The JFrog Artifactory Instances page appears.
- On the JFrog Artifactory Instances page, you can filter results by any heading and value. You can also create a new instance by selecting + Add Instance and following the onboarding wizard to define the settings.



(pencil) icon to Edit the instance, or select the

5. You can also perform actions on each JFrog Artifactory instance: for example, select the



(three dots) icon to Exclude/Include images, Delete, or Disable the instance as follows:

Action	Instructions
Edit	<p>Edit the JFrog Artifactory instance.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>If you selected Scan with Broker VM mode, you can't change to a different scan mode (such as Cloud Discovery or Scan with Outpost) when you edit the instance.</li> <li>When editing an instance configured for Scan with Broker VM, you must re-enter your authentication credentials, including Username, Password, and CA certificate.</li> </ul>



Action	Instructions
Exclude/Include images	Define conditions to automatically exclude or include specific images while scanning. Conditions can be based on Repository or Tags. These conditions apply automatically to newly discovered images in the account.
Delete	Removes the connector.
Disable	Stops image scanning for the connector without deleting it.

#### 2.2.6.10.10 | Connect Sonatype Nexus registry

Configure Cortex Cloud to scan your Nexus Registry. This allows Cortex to list all container registries or images, and secure them from vulnerabilities, malware, and secrets.

##### How to connect Nexus registry

Follow the wizard to use the Sonatype Nexus registry connector in Cortex Cloud.

1. Navigate to Settings → Data Sources & Integrations.
2. On the Add Data Source or Integrations page, click + Add New, search for Sonatype, then hover over it and click Add.
3. The Instance Name is automatically populated. You can change it to a more meaningful name.
4. Choose the Scan Mode, and then follow the steps for that mode to configure the connection.

##### Cloud Scan

Security scanning is done in the Cortex cloud environment when you select this mode.

1. Select the appropriate Cloud Provider and Region for the Cortex environment to use for registry scanning.

As a best practice, choose the region closest to your registry deployment to achieve the best scanning throughput and potentially reduce cloud costs

2. (Optional) Enable Allow access by IP's to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so the scanner can access the registry during the scanning process.

3. Enter the Registry URL.

Enter the hostname, or Fully Qualified Domain Name (FQDN), and the connector port for the Nexus registry's login server in the following format:

```
https://<hostname>:<connector_port>,
<hostname> - unique name assigned when the Nexus registry was created
<connector_port> - https connector for the specific Nexus repository.
```

For example:

```
https://ec2-100-25-223-135.compute-1.amazonaws.com:8083
```

```
https://35.209.190.220:8084
```

##### NOTE:

If you are using a CA certificate, enter the server IP address instead of the registry url.

4. Under Authentication Method, enter the Username and Password of the registry that you want to connect.
5. (Optional) Expand Show advanced settings and then enter a custom CA certificate in PEM format for Cortex to validate the Nexus registry.
6. Select Next.

##### Scan with Outpost

Security scanning is done on infrastructure deployed to a cloud account that you own. This mode requires additional cloud provider permissions and may incur extra costs.

##### PREREQUISITE:



## Ensure an Outpost is connected to your tenant. Outposts

1. Choose a Cloud Provider to initialize registry scanning.

### NOTE:

If you choose Azure as the Cloud Provider, you must also select the Tenant Id. The Tenant Id is required to approve Cortex as an enterprise application in your Azure tenant.

2. Choose Outpost account to use for this instance. If no Outposts are shown, you can Create a new one. For more details, see Outposts.

### NOTE:

If you choose Azure as the cloud provider, only Outposts associated with the selected tenant ID are displayed.

3. Select the Region where the registry is hosted.

4. (Optional) Enable Allow access by IPâ€ s if you want to specify a static IP address for the scanner to use. Make sure the static IP is allowed through your firewall so that the scanner can access the registry during the scanning process.

5. Enter the Registry URL.

Enter the hostname, or Fully Qualified Domain Name (FQDN), and the connector port for the Nexus registryâ€ s login server in the following format:

<[https://<hostname>:<connector\\_port>](https://<hostname>:<connector_port>)>

<hostname>â€ unique name assigned when the registry was created.

<connector\_port>â€ https connector for the specific Nexus repository.

For example:

<https://ec2-100-25-223-135.compute-1.amazonaws.com:8083>

<https://35.209.190.220:8084>

### NOTE:

If you are using a CA certificate, enter the server IP address instead of the registry URL.

6. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

7. (Optional) Expand Show advanced settings and then enter a custom CA certificate in PEM format for Cortex to validate the Nexus registry.

8. Select Next.

Scan with Broker VM

Security scanning in private networks is done using broker VM infrastructure when you select this mode.

## PREREQUISITE:

Ensure one of the following is configured:

- Set up and configure Broker VM.
- Configure High Availability Cluster.

1. Choose a Scan with Broker VM mode to initiate registry scanning. You can select either a standalone Broker VM or a High Availability (HA) Cluster.

2. Select Applicable Broker VMs.

Choose the appropriate Broker VM or Cluster from the list configured in your tenant.

### NOTE:

- The list of Broker VMs displays only VMs that support registry scanning.
- The list of high-availability Clusters displays only clusters that contain at least one VM supporting registry scanning.
- The registry scanning status for each VM appears in brackets if it was previously activated for that specific VM.

If the list does not display any Broker VMs or clusters, Add New Broker VM or Add New Cluster. For more details, see Set up and configure Broker VM.

3. Enter the Registry URL.

Enter the hostname, or Fully Qualified Domain Name (FQDN), and the connector port for the Nexus registryâ€ s login server in the following format:

<[https://<hostname>:<connector\\_port>](https://<hostname>:<connector_port>)>

<hostname>â€ unique name assigned when the registry was created.



<connector\_port> https connector for the specific Nexus repository.

For example:

<https://ec2-100-25-223-135.compute-1.amazonaws.com>

<https://35.209.190.220:8084>

**NOTE:**

If you are using a CA certificate, enter the server IP address instead of the registry URL.

4. Under Authentication Method, enter the Username and Password of the registry that you want to connect.

5. (Optional) Expand Show advanced settings and then enter a custom CA certificate in PEM format for Cortex to validate the Nexus registry.

6. Select Next.

5. In the Initial Scan Configuration, set your scanning process to focus on recently added or modified container images and exclude older ones that do not align with your current scanning objectives. This setting helps avoid unnecessary scans. Choose one of the following options:

- All: Scans all container images, including all versions (tags), in all discovered repositories.
- Latest Tag: Scans only images tagged 'latest' in all discovered repositories.
- Days Modified: Scans container images that have been created in the last few days. You can select a range of up to 90 days for the scan.

6. Select Save.

When the Sonatype data source is saved successfully, a new data connector is created, and the initial discovery scan begins. The connection process may take up to 15 minutes.

7. To check the connector status and scan results, follow these steps:

- Go to Settings → Data Sources & Integrations.
- Find the Sonatype instance from the list of 3rd Party Data Sources connectors, or use Search.
- In the Sonatype instance row, select View Details. The Sonatype Instances page appears.
- On the Sonatype Instances page, you can filter results by any heading and value.
- Select an instance name to open the details pane. The details pane contains the following granular information:

Instance Details	Description
Status	Shows the status of the connector: Connected, Error, Warning, Disabled, or Pending.
Applet Status on Broker VM	Shows the status of the Registry Scanner applet on the Broker VM page. This status is visible only when the Scan with Broker VM mode is selected.
Repositories	Shows the number of scanned repositories in the registry.
Scan Mode	Shows the selected scan mode for the data connector, such as Cloud Scan, Scan with Outpost, or Scan with Broker VM.
Security Capabilities	Shows a breakdown of the security capabilities enabled on the instance and their individual statuses. For example, select Registry Scanning when it shows a warning or error status to see the open errors and issues that contributed to the status.

8. Next Steps.



- After the scan is complete, you can view the list of scanned images on the Container Images Inventory page. For more details, see Container Images assets.
- If you have selected the Scan with Broker VM option, then a Registry Scanner applet is created on the selected Broker VM or Cluster. For details, see Verify Registry Scanner connection.

DEVICE NAME	STATUS	CLUSTER NAME	VERSION	CONFIGURATION STATUS	APPS	CPU USAGE	MEMORY USAGE	DISK USAGE
81	Connected		28.0.96	Up to date	Registry Scanner	31%	47%	0% (2.7GB/346.2GB)

#### 2.2.6.10.10.1 | Manage a Sonatype connector

After you add a Sonatype connector, you can modify the connector settings and configure the scanning scope to control which images are scanned in the connected registry.

To manage the connector, follow these steps:

- Select Settings  $\rightarrow$  Data Sources.
- Find the Sonatype instance from the list of 3rd Party Data Sources connectors, or use Search.
- In the Sonatype instance row, select View Details. The Sonatype Instances page appears.
- On the Sonatype Instances page, you can filter results by any heading and value. You can also create a new instance by selecting + Add Instance and following the onboarding wizard to define the settings.



5. You can also perform actions on each Sonatype instance: for example, select the (pencil) icon to Edit the instance, or select the (three dots) icon to Exclude/Include images, Delete, or Disable the instance as follows:



Action	Instructions
Edit	<p>Edit the Sonatype instance.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>If you had selected Scan with Broker VM mode, you can't change to a different scan mode (such as Cloud Discovery or Scan with Outpost) when you edit the instance.</li> <li>When editing an instance configured for Scan with Broker VM, you must re-enter your authentication credentials, including Username, Password, and CA certificate.</li> </ul>
Exclude/Include images	Define conditions to automatically include or exclude specific images while scanning. Conditions can be based on Repository or Tags. These conditions apply automatically to newly discovered images in the account.
Delete	Removes the connector.
Disable	Stops image scanning for the connector without deleting it.

#### 2.2.6.11 | Cloud service provider permissions

Abstract

Grant the correct cloud service provider permissions for Cortex Cloud.

When you set up Cortex Cloud to collect data from your cloud environments, the onboarding wizard will ensure that the correct permissions are granted for Cortex Cloud. The following tables list the permissions required for each of the options available in the onboarding wizards.



Review the permissions required for each cloud service provider:

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud Infrastructure

#### 2.2.6.11.1 | Amazon Web Services provider permissions

##### Abstract

List of Amazon Web Services provider permissions for Cortex Cloud.

When onboarding Amazon Web Services, Cortex Cloud creates an authentication template that requests the permissions needed for monitoring your cloud environment. Depending on which security capabilities you select in the onboarding wizard, different permissions are requested. The following tables are organized by security module and list the CSP permissions being requested as well as the purpose (and where relevant, the scope):

- Agentless Disk Scanning
- DSPM
- Discovery Engine
- Registry Scan
- Log Collection
- Automations
- Serverless Scan
- Outposts

##### Agentless Disk Scanning

Permission	Scope	Purpose
ec2:CopyImage	Images created with managed_by: <b>paloaltonetworks</b> tag	Create disk from Image
ec2:CopySnapshot	Snapshots copied with managed_by: <b>paloaltonetworks</b> tag	Re-encrypt snapshot with Palo Alto Network's KMS key
ec2>CreateSnapshot	Snapshots created with managed_by: <b>paloaltonetworks</b> tag	Create disk snapshot
ec2>CreateTags	Only as part of CopyImage, CreateSnapshot and CopySnapshot operations	Add tags for permission scoping and cost visibility
ec2>DeleteSnapshot	Snapshots with managed_by: <b>paloaltonetworks</b> tag	Delete scanned snapshot
ec2:DeregisterImage	Images with managed_by: <b>paloaltonetworks</b> tag	Delete ephemeral re-encrypted image
ec2:DescribeImages	Images with managed_by: <b>paloaltonetworks</b> tag	Retrieve image creation status
ec2:DescribeSnapshots	Snapshots with managed_by: <b>paloaltonetworks</b> tag	Retrieve snapshot creation status



Permission	Scope	Purpose
ec2:ModifySnapshotAttribute	<ul style="list-style-type: none"> <li>Snapshots with managed_by: <code>paloaltonetworks</code> tag</li> <li>The snapshots can be shared only with the outpost account</li> </ul>	Share snapshot with the outpost account
kms:CreateGrant	<ul style="list-style-type: none"> <li>Palo Alto Network's and customer KMS keys</li> <li>Only EC2 services can use this permission</li> </ul>	Create a new grant for a customer master key (CMK), such as to allow the re-encrypt operation
kms:DescribeKey	<ul style="list-style-type: none"> <li>Palo Alto Network's KMS key</li> <li>Only EC2 services can use this permission</li> </ul>	Retrieve detailed information about a customer master key (CMK), such as to allow and support a re-encrypt operation
kms:GenerateDataKeyWithoutPlaintext	<ul style="list-style-type: none"> <li>Palo Alto Network's KMS key</li> <li>Only EC2 services can use this permission</li> </ul>	Generate a data key for client-side encryption, such as to allow and support a re-encrypt operation

DSPM

Permission	Scope	Purpose
arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess	All DynamoDB resources in the account	Grant read-only access to the MemoryDB resources
cloudwatch:GetMetricStatistics	All DynamoDB tables in the account	Get usage statistics, which are used to ensure that classification processes do not interfere with production environments
dynamodb:DescribeTable	All DynamoDB tables in the account	Get information about DynamoDB tables in the account
dynamodb:Scan	All DynamoDB tables in the account	Access data in DynamoDB tables in the account for performing environment-wide discovery and data classification, ensuring no assets are left unmonitored
iam:PassRole	Palo Alto Networks scanner role	Create export tasks for RDS snapshots
kms:CreateGrant	KMS keys in the account	Enable the created EC2 instance to send a CreateGrant request to the AWS KMS for a customer master key (CMK) so that it, for example, can share an encrypted snapshot with an outpost account (re-encryption)
kms:DescribeKey	KMS keys in the account	Retrieve detailed information about a customer master key (CMK), such as to allow and support a re-encrypt operation



Permission	Scope	Purpose
kms:GenerateDataKeyWithoutPlaintext	AWS account	Generate a data key for client-side encryption, such as encrypting a created snapshot
rds:AddTagsToResource	All RDS database instances and clusters in the account	Create unique tags for the created RDS resourceCreateDBS snapshots in order to find them at a later stage. This permission is needed for performing environment-wide discovery and data classification, ensuring no assets are left unmonitored.
rds:CancelExportTask	All RDS database instances and clusters in the account	Cancel export tasks in case of failure or termination of the classification process. This permission is needed for performing environment-wide discovery and data classification, ensuring no assets are left unmonitored.
rds>CreateDBClusterSnapshot	All RDS database instances and clusters in the account	Create a snapshot for the RDS clusters that need to be scanned at a later stage. This permission is needed for performing environment-wide discovery and data classification, ensuring no assets are left unmonitored.
rds>CreateDBSnapshot	All RDS database instances and clusters in the account	Create a snapshot for the RDS instances that need to be scanned at a later stage. This permission is needed for performing environment-wide discovery and data classification, ensuring no assets are left unmonitored.
rds>DeleteDBSnapshot	Snapshots created by Palo Alto Networks	Delete snapshots created as part of the classification process
rds:Describe*	All RDS database instances and clusters in the account	Describe permissions to enable Palo Alto Networks to get metadata information on the RDS instance
rds>List*	All RDS database instances and clusters in the account	List permissions to enable Palo Alto Networks to understand which instances and snapshots exist in the account
rds:StartExportTask	All RDS database instances and clusters in the account	Export data from the snapshots to an S3 bucket
s3>DeleteObject*	Buckets created by Palo Alto Networks	Delete stale objects that were created
s3:Get*	All S3 buckets in the account	Enable Palo Alto Networks to read data within S3 buckets
s3>List*	All S3 buckets in the account	Allow the listing of all S3 objects



Permission	Scope	Purpose
s3:PutObject*	Buckets created by Palo Alto Networks	Write data to an object in Palo Alto Networks' bucket to export data from the RDS instances

Discovery Engine

Permission	Purpose
apigateway:GetDomainNames	Retrieve API Gateway custom domain names
arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess	Grant read-only access to Amazon Simple Queue Service (SQS), allowing the retrieval of SQS queue attributes, messages, and configurations
arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess	Grant read-only access to AWS organizations, allowing the ability to list and view configurations, metadata, and logs across AWS organizations
arn:aws:iam::aws:policy/ReadOnlyAccess	Grant read-only access to AWS services and resources, allowing the ability to list and view configurations, metadata, and logs across AWS resources
arn:aws:iam::aws:policy/SecurityAudit	Grant access to read security configuration metadata, allowing users to inspect IAM configurations, security policies, CloudTrail logs, and other security-relevant settings
bedrock-agent:GetAgents	Retrieve details of Bedrock agents
bedrock-agent:GetDataSource	Retrieve details of a specific data source
bedrock-agent:GetKnowledgeBases	Retrieve details of knowledge bases
bedrock-agent>ListAgentAliases	List aliases associated with an agent
bedrock-agent>ListAgentKnowledgeBases	List knowledge bases linked to agents
bedrock-agent>ListAgents	List all Bedrock agents
bedrock-agent>ListDataSource	List available data sources
bedrock>ListCustomModel	List custom AI models in Amazon Bedrock
cloudcontrolapi:GetResource	Retrieve the state of an AWS resource managed via the Cloud Control API
cloudformation:AmazonCloudFormation	General permission related to CloudFormation resource management
cloudformation:StackStatus	Retrieve the status of CloudFormation stacks



Permission	Purpose
cloudformation:StackSummary	Provide a summary of CloudFormation stacks
cloudwatch:describeAlarms	Describe all alarms currently owned by the user's account
comprehendmedical>ListEntitiesDetectionV2Jobs	List entity detection jobs in Comprehend Medical
configservice:DescribeDeliveryChannels	Retrieve details of AWS Config delivery channels
connect-campaigns:DescribeCampaign	Describe a specific campaign
connect-campaigns>ListCampaigns	Provide a summary of all campaigns
controltower>ListLandingZones	List landing zones for AWS Control Tower
controltower>ListTagsForResource	List tags for AWS Control Tower resources
DirectConnect: <sup>*</sup>	Enable all GET permissions for AWS Direct Connect
DirectConnect:DescribeConnections	List Direct Connect connections and their attributes
DirectConnect:DescribeDirectConnectGateways	Retrieve details about Direct Connect gateway
DirectConnect:DescribeVirtualInterfaces	Display all virtual interfaces for an AWS account
DS:DescribeDirectories	Grant read access to directory details in AWS Directory Service
DS>ListTagsForResource	List tags associated with a specific AWS Directory Service resource
elasticfilesystem:DescribeFileSystemPolicy	Retrieve policies associated with an EFS file system
elasticloadbalancingv2:DescribeSSLPolicies	Retrieve details of ELB SSL policies
forecast>ListTagsForResource	List tags associated with an Amazon Forecast resource
glue:GetConnections	List connection configurations for AWS Glue
glue:GetResourcePolicies	Retrieve Glue Data Catalog policies
Glue:GetSecurityConfigurations	Retrieve security configurations for AWS Glue
iam:AmazonIdentityManagement	General IAM access for identity and access management



<b>Permission</b>	<b>Purpose</b>
iam:AttachedPolicy	Retrieve policies attached to IAM identities
iam:PolicyRole	List IAM roles associated with a policy
iam:RoleDetail	Retrieve detailed information about IAM roles
lakeformation:*	Enable all GET permissions for AWS Lake Formation
memorydb:DescribeSnapshots	Retrieve information about cluster snapshots
memorydb:DescribeSubnetGroups	Retrieve a list of subnet group
opensearchserverless>ListCollections	List collections in OpenSearch Serverless
s3-control:GetAccessPointPolicy	Retrieve an S3 access point policy
s3-control:GetAccessPointPolicyStatus	Retrieve the status of an access point policy
s3-control:GetPublicAccessBlock	Retrieve the public access block configuration for an account
s3-control>ListAccessPoints	List S3 access points that are owned by the current account that's associated with the specified bucket
servicecatalog-appregistry>ListApplications	List applications in AWS AppRegistry
servicecatalog-appregistry>ListAttributeGroups	List attribute groups in AppRegistry
workspaces:*	Enable all GET permissions for Amazon WorkSpaces
WorkSpaces:DescribeTags	List tags associated with WorkSpaces resources
WorkSpaces:DescribeWorkspaceDirectories	Retrieve details about WorkSpaces directories
WorkSpaces:DescribeWorkspaces	List and describe WorkSpaces instances

Registry Scan

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
ecr:BatchGetImage	All ECR images in the account	Get detailed information for an image, required to pull the image



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
ecr:GetDownloadUrlForLayer	All ECR images in the account	Used in the process of pulling images, to fetch the URL for the various layers that make up the image
ecr:GetAuthorizationToken	All ECR images in the account	Used to create a login token for pulling images from ECR

Log Collection

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
kms:Decrypt	The specific KMS key used for CloudTrail encryption in the current account and region	Decrypt ciphertext using a customer master key (CMK)
s3:GetObject	The Cortex CloudTrail logs S3 bucket and its objects	Grant permission to download objects from the configured S3 bucket
s3>ListBucket	The Cortex CloudTrail logs S3 bucket and its objects	Grant permission to see the specific bucket
sqS:ChangeMessageVisibility	The specific Cortex CloudTrail logs SQS queue	Manage log message visibility during processing, such as to extend processing time for log messages to prevent timeouts
sqS:DeleteMessage	The specific Cortex CloudTrail logs SQS queue	Grant permission to delete consumed messages, preventing re-processing of the same message
sqS:GetQueueAttributes	The specific Cortex CloudTrail logs SQS queue	Grant permission to retrieve SQS queue attributes, used for metrics and monitoring
sqS:ReceiveMessage	The specific Cortex CloudTrail logs SQS queue	Grant permission to consume messages from the SQS queue to receive bucket notification messages

Automations

Retrieve configuration details and metadata for a Lambda function R and downloads the source code

<b>Permission</b>	<b>Command That Requires This Permission</b>	<b>Purpose</b>
acm:UpdateCertificateOptions	aws-acm-certificate-options-update	Update the options for a specified ACM certificate
elasticloadbalancing:ModifyLoadBalancerAttributes	aws-elb-load-balancer-attributes-modify	Modify the attributes of a specified load balancer
rds:AddTagsToResource		Add unique tags to a specific Amazon RDS resource, such as to find them at a later stage



Permission	Command That Requires This Permission	Purpose
rds>CreateTenantDatabase		Create a new tenant database within a RDS DB instance
rds>ModifyDBCluster	aws-rds-db-cluster-modify	Modify a DB cluster for remediation of an issue detected due to the rule: AWS RDS DB Cluster Publicly Accessible
rds>ModifyDBClusterSnapshotAttribute	aws-rds-db-cluster-snapshot-attribute-modify	Modify DB cluster snapshot attributes for remediation of an issue detected due to the rule: AWS RDS DB Cluster Snapshot Publicly Accessible
rds>ModifyDBInstance	aws-rds-db-instance-modify	Modify a DB instance for remediation of an issue detected due to the rule: AWS RDS DB Instance Publicly Accessible
rds>ModifyDBSnapshotAttribute	aws-rds-db-snapshot-attribute-modify	Modify DB snapshot attributes for remediation of an issue detected due to the rule: AWS RDS DB Snapshot Publicly Accessible
rds>ModifyEventSubscription	aws-rds-event-subscription-modify	Modify an existing RDS event subscription
s3>PutBucketAcl	aws-s3-bucket-acl-put	Block public ACLs for remediation of an issue detected due to the rule: S3 Bucket Public Read Access. By applying a different policy, the permission can be used to explicitly deny public access or removes public access entirely.
s3>PutBucketLogging	aws-s3-bucket-logging-put	Configure server access logging for remediation of an issue detected due to the rule: AWS S3 Bucket Logging Disabled
s3>PutBucketPolicy	aws-s3-bucket-policy-put	Block public policy for remediation of an issue detected due to the rule: S3 Bucket Policy Public Access
s3>PutBucketPublicAccessBlock	aws-s3-public-access-block-update	Block public access for remediation of an issue detected due to the rule: AWS S3 Bucket Public Access Block Disabled
s3>PutBucketVersioning	aws-s3-bucket-versioning-put	Enable versioning for remediation of an issue detected due to the rule: AWS S3 Bucket Versioning Disabled
s3>GetBucketPolicy	aws-s3-bucket-policy-get	Retrieve the resource-based access policy attached to an Amazon S3 bucket
s3>GetBucketPublicAccessBlock	aws-s3-public-access-block-get	Block public access for remediation of an issue detected due to the rule: AWS S3 Bucket Public Access Block Disabled



Permission	Command That Requires This Permission	Purpose
s3:GetEncryptionConfiguration	aws-s3-bucket-encryption-get	Retrieve the default server-side encryption settings applied to a bucket
s3>DeleteBucketPolicy	aws-s3-bucket-policy-delete	Remove the entire access policy associated with a bucket
s3:PutObject	aws-s3-file-upload	Upload a new object or replace an existing object within a bucket
s3:GetObject	aws-s3-file-download	Download an object from a bucket
s3:GetBucketWebsite	aws-s3-bucket-website-get	Retrieve of the configuration details for static website hosting on a bucket
s3:GetBucketAcl	aws-s3-bucket-acl-get	Retrieve of the Access Control List (ACL) that controls access to a bucket
s3>DeleteBucketWebsite	aws-s3-bucket-website-delete	Remove the static website configuration from a bucket
s3:PutBucketOwnershipControls	aws-s3-bucket-ownership-controls-put	Define and enforce the ownership controls configuration for a bucket
ec2:AuthorizeSecurityGroupIngress	aws-ec2-security-group-ingress-authorize	Allow inbound network access for remediation of an issue detected due to the rule: AWS EC2 Security Group with Ingress Rule Not Authorized
ec2:ModifyImageAttribute	aws-ec2-image-attribute-modify	Revoke image launch permissions for remediation of an issue detected due to the rule: AWS EC2 AMI Publicly Accessible
ec2:ModifyInstanceAttribute	aws-ec2-instance-attribute-modify	Disassociate a security group for mitigation of an issue detected due to the rule: AWS EC2 instance with network path from the internet (0.0.0.0/0)
ec2:ModifyInstanceMetadataOptions	aws-ec2-instance-metadata-options-modify	Modify EC2 instance metadata options for remediation of an issue detected due to the rule: AWS EC2 Instance Not Using IMDSv2
ec2:ModifySnapshotAttribute	aws-ec2-snapshot-attribute-modify	Revoke snapshot restore permissions for remediation of an issue detected due to the rule: AWS EC2 Snapshot Publicly Accessible
ec2:RevokeSecurityGroupEgress	aws-ec2-security-group-egress-revoke	Block outbound traffic for remediation of an issue detected due to the rule: AWS EC2 instance with network path to the internet (0.0.0.0/0)



<b>Permission</b>	<b>Command That Requires This Permission</b>	<b>Purpose</b>
ec2:RevokeSecurityGroupIngress	aws-ec2-security-group-ingress-revoke	Block inbound network access for remediation of an issue detected due to the rule: AWS EC2 instance with network path from the internet (0.0.0.0/0)
ec2:CreateSecurityGroup	aws-ec2-security-group-create	Create a new network security group
ec2:DeleteSecurityGroup	aws-ec2-security-group-delete	Delete an existing network security group
ec2:DescribeSecurityGroups	aws-ec2-security-groups-describe	Retrieve information about the security groups in the account
ec2:DescribeInstances	aws-ec2-instances-describe	Retrieve information about the EC2 instances in the account
ec2:AuthorizeSecurityGroupEgress		Authorize outbound network access for a security group
ec2:StartInstances	aws-ec2-instances-start	Start one or more stopped EC2 instances
ec2:StopInstances	aws-ec2-instances-stop	Stop one or more stopped EC2 instances
ec2:TerminateInstances	aws-ec2-instances-terminate	Terminate one or more running EC2 instances
ec2:RunInstances	aws-ec2-instances-run	Running (launch) a new EC2 instance
ec2:CreateTags	aws-ec2-tags-create	Add tags for an EC2 instance
ec2:CreateSnapshot	aws-ec2-snapshot-create	Create a point-in-time snapshot of an EBS volume/disk
ec2:DescribeVpcs	aws-ec2-vpcs-describe	Retrieve information about the VPCs in the account
ec2:DescribeSubnets	aws-ec2-subnets-describe	Retrieve information about the subnets in the account
ec2:DescribeIpamResourceDiscoveries	aws-ec2-ipam-resource-discoveries-describe	Retrieve details about IPAM resource discovery configurations
ec2:DescribeIpamResourceDiscoveryAssociations	aws-ec2-ipam-resource-discovery-associations-describe	Retrieve details about associations between IPAM and resource discoveries
ec2:DescribeImages	aws-ec2-latest-ami-get	Retrieve information about AMIs or container images



<b>Permission</b>	<b>Command That Requires This Permission</b>	<b>Purpose</b>
ec2:CreateNetworkAcl	aws-ec2-network-acl-create	Create a new network access control list (ACL)
ec2:GetIpamDiscoveredPublicAddresses	aws-ec2-ipam-discovered-public-addresses-get	Retrieve discovered public IP addresses from IPAM
ec2:ModifySubnetAttribute	aws-ec2-subnet-attribute-modify	Modify a specific attribute of a subnet
cloudtrail:UpdateTrail	aws-cloudtrail-trail-update	Disable CloudTrail log file validation for remediation of an issue detected due to the rule: AWS CloudTrail Log File Validation Disabled
cloudtrail:StartLogging	aws-cloudtrail-logging-start	Start logging for remediation of an issue detected due to the rule: AWS CloudTrail Logging Stopped
cloudtrail:DescribeTrails	aws-cloudtrail-trails-describe	Retrieve information about the trails configured in CloudTrail
eks:UpdateClusterConfig	aws-eks-cluster-config-update	Update EKS cluster configuration for remediation of an issue detected due to the rule: AWS EKS Cluster Public Access Enabled
eks:DescribeCluster	aws-eks-cluster-describe	Retrieve detailed information about a specific EKS cluster
eks:AssociateAccessPolicy	aws-eks-access-policy-associate	Associate an access policy with an EKS cluster
ecs:UpdateClusterSettings	aws-ecs-cluster-settings-update	Modifiy the settings for an existing ECS cluster
iam:DeleteLoginProfile	aws-iam-login-profile-delete	Delete a login profile for remediation of an issue detected due to the rule: AWS IAM User with Active Console Password
iam:GetAccountAuthorizationDetails		Retrieve information about all IAM users, roles, policies, and groups in the account
iam:GetAccountPasswordPolicy	aws-iam-account-password-policy-get	Get account password policy for investigation of an issue detected due to the rule: AWS IAM Account Password Policy Not Configured
iam:PassRole		Pass an IAM role to an AWS service by an entity
iam:PutUserPolicy	aws-iam-user-policy-put	Suspend access for user for mitigation of an issue detected due to the rule: AWS IAM Users with Administrator Access Permissions



<b>Permission</b>	<b>Command That Requires This Permission</b>	<b>Purpose</b>
iam:RemoveRoleFromInstanceProfile	aws-iam-role-from-instance-profile-remove	Remove role from instance profile for remediation of an issue detected due to the rule: AWS EC2 with IAM instance profile
iam:UpdateAccessKey	aws-iam-access-key-update	Deactivate access key for remediation of an issue detected due to the rule: AWS IAM User Active Access Keys Unused for 90 days
iam:UpdateAccountPasswordPolicy	aws-iam-account-password-policy-update	Configure account password policy for remediation of an issue detected due to the rule: AWS IAM Account Password Policy Not Configured
kms>CreateGrant		Enable the created EC2 instance to send a CreateGrant request to the AWS KMS so that it can share the encrypted snapshot, such as with an outpost account (re-encryption)
kms:Decrypt		Decrypt ciphertext using a customer master key (CMK)
kms:DescribeKey		Retrieve detailed information about a customer master key (CMK)
kms:GenerateDataKey		Generate a data key for client-side encryption
kms:EnableKeyRotation	aws-kms-key-rotation-enable	Activate automatic rotation for a customer master key (CMK)
lambda:GetFunctionConfiguration		Retrieve the configuration details for a Lambda function
lambda:GetFunctionUrlConfig	aws-lambda-function-url-config-get	Retrieve the configuration details for a Lambda function URL
lambda:GetPolicy	aws-lambda-policy-get	Retrieve the access policy associated with a Lambda function
lambda:InvokeFunction	aws-lambda-invoke	Execute a specified Lambda function
lambda:UpdateFunctionUrlConfig	aws-lambda-function-url-config-update	Update the configuration details for a Lambda function URL
secretsmanager>CreateSecret		Create a new secret in Secrets Manager
secretsmanager:RotateSecret		Set up or initiate rotation for a secret



<b>Permission</b>	<b>Command That Requires This Permission</b>	<b>Purpose</b>
secretsmanager:TagResource		Add tags to a secret or resource in Secrets Manager
ce:GetCostAndUsage		Retrieve detailed cost and usage data for the account
ce:GetCostForecast		Retrieve a forecast of future costs and usage
budgets:DescribeBudgets		Retrieve the configured budgets for the account
budgets:DescribeNotificationsForBudget		Retrieve the notification details associated with a specific budget

Serverless Scan

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
lambda:GetFunction	All Lambda functions in the account	View the configuration and metadata of a specific Lambda function and download the source code
lambda:GetFunctionConfiguration	All Lambda functions in the account	View only the configuration of a specific Lambda function
lambda:GetLayerVersion	All Lambda layers in the account	View the details of a specific version of a Lambda layer and download their source code
iam:GetRole	All IAM roles in the account	View details of a specific IAM role and assume the role of the monitored account from an outpost

Outposts

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
ec2:AllocateAddress	Resources with the request tag: <b>managed_by: paloaltonetworks</b>	Allocate a static public IP address for use with a proxy VM
ec2:AssociateAddress	Resources with the request tag: <b>managed_by: paloaltonetworks</b>	Associate a static public IP address with a network interface for use with a proxy VM
ec2:AttachVolume	Volumes in the specified AWS account with the <b>managed_by: paloaltonetworks</b>	Attach volume to scanner VM during deployment
ec2>CreateNetworkInterface	Any region in the specified AWS account with the tag <b>managed_by: paloaltonetworks</b> ; applies to network interfaces, subnets, and security groups.	Create a network interface for a scanner or proxy VM within managed subnets and security groups



Permission	Scope	Purpose
ec2:CreateTags	Resources with the request tag: <b>managed_by: paloaltonetworks</b> tag	For adding tags to all resources
ec2>CreateVolume	Volumes with the request tag: <b>managed_by: paloaltonetworks</b> tag	Perform the create volume operation in EC2
ec2:CreateVpcEndpoint	<p>The VPC endpoint being created must:</p> <ul style="list-style-type: none"> <li>• Have the request tag: <b>managed_by: paloaltonetworks</b></li> <li>• Only reference Palo Alto Networks-managed network components (VPCs, security groups, subnets, and route tables, and so on, with the request tag: <b>managed_by: paloaltonetworks</b>)</li> <li>• Connect to an approved VpcServiceName service as defined by policy</li> </ul>	Create endpoints that are used by scanners to access managed services using private IP addresses
ec2>DeleteNetworkInterface	Network interfaces with the request resource tag: <b>managed_by: paloaltonetworks</b>	Perform the delete network interface operation in EC2
ec2>DeleteVolume	Volumes in the specified account with the request tag: <b>managed_by: paloaltonetworks</b>	Perform the delete volume operation in EC2
ec2>DeleteVpcEndpoints	VPC endpoints in the specified account with the resource tag: <b>managed_by: paloaltonetworks</b>	Perform the delete VPC endpoints operation in EC2
ec2:DescribeAccountAttributes	*	Describe account attributes in EC2
ec2:DescribeAddresses	*	Perform the describe addresses operation in EC2
ec2:DescribeAvailabilityZones	*	Perform the describe availability zones operation in EC2
ec2:DescribeImages	*	Perform the describe images operation in EC2
ec2:DescribeInstances	*	Perform the describe instances operation in EC2
ec2:DescribeInstanceTypes	*	Perform the describe instance types operation in EC2
ec2:DescribeKeyPairs	*	Perform the describe key pairs operation in EC2
ec2:DescribeNetworkInterfaces	*	Perform the describe network interfaces operation in EC2
ec2:DescribeSecurityGroups	*	Perform the describe security groups operation in EC2



Permission	Scope	Purpose
ec2:DescribeSubnets	*	Perform the describe subnets operation in EC2
ec2:DescribeVolumeAttribute	Volumes in the specified account with the request tag: <code>managed_by: paloaltonetworks</code>	Perform the describe volume attribute operation in EC2
ec2:DescribeVolumes	*	Perform the describe volumes operation in EC2
ec2:DescribeVolumesModifications	*	Perform the describe volumes modifications operation in EC2
ec2:DescribeVolumeStatus	*	Perform the describe volume status operation in EC2
ec2:DescribeVpcEndpoints	*	Perform the describe VPC endpoints operation in EC2
ec2:DescribeVpcs	*	Perform the describe VPC operation in EC2
ec2:DetachVolume	Volumes in the specified account with the request tag: <code>managed_by: paloaltonetworks</code>	Perform the detach volume operation in EC2
ec2:DisassociateAddress	Volumes with the resource tag: <code>managed_by: paloaltonetworks</code>	Perform the disassociate address operation in EC2
ec2:GetSpotPlacementScores	*	Perform the get spot placement scores operation for prioritization of an availability zone for spot instance deployment
ec2:ImportVolume	Volumes in the specified account with the request tag: <code>managed_by: paloaltonetworks</code>	Perform the import volume operation in EC2
ec2:ModifyInstanceAttribute	Instances in the specified account, where both of the following conditions are met: <ul style="list-style-type: none"> <li>The target EC2 instance has the resource tag: <code>managed_by: paloaltonetworks</code></li> <li>The modify action must be specifically related to changing the value of the SourceDestCheck attribute</li> </ul>	Perform the modify instance attribute operation in EC2
ec2:ModifyVolume*	Volumes in the specified account with the request tag: <code>managed_by: paloaltonetworks</code>	Perform the modify volume* operation in EC2
ec2:ReleaseAddress	Resources with the resource tag: <code>managed_by: paloaltonetworks</code>	Perform the release address operation in EC2



Permission	Scope	Purpose
ec2:RunInstances	<p>The new EC2 instance must be launched into a network environment (VPC, subnets, security groups, and key pairs) that is already designated as <code>managed_by: paloaltonetworks</code>, and if the request correctly specifies that the newly-created instance, network interfaces, and volumes are also tagged as <code>managed_by: paloaltonetworks</code>.</p> <p>The use of source snapshots for volumes is permitted without any tagging restrictions</p>	Run (launch) a scanner and/or proxy VM
ec2:TerminateInstances	EC2 instances with the tag: <code>managed_by: paloaltonetworks</code>	Perform the terminate instances operation in EC2
iam:CreateServiceLinkedRole	The role being created must be exclusively for the Amazon Redshift service	Perform the create service linked role operation in IAM
iam:PassRole	Limited to the specific list of roles designated as 'scanner roles' within the account	Perform the pass role operation in IAM
kms:*	Keys must be accessed through a legitimate, identified AWS service (such as S3, RDS, EC2, and so on)	Perform the * operation in KMS
kms:ReEncryptFrom	The request must be initiated by the Amazon EC2 service and be contextually tied to the encryption of an EBS volume or snapshot	Perform the re-encrypt from operation in KMS
redshift-data:BatchExecuteStatement	*	Execute a list of SQL statements in a single batch
redshift-data:CancelStatement	*	Stop a currently running SQL statement or a batch of statements
redshift-data:Describe*	*	Provide detailed status and information about a previously executed SQL statement
redshift-data:ExecuteStatement	*	Run a single SQL statement asynchronously against a Redshift cluster or workgroup
redshift-data:GetStatementResult	*	Retrieve the result set (data) from a SQL statement that has finished execution
redshift-data>List*	*	List the IDs of all SQL statements executed within the past week
redshift-serverless>CreateNamespace	Creation request includes tag: <code>managed_by: paloaltonetworks</code>	Create a Redshift Serverless namespace



Permission	Scope	Purpose
redshift-serverless>CreateWorkgroup	Creation request includes tag: <b>managed_by: paloaltonetworks</b>	Create a Redshift Serverless workgroup
redshift-serverless>DeleteNamespace	Namespaces tagged with: <b>managed_by: paloaltonetworks</b>	Permanently delete a Redshift Serverless namespace and all associated data
redshift-serverless>DeleteWorkgroup	Workgroup tagged with: <b>managed_by: paloaltonetworks</b>	Delete a Redshift Serverless workgroup, removing its associated compute resources
redshift-serverless:GetCredentials	*	Request temporary credentials to connect directly to the database within a workgroup
redshift-serverless:GetNamespace	*	Retrieve configuration and status details for a specific namespace
redshift-serverless:GetWorkgroup	*	Retrieve configuration and status details for a specific workgroup
redshift-serverless>ListNamespaces	*	List summary information for all namespaces in the current account and region
redshift-serverless>ListTagsForResource	*	List all the tags currently attached to a specified Redshift Serverless resource
redshift-serverless>ListWorkgroups	*	List summary information for all workgroups in the current account and region
redshift-serverless>RestoreFromSnapshot	*	Create a new namespace and restore its data from a specified backup snapshot
redshift-serverless>TagResource	*	Apply, modify, or update tags on a Redshift Serverless resource. This is crucial for cost allocation and governance
s3>DeleteObject	The bucket must be owned by the user's current AWS account.	Delete a specified object from artifact bucket
s3>GetBucketPolicy	The bucket must be owned by the user's current AWS account.	Retrieve the resource-based access policy attached to an Amazon S3 bucket
s3>GetObject	Users can read (download) any file from the <b> \${cf_template_bucket} </b> Also, users can read files from any S3 bucket they own that begins with the prefix <b> \${bucket_name}- </b> , with specific access paths defined for the general bucket contents and files within the <b> output/, input/, and output/logs/ </b> folders	Retrieve the contents of a specified object from an Amazon S3 bucket



Permission	Scope	Purpose
s3:GetObjectAttributes	<p>Users can read the metadata (attributes) of files from any S3 bucket they own that begins with the prefix: <code> \${bucket_name}-</code></p> <p>This permission applies to files located anywhere within that bucket, but the specific paths are detailed as the general bucket contents and files within the <code>output/</code>, <code>input/</code>, and <code>output/logs/</code> folders</p>	Fetch system-defined metadata and object attributes for an S3 object
s3>ListBucket	<p>Users can view:</p> <ul style="list-style-type: none"> <li>The list of contents for the specific <code> \${cf_template_bucket}</code></li> <li>The contents of any S3 bucket they own that has a name starting with the prefix <code> \${bucket_name}-</code></li> </ul>	List the objects or common prefixes in an Amazon S3 bucket
s3:PutBucketPolicy	S3 buckets that users own and whose name begins with the prefix: <code> \${bucket_name}-</code>	Apply or update a resource-based access policy in an Amazon S3 bucket
s3:PutObject	<p>Users can</p> <ul style="list-style-type: none"> <li>Upload files to the specific <code> \${cf_template_bucket}</code> without restriction.</li> <li>Upload files to any S3 bucket users own that begins with the prefix: <code> \${bucket_name}-</code></li> </ul> <p>This upload permission applies broadly to the general contents of these prefixed buckets, including files placed specifically in the <code>input/</code>, <code>output/</code>, and <code>output/logs/</code> subfolders</p>	Upload or replace an object in an Amazon S3 bucket
sq:DeleteMessage	Messages from any SQS queue that is already tagged with <code>managed_by: paloaltonetworks</code> and whose name begins with the prefix: <code> \${queue_prefix}-</code>	For bucket communications
sq:GetQueueUrl	URL for any SQS queue that is already tagged with <code>managed_by: paloaltonetworks</code> and whose name begins with the prefix: <code> \${queue_prefix}-</code>	For bucket communications
sq:ListQueues	URL for any SQS queue that is already tagged with <code>managed_by: paloaltonetworks</code> and whose name begins with the prefix: <code> \${queue_prefix}-</code>	For bucket communications
sq:ReceiveMessage	Messages from any SQS queue that is already tagged with <code>managed_by: paloaltonetworks</code> and whose name begins with the prefix: <code> \${queue_prefix}-</code>	For bucket communications



Permission	Scope	Purpose
ssm:AddTagsToResource	SSM Parameter named cortex-outposts-..., but only if the tagging request itself includes the <code>managed_by: paloaltonetworks</code> tag	Perform the add tags to resource operation in SSM.
ssm>DeleteParameter	SSM parameter named <code>cortex-outposts-...</code> , but only if that specific parameter resource is already tagged with <code>managed_by: paloaltonetworks</code>	Delete a secret that was used for unmanaged container image registries by key
ssm:GetParameter	SSM parameter named <code>cortex-outposts-...</code> , but only if that specific parameter resource is already tagged with <code>managed_by: paloaltonetworks</code>	This outpost-specific permission's purpose is to get a secret by key for unmanaged container image registries
ssm:PutParameter	Group of SSM parameter store parameters in a specified AWS account with the request tag: <code>managed_by: paloaltonetworks</code>	Put secret for unmanaged container image registries
sts:AssumeRole	Resource belongs to a different AWS account than the current account	Provide temporary security credentials by assuming the specified IAM role through STS

#### 2.2.6.11.2 | Google Cloud Platform provider permissions

##### Abstract

List of Google Cloud Platform provider permissions for Cortex Cloud.

When onboarding Google Cloud Platform, Cortex Cloud creates an authentication template that requests the permissions needed for monitoring your cloud environment. Depending on which security capabilities you select in the onboarding wizard, different permissions are requested. The following tables are organized by security module and list the CSP permissions being requested as well as the purpose (and where relevant, the scope):

- Agentless Disk Scanning
- DSPM
- Discovery Engine
- Log Collection
- Registry Scan
- Automations
- Serverless Scan
- Outposts

##### Agentless Disk Scanning

Permission	Scope	Purpose
compute.disks.create	Disks with "cortex-scan-" prefix	Create disk from image
compute.disks.delete	Disks with "cortex-scan-" prefix	Delete created disk
compute.disks.get	Disks with "cortex-scan-" prefix	Retrieve disk creation status



Permission	Scope	Purpose
compute.disks.setLabels	Disks with "cortex-scan-" prefix	Set label for disks
compute.images.get	Images with "cortex-scan-" prefix	Retrieve image metadata
compute.snapshots.create	Snapshots with "cortex-scan-" prefix	Create disk snapshot
compute.snapshots.delete	Snapshots with "cortex-scan-" prefix	Delete scanned snapshot
compute.snapshots.get	Snapshots with "cortex-scan-" prefix	Retrieve snapshot creation status
compute.snapshots.setLabels	Snapshots with "cortex-scan-" prefix	Add snapshot labels for a cost visibility
compute.snapshots.useReadOnly	Snapshots with "cortex-scan-" prefix	Attach snapshot to a scanner VM

DSPM

Permission	Scope	Purpose
artifactregistry.repositories.downloadArtifacts	All Artifact Registry Repositories in the project (or higher)	Download or retrieve artifacts (like container images and packages) from an Artifact Registry repository. This is necessary for a DSPM scanner to inspect the content for security and compliance assessment.
bigrquery.bireservations.get	All BigQuery instances	Get BigQuery bireservations for classification purposes
bigrquery.capacityCommitments.get	All BigQuery instances	Get BigQuery capacity commitments for classification purposes
bigrquery.capacityCommitments.list	All BigQuery instances	List BigQuery capacity commitments for classification purposes
bigrquery.config.get	All BigQuery instances	Get BigQuery configurations for classification purposes
bigrquery.datasets.get	All BigQuery instances	Get BigQuery datasets for classification purposes
bigrquery.datasets.getIamPolicy	All BigQuery instances	Get BigQuery dataset IAM policies for classification purposes
bigrquery.models.getData	All BigQuery instances	List BigQuery model data for classification purposes



Permission	Scope	Purpose
bigquery.models.getMetadata	All BigQuery instances	Get BigQuery model metadata for classification purposes
bigquery.models.list	All BigQuery instances	List BigQuery models for classification purposes
bigquery.routines.get	All BigQuery instances	Get BigQuery routines for classification purposes
bigquery.routines.list	All BigQuery instances	List BigQuery routines for classification purposes
bigquery.tables.export	All BigQuery instances	Export BigQuery tables
bigquery.tables.get	All BigQuery instances	Get BigQuery tables for classification purposes
bigquery.tables.getData	All BigQuery instances	Get BigQuery table data for classification purposes
bigquery.tables.getIamPolicy	All BigQuery instances	Get BigQuery table IAM policies for classification purposes
bigquery.tables.list	All BigQuery instances	List BigQuery tables for classification purposes
bigtable.backup.create	All Bigtable instances	Create Bigtable backups for standard cloud and outpost deployments
bigtable.backup.delete	All Bigtable instances	Delete Bigtable backups on standard cloud and outpost deployments
bigtable.backups.get	All Bigtable instances	Get Bigtable backup metadata for standard cloud, outpost, and scanner-based deployments
bigtable.backups.list	All Bigtable instances	List Bigtable backups for standard cloud, outpost, and scanner-based deployments
bigtable.backups.restore	All Bigtable instances	Restore Bigtable from backup
bigtable.clusters.get	All Bigtable instances	Get Bigtable cluster metadata for standard cloud and scanner-based deployments
bigtable.clusters.list	All Bigtable instances	List Bigtable clusters for standard cloud and scanner-based deployments
bigtable.instances.get	All Bigtable instances	Get Bigtable instance metadata for standard cloud and scanner-based deployments



Permission	Scope	Purpose
bigtable.instances.list	All Bigtable instances	List Bigtable instances for standard cloud and scanner-based deployments
bigtable.tables.get	All Bigtable instances	Get Bigtable table metadata for standard cloud and scanner-based deployments
bigtable.tables.list	All Bigtable instances	List Bigtable instances for standard cloud, outpost, and scanner-based deployments
cloudsql.backupRuns.create	All Cloud SQL instances	Create CloudSQL backup runs for classification purposes for standard cloud and outpost deployments
cloudsql.backupRuns.delete	All Cloud SQL instances	Delete CloudSQL backup runs for standard cloud and outpost deployments
cloudsql.backupRuns.get	All CloudSQL instances	Get CloudSQL backup run metadata for classification purposes for standard cloud, outpost, and scanner-based deployments
cloudsql.backupRuns.list	All Cloud SQL instances	List CloudSQL backup runs for classification purposes for standard cloud and outpost deployments
roles/cloudfunctions.viewer  (Built-in role. managed by GCP)	All Cloud Functions in the project (or higher)	Read the configuration and metadata of all Cloud Functions resources in the project. This is necessary for inventory and security posture assessment.
roles/container.clusterViewer  (Built-in role. managed by GCP)	All Google Kubernetes Engine (GKE) Clusters in the project (or higher)	Read the configuration and status of all Google Kubernetes Engine (GKE) clusters in the project for posture assessment
roles/firebaserules.viewer  (Built-in role. managed by GCP)	All Firebase Security Rules in the project (or higher)	Read the configuration and contents of Firebase Security Rules for posture assessment
roles/storage.objectViewer  (Built-in role. managed by GCP)	All objects (files) in all Cloud Storage buckets in the project (or higher)	Read the data and metadata of objects (files) in Cloud Storage buckets, but cannot modify or delete them. This is required for data scanning and inventory.

Discovery Engine

Permission	Purpose
accesscontextmanager.accessLevels.list	List Access Context Manager (GCP ACM) access levels
accesscontextmanager.accessPolicies.list	List Access Context Manager (GCP ACM) policies



Permission	Purpose
accesscontextmanager.servicePerimeters.list	List Access Context Manager (GCP ACM) service perimeters
aiplatform.batchPredictionJobs.list	List AI Platform batch prediction jobs
aiplatform.nasJobs.list	List AI Platform Neural Architecture Search (NAS) jobs
analyticshub.dataExchanges.list	List Analytics Hub data exchanges
analyticshub.listings.getIamPolicy	Get IAM policy for Analytics Hub listings
analyticshub.listings.list	List Analytics Hub listings
baremetalsolution.instances.list	List Bare Metal Solution instances
baremetalsolution.luns.list	List Bare Metal Solution LUNs (Logical Unit Numbers)
baremetalsolution.networks.list	List Bare Metal Solution networks
baremetalsolution.nfsshare.list	List Bare Metal Solution NFS shares
baremetalsolution.volumes.list	List Bare Metal Solution volumes
cloudscheduler.jobs.list	List Cloud Scheduler jobs
cloudsecurityscanner.scans.list	List Cloud Security Scanner scans
composer.imageversions.list	List Composer image versions
datamigration.connectionprofiles.getIamPolicy	Get IAM policy for data migration connection profiles
datamigration.connectionprofiles.list	List data migration connection profiles
datamigration.conversionworkspaces.getIamPolicy	Get IAM policy for data migration conversion workspaces
datamigration.conversionworkspaces.list	List data migration conversion workspaces
datamigration.migrationjobs.getIamPolicy	Get IAM policy for data migration jobs
datamigration.migrationjobs.list	List data migration jobs
datamigration.privateconnections.getIamPolicy	View the access policy for a Database Migration Service private connection



Permission	Purpose
datamigration.privateconnections.list	List data migration private connections
notebooks.locations.list	List notebook locations
notebooks.schedules.list	List notebook schedules
roles/cloudfunctions.viewer  (Built-in role. managed by GCP)	Read the configuration and metadata of all Cloud Functions resources in the project. This is necessary for inventory and security posture assessment.
roles/container.clusterViewer  (Built-in role. managed by GCP)	Read the configuration and status of all Google Kubernetes Engine (GKE) clusters in the project for posture assessment
roles/firebaserules.viewer  (Built-in role. managed by GCP)	Read the configuration and contents of Firebase Security Rules for posture assessment
roles/storage.objectViewer  (Built-in role. managed by GCP)	Read the data and metadata of objects (files) in Cloud Storage buckets, but cannot modify or delete them. This is required to view the content and details of all stored data assets for inventory.
roles/viewer  (Built-in role. managed by GCP)	Grant read-only access to view resources and data across all Google Cloud services within the project. This is the broadest read permission required for comprehensive asset inventory.
run.jobs.getiamPolicy	Get IAM policy of Cloud Run jobs
run.jobs.list	List Cloud Run jobs
run.services.list	List Cloud Run services
serviceusage.services.use	Use cloud services
storage.buckets.get	Get metadata of a storage bucket
storage.buckets.getiamPolicy	Get IAM policy of a storage bucket
storage.buckets.list	List storage buckets
storage.buckets.listEffectiveTags	List effective tags of storage buckets
storage.buckets.listTagBindings	List tag bindings of storage buckets
storage.objects.getiamPolicy	Get IAM policy of storage objects

Log Collection



<b>Permission</b>	<b>Purpose</b>
roles/pubsub.subscriber  (Built-in role, managed by GCP)	Grants access to consume messages from the subscription where audit logs are stored

Registry Scan

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
roles/iam.serviceAccountTokenCreator	Access to this permission is limited to a specific Service Account defined within an outpost. No account other than the defined Service Account can access the permission and access is limited to the permissions defined on the target SA.	Impersonate to a specific service account
artifactregistry.repositories.downloadArtifacts	All artifacts listed in the GAR of the customer's account	Needed in order to download images from the Google Artifact Registry (GAR)

Automations

<b>Permission</b>	<b>Command That Requires This Permission</b>	<b>Purpose</b>
compute.firewalls.create	gcp-compute-firewall-insert	
compute.firewalls.get	gcp-compute-firewall-get	
compute.firewalls.list	gcp-compute-firewall-list	
compute.firewalls.update		
compute.images.get	gcp-compute-image-get	
compute.instanceGroups.get	gcp-compute-instance-group-get	
compute.instances.get	gcp-compute-instance-get	
compute.instances.list	gcp-compute-instances-list	
compute.instances.setLabels	gcp-compute-instance-labels-set	
compute.instances.setMetadata		
compute.instances.setServiceAccount		
compute.instances.setTags	gcp-compute-network-tag-set	



Permission	Command That Requires This Permission	Purpose
compute.instances.start	gcp-compute-instance-start	
compute.instances.stop	gcp-compute-instance-stop	
compute.networks.create	gcp-compute-network-insert	
compute.networks.get	gcp-compute-network-get	
compute.networks.list	gcp-compute-network-list	
compute.networks.updatePolicy		
compute.regions.get	gcp-compute-region-get	
compute.snapshots.get	gcp-compute-snapshot-get	
compute.snapshots.list	gcp-compute-snapshots-list	
compute.subnetworks.get		
compute.subnetworks.list		
compute.subnetworks.setPrivateIpGoogleAccess		
compute.subnetworks.update		
compute.zones.get	gcp-compute-zone-get	
container.clusters.get		
container.clusters.list		
container.clusters.update		
resourcemanager.projects.getIamPolicy		
resourcemanager.projects.setIamPolicy		



Permission	Command That Requires This Permission	Purpose
storage.buckets.get	<ul style="list-style-type: none"> <li>• gcp-storage-bucket-get</li> <li>• gcp-storage-bucket-policy-list</li> <li>• gcp-storage-bucket-policy-set</li> </ul>	
storage.buckets.getIamPolicy	<ul style="list-style-type: none"> <li>• gcp-storage-bucket-list</li> <li>• gcp-storage-bucket-get</li> <li>• gcp-storage-bucket-policy-list</li> <li>• gcp-storage-bucket-policy-set</li> </ul>	
storage.buckets.getIpFilter	<ul style="list-style-type: none"> <li>• gcp-storage-bucket-list</li> <li>• gcp-storage-bucket-get</li> </ul>	
storage.buckets.list	gcp-storage-bucket-list	
storage.buckets.setIamPolicy	<ul style="list-style-type: none"> <li>• gcp-storage-bucket-policy-set</li> <li>• gcp-storage-bucket-object-policy-set</li> </ul>	
storage.buckets.update	gcp-storage-bucket-policy-set	
storage.objects.getIamPolicy	<ul style="list-style-type: none"> <li>• gcp-storage-bucket-objects-list</li> <li>• gcp-storage-bucket-object-policy-list</li> </ul>	
storage.objects.list	gcp-storage-bucket-objects-list	
cloudidentity.groups.memberships.delete	gcp-iam-group-membership-delete	Revoke permissions from the Access Control List (ACL). This is to remediate an issue detected by the rule: "GCP Storage buckets are publicly accessible to all authenticated users"
cloudasset.assets.searchAllResources	gcp-compute-instances-aggregated-list-by-ip	Search and retrieve the metadata for all Google Cloud resources (VMs, buckets, networks, and so on) within a specified scope (project, folder, or organization). This is required for comprehensive asset discovery and to gain a unified, auditable view of the entire GCP environment.

Serverless Scan

Permission	Purpose
cloudfunctions.functions.get	Read the metadata of a specific Cloud function. Needed for reading function metadata.



<b>Permission</b>	<b>Purpose</b>
cloudfunctions.functions.sourceCodeGet	Read and download the source code of a deployed Cloud function. Needed to download function source code for scanning.
storage.objects.get	Read the data of a specific object in a Cloud storage bucket. Needed to download function source code for scanning.

Outposts

<b>Permission</b>	<b>Purpose</b>
roles/compute.admin	Grant full administrative control over Compute Engine resources (VMs, disks, networks, and so on), but not the project-wide IAM
roles/bigtable.admin	Grant full administrative control over Bigtable instances, clusters, and tables
roles/bigtable.reader	Read all data and metadata from Bigtable tables. This is necessary for Data Security Posture Management (DSPM) scanners so they can get data from the customer environment
roles/cloudsql.client	Connect to and execute data operations (read/write) on Cloud SQL databases
roles/iam.serviceAccountUser	Allow a user or service to delegate its identity by acting as a service account for running workloads (for example, VMs, Cloud Run, or GKE)
roles/iam.serviceAccountTokenCreator	Allow a user or service to impersonate a service account directly by creating access tokens, signing blobs, or signing JSON Web Tokens (JWTs). Useful for workload identity federation or automation.
roles/cloudkms.cryptoKeyEncrypterDecrypter	Encrypt and decrypt data using a specific Cloud Key Management Service (Cloud KMS) cryptographic key
roles/cloudkms.viewer	Read the details and metadata of cryptographic keys and key rings in Cloud KMS
roles/secretmanager.secretAccessor	For use by outpost only: Allow reading secret values from the Secret Manager
roles/servicenetworking.serviceAgent	Allow the Google-managed service accounts to manage private service networking connections
roles/pubsub.subscriber	Consume messages from a Pub/Sub subscription for inter-service communication (for example, bucket events)
bigrquery.jobs.create	Create an export job to transfer data from BigQuery to Google Cloud Storage (GCS). Used from ST.
cloudsql.databases.create	Create databases as part of the instance restore. Used from ST.
cloudsql.databases.delete	Delete databases as part of the instance cleanup operation. Used from ST.
cloudsql.databases.update	Modify database properties as part of the instance restore operation. Used from ST.



Permission	Purpose
cloudsql.databases.get	Retrieve database details as part of the instance restore operation. Used from ST.
cloudsql.databases.list	List databases as part of the instance restore operation. Used from ST.
cloudsql.instances.list	List Cloud SQL instances as part of the instance restore operation. Used from ST.
cloudsql.instances.get	Retrieve instance details as part of the instance restore operation. Used from ST.
cloudsql.instances.connect	Connect to a Cloud SQL instance for data scanning. Used from scanners.
cloudsql.instances.create	Create a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.instances.delete	Delete Cloud SQL instances as part of the instance cleanup operation. Used from ST.
cloudsql.instances.login	Log into a Cloud SQL instance for data scanning. Used from scanners.
cloudsql.instances.restart	Restart a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.instances.restoreBackup	Restore a Cloud instance from a backup as part of the instance restore operation. Used from ST.
cloudsql.instances.update	Modify Cloud SQL instance properties as part of the instance restore operation. Used from ST.
cloudsql.instances.createTagBinding	Apply a TagKey and TagValue to a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.instances.deleteTagBinding	Update (remove) TagKey and TagValue from a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.instances.listTagBindings	List instance tags as part of the instance restore operation. Used from ST.
cloudsql.users.create	Create a new user for a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.users.delete	Delete an existing user from a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.users.update	Modify the settings of a user on a Cloud SQL instance as part of the instance restore operation. Used from ST.
cloudsql.users.get	Retrieve instance users as part of the instance restore operation. Used from ST.
cloudsql.users.list	List all users on a Cloud SQL instance as part of the instance restore operation. Used from ST.
secretmanager.secrets.create	Create a new Secret Manager secret for use by a scanner



<b>Permission</b>	<b>Purpose</b>
secretmanager.secrets.update	Update secret metadata such as labels and replication settings
secretmanager.secrets.delete	Delete an existing Secret Manager secret
secretmanager.secrets.get	View the metadata and configuration of a Secret Manager secret
secretmanager.secrets.list	List all Secret Manager secrets within a project
secretmanager.versions.access	Access the actual secret payload (value) for a specific secret version
secretmanager.versions.add	Add a new version containing updated data to an existing secret
secretmanager.versions.destroy	Permanently destroy a secret version (irreversible)
secretmanager.versions.disable	Disable an existing secret version, making its payload inaccessible
secretmanager.versions.enable	Enable a previously-disabled secret version, making its payload accessible
secretmanager.versions.get	View the metadata and state of a secret version
secretmanager.versions.list	List all versions associated with a Secret Manager secret
storage.objects.create	Upload or create a new object (file) in a Cloud Storage bucket for scan runner communication
storage.objects.delete	Delete an existing object (file) from an artifact bucket
storage.objects.list	List all objects (files) contained within a Cloud Storage bucket
cloudkms.cryptoKeyVersions.create	Create a new version for a cryptographic key, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeyVersions.destroy	Permanently destroy a cryptographic key version, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeyVersions.get	Retrieve the details and metadata of a cryptographic key version, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeyVersions.list	List all versions of a cryptographic key, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeyVersions.update	Modify the settings and state of a cryptographic key version, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeyVersions.useToDecrypt	Use a cryptographic key version to decrypt data, used for Bigtable encryption. Used from scanner.
cloudkms.cryptoKeyVersions.useToEncrypt	Use a cryptographic key version to encrypt data, used for Bigtable encryption. Used from ST.



<b>Permission</b>	<b>Purpose</b>
cloudkms.cryptoKeys.create	Create a new cryptographic key, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeys.setIamPolicy	Set the IAM policy (permissions) for a cryptographic key, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeys.getIamPolicy	Retrieve the IAM policy (permissions) for a cryptographic key, used for Bigtable encryption. Used from ST.
cloudkms.cryptoKeys.update	Modify the properties of a cryptographic key, used for Bigtable encryption. Used from ST.
cloudkms.keyRings.create	Create a new key ring to hold cryptographic keys, used for Bigtable encryption. Used from ST.

#### 2.2.6.11.3 | Microsoft Azure provider permissions

##### Abstract

List of Microsoft Azure provider permissions for Cortex Cloud.

When onboarding Microsoft Azure, Cortex Cloud creates an authentication template that requests the permissions needed for monitoring your cloud environment. Depending on which security capabilities you select in the onboarding wizard, different permissions are requested. The following tables are organized by security module and list the CSP permissions being requested as well as the purpose (and where relevant, the scope):

- Agentless Disk Scanning
- DSPM
- Discovery Engine
- Log Collection
- Registry Scan
- Outposts
- Onboarding managed identity
- Automations

##### Agentless Disk Scanning

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Compute/disks/delete	No scoping	Delete a scanned disk, after image scanning, ensuring resource cleanup
Microsoft.Compute/disks/read	Management Group	Retrieve disk status and properties to verify the disk is ready, such as for image scanning
Microsoft.Compute/disks/write	Management Group	Create a disk from the volume's image, for image scanning
Microsoft.Compute/galleries/images/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete a temporary gallery image, for legacy image scanning



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Compute/galleries/images/read	Management Group	Read a gallery image in order to create a disk for image scanning
Microsoft.Compute/galleries/images/versions/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete a temporary gallery image version after legacy image scanning
Microsoft.Compute/galleries/images/versions/write	Resource groups starting with the prefix <b>cortex-</b>	Create a temporary gallery image version, for legacy image scanning
Microsoft.Compute/galleries/images/write	Resource groups starting with the prefix <b>cortex-</b>	Create a temporary gallery image, for legacy image scanning
Microsoft.Compute/snapshots/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete a scanned snapshot after instance/image scanning
Microsoft.Compute/snapshots/read	Management Group	Read source snapshot's data to facilitate the conversion of a snapshot to a disk that will be attached to a scanner
Microsoft.Compute/snapshots/write	Resource groups starting with the prefix <b>cortex-</b>	Create a disk snapshot, before instance/image scanning
Microsoft.Compute/virtualMachines/read	Management Group	Allow disk snapshot operations, for instance scanning

DSPM

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.CognitiveServices/*/action	All deployments	Read and scan OpenAI files and other Azure AI data resources
Microsoft.CognitiveServices/*/read	All deployments	Discover of OpenAI resources and other Azure AI services
Microsoft.DocumentDB/databaseAccounts/listKeys	* Entire subscription	Get SAS token of CosmosDB to enable access
Microsoft.Network/networkSecurityGroups/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete security groups
Microsoft.Network/networkSecurityGroups/join/action	Resource groups starting with the prefix <b>cortex-</b>	Associate a network security group with a subnet or network interface
Microsoft.Network/networkSecurityGroups/securityRules/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete security rules for a security group



Permission	Scope	Purpose
Microsoft.Network/networkSecurityGroups/securityRules/write	Resource groups starting with the prefix <b>cortex-</b>	Create or update security rules within a network security group
Microsoft.Network/networkSecurityGroups/write	Resource groups starting with the prefix <b>cortex-</b>	Create or update a network security group
Microsoft.Network/routeTables/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete a route table from a subscription
Microsoft.Network/routeTables/join/action	Resource groups starting with the prefix <b>cortex-</b>	Associate a route table with a subnet
Microsoft.Network/routeTables/write	Resource groups starting with the prefix <b>cortex-</b>	Create or update a route table
Microsoft.Network/virtualNetworks/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete a virtual network
Microsoft.Network/virtualNetworks/join/action	Resource groups starting with the prefix <b>cortex-</b>	Associate a virtual network with a subnet
Microsoft.Network/virtualNetworks/subnets/delete	Resource groups starting with the prefix <b>cortex-</b>	Delete a virtual network subnet
Microsoft.Network/virtualNetworks/subnets/join/action	Resource groups starting with the prefix <b>cortex-</b>	Associate a subnet with a resource
Microsoft.Network/virtualNetworks/subnets/write	Resource groups starting with the prefix <b>cortex-</b>	Create or update a subnet
Microsoft.Network/virtualNetworks/write	Resource groups starting with the prefix <b>cortex-</b>	Create or update a virtual network
Microsoft.Sql/managedInstances/databases/write	Resource groups starting with the prefix <b>cortex-</b>	Used for copying PITR of SQL managed instances to Palo Alto Networks' resource group, enabling Palo Alto Networks to restore and scan it
Microsoft.Sql/managedInstances/delete	Resource groups starting with the prefix <b>cortex-</b>	Clean stale assets such as Palo Alto Networks' Azure SQL Managed Instance
Microsoft.Sql/managedInstances/write	Resource groups starting with the prefix <b>cortex-</b>	Create SQL Managed Instance for classification of managed instances
Microsoft.Sql/servers/databases/delete	Resource groups starting with the prefix <b>cortex-</b>	Clean stale assets such as Palo Alto Networks' Azure SQL server databases



Permission	Scope	Purpose
Microsoft.Sql/servers/databases/read	Resource groups starting with the prefix <b>cortex-</b>	Get configurations on Azure SQL databases
Microsoft.Sql/servers/databases/resume/action	Resource groups starting with the prefix <b>cortex-</b>	Copy and manage SQL databases in Azure SQL server
Microsoft.Sql/servers/databases/write	Resource groups starting with the prefix <b>cortex-</b>	Copy and manage SQL databases in Azure SQL server
Microsoft.Sql/servers/delete	Resource groups starting with the prefix <b>cortex-</b>	Clean stale assets such as Palo Alto Networks' Azure SQL server
Microsoft.Sql/servers/privateEndpointConnections/approve/action	Resource groups starting with the prefix <b>cortex-</b>	Connection using endpoints
Microsoft.Sql/servers/virtualNetworkRules/write	Resource groups starting with the prefix <b>cortex-</b>	Configure network accessibility from the scanning VMs on Palo Alto Networks' Azure SQL servers
Microsoft.Sql/servers/write	Resource groups starting with the prefix <b>cortex-</b>	Create and manage Palo Alto Networks' Azure SQL servers
Microsoft.Storage/*/read	Entire subscription	Read blob data for data classification
Microsoft.Storage/storageAccounts/blobServices/containers/slobs/read	Entire subscription	Enable classification of data in storage blobs
Microsoft.Storage/storageAccounts/blobServices/generateSas/action	Entire subscription	Get SAS token of blobServices to enable access
Microsoft.Storage/storageAccounts/fileServices/fileshares/read	Entire subscription	Enable classification of data in storage fileshares
Microsoft.Storage/storageAccounts/ListAccountSas/action	Entire subscription	Get access SAS token to the storage account to scan file share instances using API
Microsoft.Storage/storageAccounts/listKeys/action	Entire subscription	Get access key to the storage account to scan file share instances using API
Microsoft.Storage/storageAccounts/PrivateEndpointConnections/approve/action	Entire subscription	Enable a scan by assigning private endpoints to a storage account located in a private network
Microsoft.Storage/storageAccounts/tableServices/tables/read	Entire subscription	Enable classification of data in storage tables
*/read	Entire subscription	Read-only access, used to get metadata of all managed data assets in the subscription

Discovery Engine



Permission	Scope	Purpose
AuditLog.Read.All	Tenants or management groups using Microsoft Graph	Read all audit log data for any tenant or management group
Directory.Read.All	Tenants or management groups using Microsoft Graph	Read full property sets for all directory objects
Domain.Read.All	Tenants or management groups using Microsoft Graph	Read all domain properties in a tenant
EntitlementManagement.Read.All	Tenants or management groups using Microsoft Graph	Read all access packages, assignments, and catalog configurations
GroupMember.Read.All	Tenants or management groups using Microsoft Graph	Read all group memberships in the directory
Group.Read.All	Tenants or management groups using Microsoft Graph	Read full property sets for all groups without editing group membership
IdentityProvider.Read.All	Tenants or management groups using Microsoft Graph	Read all identity provider configurations
Microsoft.Advisor/configurations/read	Management Group	Read Advisor configuration
Microsoft.AlertsManagement/prometheusRuleGroups/read	Management Group	Read Prometheus rule groups
Microsoft.AlertsManagement/smartDetectorAlertRules/read	Management Group	Read smart detector alert rules
Microsoft.AnalysisServices/servers/read	Management Group	Read Analysis Services servers
Microsoft.ApiManagement/service/apis/diagnostics/read	Management Group	Read diagnostics info of APIs



Permission	Scope	Purpose
Microsoft.ApiManagement/service/apis/policies/read	Management Group	Read policies on APIs
Microsoft.ApiManagement/service/apis/read	Management Group	Read API details
Microsoft.ApiManagement/service/identityProviders/read	Management Group	Read API Management identity providers
Microsoft.ApiManagement/service/portalsettings/read	Management Group	Read developer portal settings
Microsoft.ApiManagement/service/products/policies/read	Management Group	Read policies on API products
Microsoft.ApiManagement/service/products/read	Management Group	Read API products
Microsoft.ApiManagement/service/read	Management Group	Read API Management service info
Microsoft.ApiManagement/service/tenant/read	Management Group	Read tenant info in API Management
Microsoft.AppConfiguration/configurationStores/read	Management Group	Read Azure App Configuration stores
Microsoft.app/containerapps/read	Management Group	Read App container apps
Microsoft.AppPlatform/Spring/apps/read	Management Group	Read Spring apps in Azure App Platform
Microsoft.AppPlatform/Spring/read	Management Group	Read Azure App Platform Spring resource info
Microsoft.Attestation/attestationProviders/read	Management Group	Read attestation providers
Microsoft.Authorization/classicAdministrators/read	Management Group	Read classic administrators info
Microsoft.Authorization/locks/read	Management Group	Read resource locks
Microsoft.Authorization/permissions/read	Management Group	Read permissions



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Authorization/policyAssignments/read	Management Group	Read policy assignments
Microsoft.Authorization/policyDefinitions/read	Management Group	Read policy definitions
Microsoft.Authorization/roleAssignments/read	Management Group	Read role assignments
Microsoft.Authorization/roleDefinitions/read	Management Group	Read role definitions
Microsoft.Automanage/configurationProfiles/Read	Management Group	Read Automanage configuration profiles
Microsoft.Automation/automationAccounts/credentials/read	Management Group	Read credentials in automation accounts
Microsoft.Automation/automationAccounts/hybridRunbookWorkerGroups/read	Management Group	Read hybrid runbook worker groups
Microsoft.Automation/automationAccounts/read	Management Group	Read automation accounts
Microsoft.Automation/automationAccounts/runbooks/read	Management Group	Read runbooks
Microsoft.Automation/automationAccounts/variables/read	Management Group	Read variables in automation accounts
Microsoft.AzureStackHCI/Clusters/Read	Management Group	Read Azure Stack HCI clusters
Microsoft.Batch/batchAccounts/pools/read	Management Group	Read batch account pools
Microsoft.Batch/batchAccounts/read	Management Group	Read batch accounts
Microsoft.Blueprint/blueprints/read	Management Group	Read blueprints
Microsoft.BotService/botServices/read	Management Group	Read bot services
Microsoft.Cache/redisEnterprise/read	Management Group	Read Redis Enterprise caches



Permission	Scope	Purpose
Microsoft.Cache/redis/firewallRules/read	Management Group	Read firewall rules on Redis cache
Microsoft.Cache/redis/read	Management Group	Read Redis caches
Microsoft.Cdn/profiles/afdendpoints/read	Management Group	Read CDN profile AFD endpoints
Microsoft.Cdn/profiles/afdendpoints/routes/read	Management Group	Read routes of CDN profile AFD endpoints
Microsoft.Cdn/profiles/customdomains/read	Management Group	Read custom domains in CDN profiles
Microsoft.Cdn/profiles/endpoints/customdomains/read	Management Group	Read custom domains of CDN endpoints
Microsoft.Cdn/profiles/endpoints/read	Management Group	Read CDN profile endpoints
Microsoft.Cdn/profiles/origingroups/read	Management Group	Read origin groups in CDN profiles
Microsoft.Cdn/profiles/read	Management Group	Read CDN profiles
Microsoft.Cdn/profiles/securitypolicies/read	Management Group	Read CDN profile security policies
Microsoft.Chaos/experiments/read	Management Group	Read Chaos experiments
Microsoft.classicCompute/domainNames/read	Management Group	Read Classic Compute domain names
Microsoft.ClassicCompute/VirtualMachines/read	Management Group	Read classic compute virtual machines
Microsoft.ClassicNetwork/networkSecurityGroups/read	Management Group	Read classic network security groups
Microsoft.ClassicNetwork/reservedIps/read	Management Group	Read classic network reserved IPs
Microsoft.ClassicNetwork/virtualNetworks/read	Management Group	Read classic virtual networks



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.ClassicStorage/StorageAccounts/read	Management Group	Read classic storage accounts
Microsoft.CognitiveServices/accounts/deployments/read	Management Group	Read deployments in Cognitive Services accounts
Microsoft.CognitiveServices/accounts/models/read	Management Group	Read models in Cognitive Services accounts
Microsoft.CognitiveServices/accounts/raiPolicies/read	Management Group	Read RAI policies in Cognitive Services accounts
Microsoft.CognitiveServices/accounts/read	Management Group	Read Cognitive Services accounts
Microsoft.CognitiveServices/models/read	Management Group	Read Cognitive Services models
Microsoft.Communication/CommunicationServices/Read	Management Group	Read Communication Services
Microsoft.Compute/availabilitySets/read	Management Group	Read availability sets
Microsoft.Compute/cloudServices/read	Management Group	Read cloud services
Microsoft.Compute/cloudServices/roleInstances/read	Management Group	Read cloud service role instances
Microsoft.Compute/diskEncryptionSets/read	Management Group	Read disk encryption sets
Microsoft.Compute/disks/beginGetAccess/action	Management Group	Begin get access on disks (action)
Microsoft.Compute/disks/read	Management Group	Read disks
Microsoft.Compute/galleries/images/read	Management Group	Read gallery images
Microsoft.Compute/galleries/read	Management Group	Read galleries
Microsoft.Compute/hostGroups/read	Management Group	Read host groups



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Compute/snapshots/read	Management Group	Read snapshots
Microsoft.Compute/virtualMachineScaleSets/networkInterfaces/read	Management Group	Read network interfaces of VM scale sets
Microsoft.Compute/virtualMachineScaleSets/publicIPAddresses/read	Management Group	Read public IP addresses of VM scale sets
Microsoft.Compute/virtualMachineScaleSets/read	Management Group	Read virtual machine scale sets
Microsoft.Compute/virtualMachineScaleSets/virtualmachines/instanceView/read	Management Group	Read instance view of VM scale set VMs
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ /ipConfigurations/publicIPAddresses/read	Management Group	Read public IPs of VM scale set VM NICs IP configurations
Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read	Management Group	Read virtual machines in VM scale sets
Microsoft.Compute/virtualMachines/extensions/read	Management Group	Read VM extensions
Microsoft.Compute/virtualMachines/instanceView/read	Management Group	Read VM instance view
Microsoft.Compute/virtualMachines/read	Management Group	Read virtual machines
Microsoft.Confluent/organizations/Read	Management Group	Read Confluent organizations
Microsoft.Container/containerGroups/containers/exec/action	Management Group	Execute commands in a container
Microsoft.ContainerInstance/containerGroups/containers/exec/action	Management Group	Execute commands in container instances
Microsoft.ContainerInstance/containerGroups/read	Management Group	Read container groups
Microsoft.ContainerRegistry/registries/metadata/read	Management Group	Read container registry metadata
Microsoft.ContainerRegistry/registries/pull/read	Management Group	Read/pull from container registries



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.ContainerRegistry/registries/read	Management Group	Read container registries
Microsoft.ContainerRegistry/registries/webhooks/getCallbackConfig/action	Management Group	Get webhook callback configurations
Microsoft.ContainerService/managedClusters/read	Management Group	Read managed Kubernetes clusters
Microsoft.Dashboard/grafana/read	Management Group	Read Grafana dashboards
Microsoft.DataBoxEdge/dataBoxEdgeDevices/read	Management Group	Read DataBox Edge devices
Microsoft.Databricks/accessConnectors/read	Management Group	Read Databricks access connectors
Microsoft.Databricks/workspaces/read	Management Group	Read Databricks workspaces
Microsoft.Datadog/monitors/read	Management Group	Read Datadog monitors
Microsoft.DataFactory/datafactories/read	Management Group	Read Data Factory data factories
Microsoft.DataFactory/factories/integrationruntimes/read	Management Group	Read Data Factory integration runtimes
Microsoft.DataFactory/factories/linkedservices/read	Management Group	Read Data Factory linked services
Microsoft.DataFactory/factories/read	Management Group	Read Data Factories
Microsoft.DataLakeAnalytics/accounts/dataLakeStoreAccounts/read	Management Group	Read Data Lake Analytics associated Data Lake Store accounts
Microsoft.DataLakeAnalytics/accounts/firewallRules/read	Management Group	Read Data Lake Analytics firewall rules
Microsoft.DataLakeAnalytics/accounts/read	Management Group	Read Data Lake Analytics accounts



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.DataLakeAnalytics/accounts/storageAccounts/read	Management Group	Read Data Lake Analytics storage accounts
Microsoft.DataLakeStore/accounts/firewallRules/read	Management Group	Read Data Lake Store firewall rules
Microsoft.DataLakeStore/accounts/read	Management Group	Read Data Lake Store accounts
Microsoft.DataLakeStore/accounts/trustedIdProviders/read	Management Group	Read Data Lake Store trusted ID providers
Microsoft.DataLakeStore/accounts/virtualNetworkRules/read	Management Group	Read Data Lake Store virtual network rules
Microsoft.DataMigration/services/read	Management Group	Read Data Migration services
Microsoft.DataShare/accounts/read	Management Group	Read Data Share accounts
Microsoft.DBforMariaDB/servers/firewallRules/read	Management Group	Read MariaDB server firewall rules
Microsoft.DBforMariaDB/servers/read	Management Group	Read MariaDB servers
Microsoft.DBforMySQL/flexibleServers/configurations/read	Management Group	Read MySQL flexible server configurations
Microsoft.DBforMySQL/flexibleServers/databases/read	Management Group	Read MySQL flexible server databases
Microsoft.DBforMySQL/flexibleServers/firewallRules/read	Management Group	Read MySQL flexible server firewall rules
Microsoft.DBforMySQL/flexibleServers/read	Management Group	Read MySQL flexible servers
Microsoft.DBforMySQL/servers/firewallRules/read	Management Group	Read MySQL server firewall rules
Microsoft.DBforMySQL/servers/read	Management Group	Read MySQL servers
Microsoft.DBforMySQL/servers/virtualNetworkRules/read	Management Group	Read MySQL server virtual network rules



Permission	Scope	Purpose
Microsoft.DBforPostgreSQL/flexibleServers/configurations/read	Management Group	Read PostgreSQL flexible server configurations
Microsoft.DBforPostgreSQL/flexibleServers/databases/read	Management Group	Read PostgreSQL flexible server databases
Microsoft.DBforPostgreSQL/flexibleServers/firewallRules/read	Management Group	Read PostgreSQL flexible server firewall rules
Microsoft.DBforPostgreSQL/flexibleServers/read	Management Group	Read PostgreSQL flexible servers
Microsoft.DBforPostgreSQL/servers/configurations/read	Management Group	Read PostgreSQL server configurations
Microsoft.DBforPostgreSQL/servers/firewallRules/read	Management Group	Read PostgreSQL server firewall rules
Microsoft.DBforPostgreSQL/servers/read	Management Group	Read PostgreSQL servers
Microsoft.DBforPostgreSQL/serversv2/firewallRules/read	Management Group	Read PostgreSQL servers v2 firewall rules
Microsoft.DesktopVirtualization/applicationgroups/read	Management Group	Read Desktop Virtualization application groups
Microsoft.DesktopVirtualization/hostpools/read	Management Group	Read Desktop Virtualization host pools
Microsoft.DesktopVirtualization/hostpools/sessionhostconfigurations/read	Management Group	Read Desktop Virtualization host pool session host configurations
Microsoft.DesktopVirtualization/hostpools/sessionhosts/read	Management Group	Read Desktop Virtualization host pool session hosts
Microsoft.DesktopVirtualization/workspaces/providers/Microsoft.Insights/diagnosticSettings/read	Management Group	Read Desktop Virtualization workspace diagnostic settings
Microsoft.DesktopVirtualization/workspaces/read	Management Group	Read Desktop Virtualization workspaces
Microsoft.DevCenter/devcenters/read	Management Group	Read DevCenter devcenters
Microsoft.Devices/iotHubs/privateLinkResources/Read	Management Group	Read IoT Hubs private link resources



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Devices/iotHubs/Read	Management Group	Read IoT Hubs
Microsoft.DevTestLab/schedules/read	Management Group	Read DevTestLab schedules
Microsoft.DigitalTwins/digitalTwinsInstances/read	Management Group	Read Digital Twins instances
Microsoft.DocumentDB/cassandraClusters/read	Management Group	Read DocumentDB Cassandra clusters
Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action	Management Group	List connection strings of DocumentDB accounts (action)
Microsoft.DocumentDB/databaseAccounts/listKeys/action	Management Group	List keys of DocumentDB accounts (action)
Microsoft.DocumentDB/databaseAccounts/read	Management Group	Read DocumentDB database accounts
Microsoft.DocumentDB/databaseAccounts/readonlykeys/action	Management Group	List readonly keys of DocumentDB accounts (action)
Microsoft.DomainRegistration/domains/Read	Management Group	Read Domain registrations
Microsoft.Easm/workspaces/read	Management Group	Read Easm workspaces
Microsoft.Elastic/monitors/read	Management Group	Read Elastic monitors
Microsoft.EventGrid/domains/privateLinkResources/read	Management Group	Read Event Grid domains private link resources
Microsoft.EventGrid/domains/read	Management Group	Read Event Grid domains
Microsoft.EventGrid/namespaces/read	Management Group	Read Event Grid namespaces
Microsoft.EventGrid/partnerNamespaces/read	Management Group	Read Event Grid partner namespaces
Microsoft.EventGrid/topics/privateLinkResources/read	Management Group	Read Event Grid topics private link resources



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.EventGrid/topics/read	Management Group	Read Event Grid topics
Microsoft.EventHub/clusters/read	Management Group	Read EventHub clusters
Microsoft.EventHub/namespaces/authorizationRules/read	Management Group	Read EventHub namespaces authorization rules
Microsoft.EventHub/namespaces/eventhubs/authorizationRules/read	Management Group	Read EventHub event hub authorization rules
Microsoft.EventHub/namespaces/eventhubs/read	Management Group	Read EventHub event hubs
Microsoft.EventHub/namespaces/ipfilterrules/read	Management Group	Read EventHub IP filter rules
Microsoft.EventHub/Namespace/PrivateEndpointConnections/read	Management Group	Read EventHub Namespace private endpoint connections
Microsoft.EventHub/namespaces/read	Management Group	Read EventHub namespaces
Microsoft.EventHub/namespaces/virtualnetworkrules/read	Management Group	Read EventHub virtual network rules
Microsoft.HDInsight/clusters/applications/read	Management Group	Read HDInsight cluster applications
Microsoft.HDInsight/clusters/read	Management Group	Read HDInsight clusters
Microsoft.HealthBot/healthBots/Read	Management Group	Read HealthBot bots
Microsoft.HealthcareApis/workspaces/read	Management Group	Read Healthcare APIs workspaces
Microsoft.HybridCompute/machines/read	Management Group	Read Hybrid Compute machines
Microsoft.Insights/actionGroups/read	Management Group	Read Insights action groups
Microsoft.Insights/ActivityLogAlerts/read	Management Group	Read Insights activity log alerts



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Insights/Components/read	Management Group	Read Insights components
Microsoft.Insights/DataCollectionEndpoints/Read	Management Group	Read Insights data collection endpoints
Microsoft.Insights/DataCollectionRules/Read	Management Group	Read Insights data collection rules
Microsoft.Insights/diagnosticSettings/read	Management Group	Read Insights diagnostic settings
Microsoft.Insights/eventtypes/values/read	Management Group	Read Insights event type values
Microsoft.Insights/LogProfiles/read	Management Group	Read Insights log profiles
Microsoft.Insights/MetricAlerts/Read	Management Group	Read Insights metric alerts
Microsoft.IoTCentral/IoTApps/read	Management Group	Read IoT Central applications
Microsoft.KeyVault/vaults/keys/read	Management Group	Read Key Vault keys
Microsoft.KeyVault/vaults/privateLinkResources/read	Management Group	Read Key Vault private link resources
Microsoft.KeyVault/vaults/read	Management Group	Read Key Vault vaults
Microsoft.Kusto/Clusters/Databases/read	Management Group	Read Kusto cluster databases
Microsoft.Kusto/clusters/read	Management Group	Read Kusto clusters (alternative)
Microsoft.Kusto/Clusters/read	Management Group	Read Kusto clusters
Microsoft.LabServices/labs/read	Management Group	Read Lab Services labs
Microsoft.LoadTestService/loadTests/read	Management Group	Read Load Test Service tests



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Logic/integrationAccounts/read	Management Group	Read Logic integration accounts
Microsoft.Logic/workflows/read	Management Group	Read Logic workflows
Microsoft.Logic/workflows/versions/read	Management Group	Read Logic workflow versions
Microsoft.MachineLearningServices/workspaces/computes/read	Management Group	Read Machine Learning Services workspace computes
Microsoft.MachineLearningServices/workspaces/outboundRules/read	Management Group	Read Machine Learning Services workspace outbound rules
Microsoft.MachineLearningServices/workspaces/read	Management Group	Read Machine Learning Services workspaces
Microsoft.ManagedIdentity/userAssignedIdentities/read	Management Group	Read Managed Identity user assigned identities
Microsoft.ManagedServices/marketplaceRegistrationDefinitions/read	Management Group	Read Managed Services marketplace registration definitions
Microsoft.ManagedServices/registrationAssignments/read	Management Group	Read Managed Services registration assignments
Microsoft.Management/managementGroups/descendants/read	Management Group	Read Management Groups descendants
Microsoft.Management/managementGroups/read	Management Group	Read Management Groups
Microsoft.Management/managementGroups/subscriptions/read	Management Group	Read Management Groups subscriptions
MicrosoftMaps/accounts/read	Management Group	Read Maps accounts
Microsoft.Migrate/moveCollections/read	Management Group	Read Migrate move collections
Microsoft.MixedReality/ObjectAnchorsAccounts/read	Management Group	Read Mixed Reality Object Anchors accounts



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.monitor/accounts/read	Management Group	Read Monitor accounts
Microsoft.NetApp/netAppAccounts/capacityPools/read	Management Group	Read NetApp capacity pools
Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read	Management Group	Read NetApp capacity pool volumes
Microsoft.NetApp/netAppAccounts/read	Management Group	Read NetApp accounts
Microsoft.Network/applicationGateways/read	Management Group	Read Application Gateways
Microsoft.Network/ApplicationGatewayWebApplicationFirewallPolicies/read	Management Group	Read Application Gateway Web Application Firewall Policies
Microsoft.Network/applicationSecurityGroups/read	Management Group	Read Application Security Groups
Microsoft.Network/azurefirewalls/read	Management Group	Read Azure Firewalls
Microsoft.Network/bastionHosts/read	Management Group	Read Bastion Hosts
Microsoft.Network/connections/read	Management Group	Read Network Connections
Microsoft.Network/ddosProtectionPlans/read	Management Group	Read DDoS Protection Plans
Microsoft.Network/dnsZones/read	Management Group	Read DNS Zones
Microsoft.Network/expressRouteCircuits/authorizations/read	Management Group	Read ExpressRoute Circuit authorizations
Microsoft.Network/expressRouteCircuits/peerings/connections/read	Management Group	Read ExpressRoute Circuit peerings connections
Microsoft.Network/expressRouteCircuits/peerings/peerConnections/read	Management Group	Read ExpressRoute Circuit peer connections
Microsoft.Network/expressRouteCircuits/peerings/read	Management Group	Read ExpressRoute Circuit peerings



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Network/expressRouteCircuits/read	Management Group	Read ExpressRoute Circuits
Microsoft.Network/expressRouteCrossConnections/peerings/read	Management Group	Read ExpressRoute Cross Connections peerings
Microsoft.Network/expressRouteCrossConnections/read	Management Group	Read ExpressRoute Cross Connections
Microsoft.Network/expressRouteGateways/expressRouteConnections/read	Management Group	Read ExpressRoute Gateways connections
Microsoft.Network/expressRouteGateways/read	Management Group	Read ExpressRoute Gateways
Microsoft.Network/expressRoutePorts/authorizations/read	Management Group	Read ExpressRoute Ports authorizations
Microsoft.Network/expressRoutePorts/links/read	Management Group	Read ExpressRoute Ports links
Microsoft.Network/expressRoutePortsLocations/read	Management Group	Read ExpressRoute Ports locations
Microsoft.Network/expressRoutePorts/read	Management Group	Read ExpressRoute Ports
Microsoft.Network/firewallPolicies/read	Management Group	Read Firewall Policies
Microsoft.Network/frontDoors/backendPools/read	Management Group	Read Front Door backend pools
Microsoft.Network/frontDoors/frontendEndpoints/read	Management Group	Read Front Door frontend endpoints
Microsoft.Network/frontDoors/healthProbeSettings/read	Management Group	Read Front Door health probe settings
Microsoft.Network/frontDoors/loadBalancingSettings/read	Management Group	Read Front Door load balancing settings
Microsoft.Network/frontDoors/read	Management Group	Read front doors
Microsoft.Network/frontDoors/routingRules/read	Management Group	Read Front Door routing rules



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Network/frontDoors/rulesEngines/read	Management Group	Read Front Door rules engines
Microsoft.Network/frontDoorWebApplicationFirewallPolicies/read	Management Group	Read Front Door Web Application Firewall Policies
Microsoft.NetworkFunction/azureTrafficCollectors/read	Management Group	Read Azure Traffic Collectors
Microsoft.Network/loadBalancers/read	Management Group	Read Load Balancers
Microsoft.Network/localnetworkgateways/read	Management Group	Read Local Network Gateways
Microsoft.Network/locations/usages/read	Management Group	Read Network locations usage
Microsoft.Network/natGateways/read	Management Group	Read NAT Gateways
Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action	Management Group	View and/or execute effective network security groups action
Microsoft.Network/networkInterfaces/effectiveRouteTable/action	Management Group	Execute effective route table on NICs action
Microsoft.Network/networkInterfaces/read	Management Group	Read Network Interfaces
Microsoft.Network/networkSecurityGroups/defaultSecurityRules/read	Management Group	Read Network Security Groups default security rules
Microsoft.Network/networkSecurityGroups/read	Management Group	Read Network Security Groups
Microsoft.Network/networkSecurityGroups/securityRules/read	Management Group	Read Network Security Groups security rules
Microsoft.Network/networkWatchers/queryFlowLogStatus/*	Management Group	Query NSG network watcher flow log status
Microsoft.Network/networkWatchers/read	Management Group	Read network watcher settings
Microsoft.Network/networkWatchers/read	Management Group	Read Network Watchers



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Network/networkWatchers/securityGroupView/action	Management Group	View and/or execute effective security group view action
Microsoft.Network/p2sVpnGateways/read	Management Group	Read P2S VPN Gateways
Microsoft.Network/privateDnsZones/ALL/read	Management Group	Read Private DNS Zones ALL
Microsoft.Network/privateDnsZones/read	Management Group	Read Private DNS Zones
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read	Management Group	Read Private Endpoints DNS Zone Groups
Microsoft.Network/privateEndpoints/read	Management Group	Read Private Endpoints
Microsoft.Network/privateLinkServices/read	Management Group	Read Private Link Services
Microsoft.Network/publicIPAddresses/read	Management Group	Read Public IP Addresses
Microsoft.Network/publicIPPrefixes/read	Management Group	Read Public IP Prefixes
Microsoft.Network/routeFilters/read	Management Group	Read Route Filters
Microsoft.Network/routeFilters/routeFilterRules/read	Management Group	Read Route Filter Rules
Microsoft.Network/routeTables/read	Management Group	Read Route Tables
Microsoft.Network/routeTables/routes/read	Management Group	Read Route Table Routes
Microsoft.Network/serviceEndpointPolicies/read	Management Group	Read Service Endpoint Policies
Microsoft.Network/serviceEndpointPolicies/serviceEndpointPolicyDefinitions/read	Management Group	Read Service Endpoint Policy Definitions
Microsoft.Network/trafficManagerProfiles/read	Management Group	Read Traffic Manager Profiles



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.network/virtualnetworkgateways/connections/read	Management Group	Read Virtual network gateways connections
Microsoft.Network/virtualNetworkGateways/read	Management Group	Read Virtual Network Gateways
Microsoft.Network/virtualNetworks/read	Management Group	Read Virtual Networks
Microsoft.Network/virtualNetworks/subnets/read	Management Group	Read Virtual Network Subnets
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read	Management Group	Read Virtual Network Peerings
Microsoft.Network/virtualWans/read	Management Group	Read Virtual WANs
Microsoft.Network/virtualwans/vpnconfiguration/action	Management Group	Download and/or execute VPN configuration action
Microsoft.Network/vpnServerConfigurations/read	Management Group	Read VPN Server Configurations
Microsoft.NotificationHubs/NamespaceNamespaces/NotificationHubs/read	Management Group	Read Notification Hubs
Microsoft.NotificationHubs/NamespaceNamespaces/read	Management Group	Read Notification Hub namespaces
Microsoft.OperationalInsights/clusters/read	Management Group	Read Operational Insights clusters
Microsoft.OperationalInsights/querypacks/read	Management Group	Read Operational Insights query packs
Microsoft.OperationalInsights/workspaces/read	Management Group	Read Operational Insights workspaces
Microsoft.OperationalInsights/workspaces/tables/read	Management Group	Read Operational Insights workspace tables
Microsoft.Orbital/spacecrafts/read	Management Group	Read Orbital spacecrafts
Microsoft.PowerBIDedicated/capacities/read	Management Group	Read Power BI Dedicated capacities



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.PowerBIDedicated/servers/read	Management Group	Read Power BI Dedicated servers
Microsoft.Quantum/Workspaces/Read	Management Group	Read Quantum Workspaces
Microsoft.RecoveryServices/vaults/backupPolicies/read	Management Group	Read Recovery Services Vault backup policies
Microsoft.RecoveryServices/Vaults/backupProtectedItems/read	Management Group	Read Recovery Services Vault backup protected items
Microsoft.RecoveryServices/Vaults/read	Management Group	Read Recovery Services Vaults
Microsoft.RedHatOpenShift/openShiftClusters/read	Management Group	Read Red Hat OpenShift clusters
Microsoft.Relay/Namespaces/read	Management Group	Read Relay namespaces
Microsoft.Resources/Resources/read	Management Group	Read generic resources
Microsoft.Resources/subscriptions/providers/read	Management Group	Read subscription providers
Microsoft.Resources/subscriptions/read	Management Group	Read subscriptions
Microsoft.Resources/subscriptions/resourceGroups/read	Management Group	Read resource groups
Microsoft.Resources/subscriptions/resourceGroups/write	Management Group	Write resource groups
Microsoft.Resources/templateSpecs/read	Management Group	Read template specs
Microsoft.SaaS/applications/read	Management Group	Read SaaS applications
Microsoft.Search/searchServices/dataSources/read	Entire Subscription	Read Azure Search service data sources
Microsoft.Search/searchServices/indexers/read	Entire Subscription	Read Azure Search service indexers



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Search/searchServices/indexes/documents/read	Entire Subscription	Read Azure Search service indexer documents
Microsoft.Search/searchServices/indexes/read	Entire Subscription	Read Azure Search service indexes
Microsoft.Search/searchServices/listAdminKeys/action	Entire Subscription	Retrieve the administrative API keys required to authenticate and manage the search service
Microsoft.Search/searchServices/listQueryKeys/action	Entire Subscription	
Microsoft.Search/searchServices/PrivateEndpointConnectionsApproval/action	Entire Subscription	
Microsoft.Search/searchServices/read	Entire Subscription	Read Azure Search services
Microsoft.Security/advancedThreatProtectionSettings/read	Management Group	Read Security advanced threat protection settings
Microsoft.Security/automations/read	Management Group	Read Security automations
Microsoft.Security/autoProvisioningSettings/read	Management Group	Read Security auto provisioning settings
Microsoft.Security/iotSecuritySolutions/read	Management Group	Read IoT Security Solutions
Microsoft.Security/locations/jitNetworkAccessPolicies/read	Management Group	Read Just-in-Time network access policies
Microsoft.Security/locations/read	Management Group	Read Security locations
Microsoft.Security/pricings/read	Management Group	Read Security pricings
Microsoft.Security/secureScores/read	Management Group	Read Security secure scores
Microsoft.Security/securityContacts/read	Management Group	Read Security contacts
Microsoft.Security/settings/read	Management Group	Read Security settings



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Security/workspaceSettings/read	Management Group	Read Security workspace settings
Microsoft.ServiceBus/namespaces/authorizationRules/read	Management Group	Read Service Bus namespace authorization rules
Microsoft.ServiceBus/namespaces/networkrulesets/read	Management Group	Read Service Bus namespace network rule sets
Microsoft.ServiceBus/namespaces/privateEndpointConnections/read	Management Group	Read Service Bus namespace private endpoint connections
Microsoft.ServiceBus/namespaces/providers/Microsoft.Insights/diagnosticSettings/read	Management Group	Read Service Bus namespace diagnostic settings
Microsoft.ServiceBus/namespaces/queues/read	Management Group	Read Service Bus queues
Microsoft.ServiceBus/namespaces/read	Management Group	Read Service Bus namespaces
Microsoft.ServiceBus/namespaces/topics/read	Management Group	Read Service Bus topics
Microsoft.ServiceBus/namespaces/topics/subscriptions/read	Management Group	Read Service Bus topic subscriptions
Microsoft.ServiceFabric/clusters/read	Management Group	Read Service Fabric clusters
Microsoft.SignalRService/SignalR/read	Management Group	Read SignalR Service SignalR
Microsoft.SignalRService/WebPubSub/read	Management Group	Read SignalR Web PubSub
Microsoft.Solutions/applications/read	Management Group	Read Solutions applications
Microsoft.Sql/managedInstances/databases/read	Management Group	Read SQL managed instances databases
Microsoft.Sql/managedInstances/databases/transparentDataEncryption/read	Management Group	Read SQL managed instances databases Transparent Data Encryption



Permission	Scope	Purpose
Microsoft.Sql/managedInstances/encryptionProtector/Read	Management Group	Read SQL managed instances encryption protector
Microsoft.Sql/managedInstances/read	Management Group	Read SQL managed instances
Microsoft.Sql/managedInstances/vulnerabilityAssessments/Read	Management Group	Read SQL managed instances vulnerability assessments
Microsoft.Sql/servers/administrators/read	Management Group	Read SQL server administrators
Microsoft.Sql/servers/auditingSettings/read	Management Group	Read SQL server auditing settings
Microsoft.Sql/servers/databases/auditingSettings/read	Management Group	Read SQL server databases auditing settings
Microsoft.Sql/servers/databases/dataMaskingPolicies/read	Management Group	Read SQL server databases data masking policies
Microsoft.Sql/servers/databases/dataMaskingPolicies/rules/read	Management Group	Read SQL server databases data masking policies rules
Microsoft.Sql/servers/databases/read	Management Group	Read SQL server databases
Microsoft.Sql/servers/databases/securityAlertPolicies/read	Management Group	Read SQL server databases security alert policies
Microsoft.Sql/servers/databases/transparentDataEncryption/read	Management Group	Read SQL server databases Transparent Data Encryption
Microsoft.Sql/servers/encryptionProtector/read	Management Group	Read SQL server encryption protector
Microsoft.Sql/servers/firewallRules/read	Management Group	Read SQL server firewall rules
Microsoft.Sql/servers/read	Management Group	Read SQL servers
Microsoft.Sql/servers/securityAlertPolicies/read	Management Group	Read SQL server security alert policies
Microsoft.Sql/servers/vulnerabilityAssessments/read	Management Group	Read SQL server vulnerability assessments



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.SqlVirtualMachine/sqlVirtualMachines/read	Management Group	Read SQL Virtual Machines
Microsoft.StorageCache/caches/read	Management Group	Read Storage Cache caches
Microsoft.StorageCache/Subscription/caches/read	Management Group	Read Storage Cache subscription caches
Microsoft.StorageMover/storageMovers/read	Management Group	Read Storage Mover storage movers
Microsoft.Storage/storageAccounts/blobServices/read	Management Group	Read Storage blob services
Microsoft.Storage/storageAccounts/fileServices/read	Management Group	Read Storage file services
Microsoft.Storage/storageAccounts/fileServices/shares/read	Management Group	Read Storage file shares
Microsoft.Storage/storageAccounts/listKeys/action	Management Group	List Storage account keys (action)
Microsoft.Storage/storageAccounts/providers/Microsoft.Insights/diagnosticSettings/read	Management Group	Read Storage account diagnostic settings
Microsoft.Storage/storageAccounts/queueServices/read	Management Group	Read Storage queue services
Microsoft.Storage/storageAccounts/read	Management Group	Read Storage accounts
Microsoft.Storage/storageAccounts/tableServices/read	Management Group	Read Storage table services
Microsoft.StorageSync/storageSyncServices/privateLinkResources/read	Management Group	Read Storage Sync private link resources
Microsoft.StorageSync/storageSyncServices/read	Management Group	Read Storage Sync services
Microsoft.StreamAnalytics/clusters/Read	Management Group	Read Stream Analytics clusters
Microsoft.StreamAnalytics/streamingjobs/Read	Management Group	Read Stream Analytics streaming jobs



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Subscription/Policies/default/read	Management Group	Read Subscription default policies
Microsoft.Synapse/privateLinkHubs/privateLinkResources/read	Management Group	Read Synapse private link hubs private link resources
Microsoft.Synapse/privateLinkHubs/read	Management Group	Read Synapse private link hubs
Microsoft.Synapse/workspaces/privateLinkResources/read	Management Group	Read Synapse workspace private link resources
Microsoft.Synapse/workspaces/read	Management Group	Read Synapse workspaces
Microsoft.Synapse/workspaces/sparkConfigurations/read	Management Group	Read Synapse workspaces spark configurations
Microsoft.Synapse/workspaces/sqlPools/geoBackupPolicies/read	Management Group	Read Synapse workspaces SQL pools geo backup policies
Microsoft.Synapse/workspaces/sqlPools/read	Management Group	Read Synapse workspaces SQL pools
Microsoft.VideoIndexer/accounts/read	Management Group	Read Video Indexer accounts
Microsoft.VisualStudio/Account/Read	Management Group	Read Visual Studio accounts
Microsoft.Web/certificates/read	Management Group	Read Web certificates
Microsoft.Web/customApis/read	Management Group	Read Web custom APIs
Microsoft.Web/hostingEnvironments/Read	Management Group	Read Web hosting environments
Microsoft.Web/serverfarms/Read	Management Group	Read Web server farms
Microsoft.web/serverfarms/sites/read	Management Group	Read Server farms sites
Microsoft.Web/sites/basicPublishingCredentialsPolicies/Read	Management Group	Read Web sites basic publishing credentials policies



Permission	Scope	Purpose
Microsoft.web/sites/config/appsettings/read	Management Group	Read Web sites app settings
Microsoft.Web/sites/config/list/action	Management Group	Execute action to list Web site configuration
Microsoft.Web/sites/config/read	Management Group	Read Web sites configuration
Microsoft.web/sites/functions/action	Management Group	Invoke or trigger specific Azure Functions hosted within a Web App/Function App
Microsoft.web/sites/functions/read	Management Group	Read Web Sites functions
Microsoft.Web/sites/privateEndpointConnections/Read	Management Group	Read Web sites private endpoint connections
Microsoft.Web/sites/publishxml/Action	Management Group	Retrieve the publishing profile (XML) used to authenticate and deploy code or configurations to the Azure Web App
Microsoft.Web/sites/read	Management Group	Read Web sites
Microsoft.Web/sites/Read	Management Group	Read Web sites
Microsoft.Web/sites/slots/Read	Management Group	Read Web sites slots
Microsoft.Web/staticSites/Read	Management Group	Read Web static sites
Microsoft.Workloads/monitors/read	Management Group	Read Workloads monitors
Organization.Read.All	Tenants or management groups using Microsoft Graph	Read all properties and data of the current Azure Active Directory (AD) organization (tenant)
Policy.Read.All	Tenants or management groups using Microsoft Graph	Read all policies configured in Azure Active Directory (AD)



Permission	Scope	Purpose
Policy.ReadWrite.AuthenticationMethod	Tenants or management groups using Microsoft Graph	Read and write (configure/modify) all user authentication methods in Azure Active Directory (AD)
*/read	Management Group	Read-only access, used to get metadata of all managed data assets in the subscription
RoleManagement.Read.All	Tenants or management groups using Microsoft Graph	Read all Azure Active Directory (AD) role definitions and role assignments within the organization
User.Read.All	Tenants or management groups using Microsoft Graph	Read the full set of profile properties and data for every user in the organization's directory

#### Log Collection

Permission	Scope	Purpose
Azure Event Hubs Data Receiver	Event Hub namespaces starting with the prefix <b>CortexEventHubNamespace</b>	Used for audit log collection. Logs are collected via Event Hubs and are later collected.
Storage Blob Data Contributor	Resources starting with the prefix <b>cxa</b>	Used for audit log collection. Logs are stored in a dedicated storage account and are later collected.

#### Registry Scan

Permission	Scope	Purpose
Microsoft.ContainerRegistry/registries/metadata/read	Management Group	Enable the retrieval of manifest and tag information for images stored in the container registry
Microsoft.ContainerRegistry/registries/pull/read	Management Group	Enable the pulling (downloading) of container images from the repository for scanning or deployment
Microsoft.ContainerRegistry/registries/read	Management Group	Enable the reading of general properties and metadata about the container registry itself
Microsoft.ContainerRegistry/registries/webhooks/get	<b>Callback Configuration</b>	Enable the retrieval of the callback URL and configuration details for a registry webhook

#### Outposts



Permission	Scope	Purpose
Microsoft.Compute/disks/delete	Resource group	Delete disks after scanning has finished. This action is critical for remediation and resource hygiene, preventing data exfiltration, and reducing the attack surface. For example, the outpost can delete dangling disks, which are a significant security risk.
Microsoft.Compute/disks/read	Resource group	Retrieve disk metadata for identifying, for example, dangling disks.
Microsoft.Compute/disks/write	Resource group	Create a disk from a snapshot before attaching it to a workload. This permission is essential for dynamic scanning and analysis. It enables the creation of a temporary disk copy from a snapshot, a necessary step to analyze a workload without affecting the live environment.
Microsoft.Compute/locations/usages/read	Resource group	View regional usage and quota limits for compute resources
Microsoft.Compute/skus/read	Resource group	View available VM sizes (SKUs) for dynamic size selection
Microsoft.Compute/virtualMachines/delete	Resource group	Delete a scanner or proxy VM. This permission is necessary for secure lifecycle management. It ensures that Cortex Cloud can clean up and delete temporary VMs, such as scanner or proxy VMs, after a security task is complete. This prevents them from becoming an unmonitored risk.
Microsoft.Compute/virtualMachines/read	Resource group	View a scanner or proxy VM
Microsoft.Compute/virtualMachines/write	Resource group	Create a scanner or proxy VM. This is a core provisioning permission required to dynamically deploy security resources. This is needed for creating ephemeral scanner or proxy VMs that are spun up to perform specific security tasks.
Microsoft.ManagedIdentity/userAssignedIdentities/assign	Resource group	Assign a user-assigned managed identity to a resource. This is a fundamental permission for secure, credential-less access. It allows the outpost to assign a managed identity to a resource, which is a best practice for securely authenticating to other Azure services without needing to store or manage static credentials.
Microsoft.Network/applicationSecurityGroups/joinIpConfigurations	Resource group	Attach an NIC IP configuration to an Application Security Group. This permission is required for Cortex Cloud to perform its core security functions, ensuring it has the necessary access to monitor and manage resources within the customer's account.



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Network/networkInterfaces/delete	Resource group	Delete NICs. This delete permission is critical for network security hygiene. It allows Cortex to clean up temporary or unused network resources, such as network interfaces (NICs) or public IPs, to prevent them from becoming dangling resources and a potential security risk.
Microsoft.Network/networkInterfaces/join/action	Resource group	Attach NICs to VMs. This permission is necessary for secure network configuration. It enables Cortex to connect a VM's network interface to the correct subnet or security group, ensuring it can communicate securely and in accordance with the network's security policy.
Microsoft.Network/networkInterfaces/read	Resource group	View network interface (NIC) properties.
Microsoft.Network/networkInterfaces/write	Resource group	Create or update NICs. This write permission is required to configure the network for secure operations. It allows Cortex to create or update network components like NICs, public IPs, or private endpoints, which is necessary to ensure secure and isolated communication for its security tools.
Microsoft.Network/networkSecurityGroups/join/action	Resource group	Associate NICs or subnets with a Network Security Group. This permission is necessary for secure network configuration. It enables Cortex to connect a VM's network interface to the correct subnet or security group, ensuring it can communicate securely and in accordance with the network's security policy.
Microsoft.Network/operations/read	Resource group	View available network-related operations used for work with private endpoints.
Microsoft.Network/privateEndpoints/delete	Resource group	Delete permission is critical for network security hygiene. It allows Cortex to clean up temporary or unused network resources, such as network interfaces (NICs) or public IPs, to prevent them from becoming dangling resources and a potential security risk.
Microsoft.Network/privateEndpoints/read	Resource group	View private endpoint properties.
Microsoft.Network/privateEndpoints/write	Resource group	Create or update private endpoints. This write permission is required to configure the network for secure operations. It allows Cortex to create or update network components like NICs, public IPs, or private endpoints, which is necessary to ensure secure and isolated communication for its security tools.



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Network/publicIPAddresses/delete	Resource group	Delete unused public IPs. This delete permission is critical for network security hygiene. It allows Cortex to clean up temporary or unused network resources, such as network interfaces (NICs) or public IPs, to prevent them from becoming dangling resources and a potential security risk.
Microsoft.Network/publicIPAddresses/join/action	Resource group	Attach public IPs to NIC of proxy VM. This permission is necessary for secure network configuration. It enables Cortex to connect a VM's network interface to the correct subnet or security group, ensuring it can communicate securely and in accordance with the network's security policy.
Microsoft.Network/publicIPAddresses/read	Resource group	List existing static public IPs that can be used by proxy VMs.
Microsoft.Network/publicIPAddresses/write	Resource group	Create or update public IPs. This write permission is required to configure the network for secure operations. It allows Cortex to create or update network components like NICs, public IPs, or private endpoints, which is necessary to ensure secure and isolated communication for its security tools.
Microsoft.Network/virtualNetworks/subnets/join/action	Resource group	Attach NICs to a subnet. This permission is necessary for secure network configuration. It enables Cortex to connect a VM's network interface to the correct subnet or security group, ensuring it can communicate securely and in accordance with the network's security policy.
Microsoft.Network/virtualNetworks/subnets/joinViaServiceEndpoint/action	Resource group	Enable usage of a subnet's service endpoint by scanner VM to access managed services. This permission is necessary for secure network configuration. It enables Cortex to connect a VM's network interface to the correct subnet or security group, ensuring it can communicate securely and in accordance with the network's security policy.
Microsoft.ResourceGraph/resources/read	Resource group	Query spot eviction history rates using Azure Resource Graph for dynamic VM size selection.

Onboarding managed identity

Managed identity is used by compliance policy to onboard the subscriptions.

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Authorization/policyAssignments/*	Management Group and Tenant	Assign compliance policies. When onboarding, we assign a compliance policy to the selected management group or tenant.



<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Authorization/policyDefinitions/*	Management Group and Tenant	Define compliance policies to ensure all subscriptions within a management group are fully onboarded
Microsoft.Authorization/*/read	Management Group and Tenant	Read audit log collection
Microsoft.Authorization/roleAssignments/*	Management Group and Tenant	Assign role to the onboarding identity. Used to onboard subscriptions. Roles and assignments are used by different modules to grant minimal access to the monitored subscription.
Microsoft.Authorization/roleDefinitions/*	Management Group and Tenant	Create a role for the onboarding identity. Used to onboard subscriptions. Roles and assignments are used by different modules to grant minimal access to the monitored subscription.
Microsoft.Compute/galleries/*	Management Group and Tenant	Used to onboard the ADS module. Gallery is used for image scanning
Microsoft.EventHub/namespaces/*	Management Group and Tenant	Audit logs are collected by Event Hubs and later collected for analysis
Microsoft.Insights/diagnosticSettings/*	Management Group and Tenant	Diagnostic settings are part of the audit logs that are collected by Event Hubs and later collected for analysis
Microsoft.Resources/deployments/*	Management Group and Tenant	Used to create deployments that will onboard future subscriptions. The deployments are created by remediation tasks for the Cortex compliance policy created when first onboarding.
Microsoft.Resources/subscriptions/read	Management Group and Tenant	Facilitate onboarding of subscriptions in the defined scope
Microsoft.Resources/subscriptions/resourceGroups/*	Management Group and Tenant	Used to onboard subscriptions. The resource group is used by different modules for scanning and to facilitate workload separation.

Automations

<b>Permission</b>	<b>Scope</b>	<b>Purpose</b>
Microsoft.Authorization/policyAssignments/read	Subscription	Read the configuration of Microsoft Defender for Cloud policy assignments



Permission	Scope	Purpose
Microsoft.Authorization/policyAssignments/write	Subscription	Apply Microsoft Defender for Cloud policy assignments to enable security configurations monitoring. This helps remediate issues detected by the "Azure Microsoft Defender for Cloud security configurations monitoring is set to disabled" rule.
Microsoft.Compute/disks/read	Subscription	Read the configuration of the Azure VM disk
Microsoft.Compute/disks/write	Subscription	Modify the Azure VM disk configuration to disable public network access. This helps remediate issues detected by the "Azure VM disk configured with public network access" rule.
Microsoft.Compute/virtualMachines/powerOff/action	Subscription	Power off an existing Azure Virtual Machine. This permission is specifically required to change the state of a VM from <b>Running</b> to <b>Stopped</b> or <b>Deallocated</b> . It is necessary when you want the VM to stop running and thus stop incurring compute charges, unlike the delete permission which removes the resource entirely. Required for command: <b>azure-vm-instance-power-off</b>
Microsoft.Compute/virtualMachines/read	Subscription	Read the status and configuration details of an existing Azure Virtual Machine (VM). This permission is necessary for any monitoring, inventory, or auditing system that needs to know information like the VM size, operating system, network configuration, tags, and whether the VM is currently running or stopped. Required for command: <b>azure-vm-instance-details-get</b>
Microsoft.Compute/virtualMachines/start/action	Subscription	Power on an existing Azure Virtual Machine (VM) to change the state of a VM from <b>Stopped</b> to <b>Running</b> . Required for command: <b>azure-vm-instance-start</b>
Microsoft.Consumption/budgets/read	Subscription	Read the configuration and current status of established Azure budgets
Microsoft.Consumption/usageDetails/read	Subscription	Read detailed usage information for resources, including costs and quantity
Microsoft.ContainerRegistry/registries/read	Subscription	Read the configuration of the Azure Container Registry (ACR)
Microsoft.ContainerRegistry/registries/write	Subscription	Update the Azure Container Registry (ACR) configuration to disable exports. This helps remediate issues detected by the "Azure Container Registry with exports enabled" rule.



Permission	Scope	Purpose
Microsoft.CostManagement/forecast/read	Subscription	Read predictive forecasts and historical trends for future Azure costs
Microsoft.DBforMySQL/flexibleServers/configurations/read	Subscription	Read the configuration settings of the Azure MySQL flexible server
Microsoft.DBforMySQL/flexibleServers/configurations/write	Subscription	Update the Azure MySQL flexible server configuration to enforce SSL. This helps remediate issues detected by the "Azure MySQL database flexible server SSL enforcement is disabled" rule.
Microsoft.DBforPostgreSQL/servers/configurations/read	Subscription	Read the configurations of the Azure PostgreSQL server
Microsoft.DBforPostgreSQL/servers/configurations/write	Subscription	Update the Azure PostgreSQL server configurations to enable the connection throttling parameter. This helps remediate issues detected by the "Azure PostgreSQL database server with connection throttling parameter is disabled" rule.
Microsoft.DBforPostgreSQL/servers/read	Subscription	Read the configuration of the Azure PostgreSQL server
Microsoft.DBforPostgreSQL/servers/write	Subscription	Update the Azure PostgreSQL server configuration to enable the SSL connection feature. This helps remediate issues detected by the "Azure PostgreSQL database server with SSL connection disabled" rule.
Microsoft.DocumentDB/databaseAccounts/read	Subscription	Read the configuration of the Azure Cosmos DB database account
Microsoft.DocumentDB/databaseAccounts/write	Subscription	Modify the Azure Cosmos DB account to disable key-based metadata write authentication. This helps remediate issues detected by the "Azure Cosmos DB key based authentication is enabled" rule.
Microsoft.Insights/logprofiles/read	Subscription	Read the configuration of the Azure Activity Log profile
Microsoft.Insights/logprofiles/write	Subscription	Set the Azure Activity Log retention period to 365 days or more. This helps remediate issues detected by the "Azure Activity Log retention should not be set to less than 365 days" rule.
Microsoft.KeyVault/vaults/read	Subscription	Read the configuration and properties of the Azure Key Vault



Permission	Scope	Purpose
Microsoft.KeyVault/vaults/write	Subscription	Modify the Key Vault configuration to ensure it is recoverable. This helps remediate issues detected by the "Azure Key Vault is not recoverable" rule.
Microsoft.Network/networkInterfaces/read	Subscription	Read the list of Network Security Group (NSG) Interfaces. Required for command: <code>azure-nsg-network-interfaces-list</code>
Microsoft.Network/networkSecurityGroups/read	Subscription	Read the list of the Network Security Groups (NSGs). Required for command: <code>azure-nsg-security-groups-list</code>
Microsoft.Network/networkSecurityGroups/securityRules/* Microsoft.Network/networkSecurityGroups/securityRules/read Microsoft.Network/networkSecurityGroups/securityRules/delete Microsoft.Network/networkSecurityGroups/securityRules/get Microsoft.Network/networkSecurityGroups/securityRules/create	Subscription	Delete a Network Security Group (NSG) rule to stop overly permissive outbound traffic. This helps remediate issues detected by the "Azure Network Security Group with overly permissive outbound rule" rule. Required for command: <code>azure-nsg-security-rule-delete</code>
Microsoft.Network/networkSecurityGroups/securityRules/* Microsoft.Network/networkSecurityGroups/securityRules/read Microsoft.Network/networkSecurityGroups/securityRules/delete Microsoft.Network/networkSecurityGroups/securityRules/get Microsoft.Network/networkSecurityGroups/securityRules/create	Subscription	Read the configuration of a Network Security Group (NSG) rule to assess traffic permissions. Required for command: <code>azure-nsg-security-rule-get</code>
Microsoft.Network/networkSecurityGroups/securityRules/* Microsoft.Network/networkSecurityGroups/securityRules/read Microsoft.Network/networkSecurityGroups/securityRules/delete Microsoft.Network/networkSecurityGroups/securityRules/get Microsoft.Network/networkSecurityGroups/securityRules/create	Subscription	Modify a Network Security Group (NSG) rule to stop overly permissive outbound traffic. This helps remediate issues detected by the "Azure Network Security Group with overly permissive outbound rule" rule. Required for command: <code>azure-nsg-security-rule-create</code>
Microsoft.Network/publicIPAddresses/read	Subscription	Read and list the Network Security Group (NSG) and VM public IP addresses and details. Required for commands: <code>azure-nsg-public-ip-addresses-list</code> and <code>azure-vm-public-ip-details-get</code>
Microsoft.Resources/subscriptions/read	Subscription	Read the status and details of an Azure subscription. Required for command: <code>azure-nsg-subscriptions-list</code>
Microsoft.Resources/subscriptions/resourceGroups/* Microsoft.Resources/subscriptions/resourceGroups/read	Subscription	Read the status and details of resource groups within a subscription. Required for command: <code>azure-nsg-resource-group-list</code>
Microsoft.Sql/servers/databases/securityAlertPolicies/* Microsoft.Sql/servers/databases/securityAlertPolicies/read	Subscription	Read the security alert policy configuration for an Azure SQL Database



Permission	Scope	Purpose
Microsoft.Sql/servers/databases/securityAlertPolicies	Subscription	Update the security alert policy for an Azure SQL Database to enable email notifications for Threat Detection. This helps remediate issues detected by the "Azure SQL Databases with disabled Email service and co-administrators for Threat Detection" rule.
Microsoft.Sql/servers/databases/transparentDataEncryption	Subscription	Read the Transparent Data Encryption (TDE) status for an Azure SQL database
Microsoft.Sql/servers/databases/transparentDataEncryption	Subscription	Enable Transparent Data Encryption (TDE) on an Azure SQL database. This helps remediate issues detected by the "Azure SQL database Transparent Data Encryption (TDE) encryption disabled" rule.
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read	Subscription	Read or download the content of a blob (file) stored in Azure Storage. This permission is necessary for any application or user that needs to access the actual data stored inside the containers of an Azure Storage Account. Required for commands: <code>azure-storage-container-blob-get</code> and <code>azure-storage-container-blob-property-get</code>
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/read	Subscription	Read the index tags (metadata) applied to a specific blob (file) in Azure Storage. This permission is necessary for any application or user that needs to query or filter blobs based on the custom tags applied to them, without necessarily reading the entire blob content. Required for command: <code>azure-storage-container-blob-tag-get</code>
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write	Subscription	Write, set, or update the index tags (metadata) applied to a specific blob (file) in Azure Storage. This permission is necessary for any application or user that needs to modify the custom index tags on blobs, which is crucial for data lifecycle management and searching. Required for command: <code>azure-storage-container-blob-tag-set</code>
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write	Subscription	Write, upload, or create a new blob (file) in Azure Storage, or overwrite the content of an existing blob. This permission is necessary for any application or user that needs to store new data or modify existing file data within the containers of an Azure Storage Account. Required for command: <code>azure-storage-container-blob-property-set</code>



Permission	Scope	Purpose
Microsoft.Storage/storageAccounts/blobServices/config/delete	Subscription	Enable delete functionality on the Azure Storage account blob service containers. Required for command: <code>azure-storage-container-delete</code>
Microsoft.Storage/storageAccounts/blobServices/config/read	Subscription	Read the configuration of Azure Storage account blob service containers. Required for command: <code>azure-storage-container-property-get</code>
Microsoft.Storage/storageAccounts/blobServices/config/write	Subscription/ACL/action	Set or modify the access control list (ACL) for folders or files within a storage container
Microsoft.Storage/storageAccounts/blobServices/config/update	Subscription	Enable modification of Azure Storage account blob service containers. Required for command: <code>azure-storage-blob-containers-update</code>
Microsoft.Storage/storageAccounts/blobServices/read	Subscription	Read the configuration of the Azure Storage account blob service. Required for command: <code>azure-storage-blob-service-properties-get</code>
Microsoft.Storage/storageAccounts/blobServices/write	Subscription	Enable soft delete functionality on the Azure Storage account blob service. This helps remediate issues detected by the "Azure Storage account soft delete is disabled" rule.
Microsoft.Storage/storageAccounts/read	Subscription	Read the configuration of the Azure Storage Account
Microsoft.Storage/storageAccounts/write	Subscription	Enable access for trusted Microsoft services. This helps remediate issues detected by the "Azure Storage Account 'Trusted Microsoft Services' access not enabled" rule.
Microsoft.Web/sites/config/read	Subscription	Read the configuration settings of the Azure App Service Web app
Microsoft.Web/sites/config/write	Subscription	Set the HTTP version to 2.0 within the Azure App Service Web app configuration. This helps remediate issues detected by the "Azure App Service Web app doesn't use HTTP 2.0" rule.
Microsoft.Web/sites/read	Subscription	Read the status and properties of the Azure App Service Web app
Microsoft.Web/sites/write	Subscription	Set the HTTPS-only feature for the Azure App Service Web app to enforce redirection from HTTP to HTTPS. This helps remediate issues detected by the "Azure App Service Web app doesn't redirect HTTP to HTTPS" rule. Required for command: <code>azure-webapp-update</code>



## Abstract

List of Oracle Cloud Infrastructure provider permissions for Cortex Cloud.

ADS

Permission	Module	Scope	Purpose
Admit group CortexOutpostGroup of tenancy CortexOutpost to use volumes in tenancy	ADS	In tenancy	Allow creation of backups from volumes
Admit group CortexOutpostGroup of tenancy CortexOutpost to use key-delegate in tenancy	ADS	In tenancy	Re-encrypt backups during copy/restore operations
Admit group CortexOutpostGroup of tenancy CortexOutpost to associate keys in tenancy with volumes in tenancy CortexOutpost	ADS	Volumes in tenancy	Associate encryption keys with volumes during backup/restore
Admit group CortexOutpostGroup of tenancy CortexOutpost to use tag-namespaces in tenancy	ADS	In tenancy	Enable tagging for permission scoping, resource tracking, and cost visibility
Admit group CortexOutpostGroup of tenancy CortexOutpost to manage boot-volume-backups in tenancy where request.operation != 'DeleteBootVolumeBackup'	ADS	Excludes delete	Allow full management of boot volume backups except deletion
Admit group CortexOutpostGroup of tenancy CortexOutpost to manage boot-volume-backups in tenancy where target.resource.tag.cortex_m-o-lcaas_id.panw_capability = 'cortex-scan-platform'	ADS	Only boot-volume-backups tagged with panw_capability = cortex-scan-platform	Restrict deletion to Cortex scan-related resources only
Admit group CortexOutpostGroup of tenancy CortexOutpost to read all-resources in tenancy	ADS	In tenancy	Read-only access to all resources

## Discovery Engine

"Discovery Engine" read only access. Grants read-only access to OCI tenancy and resources.

## Registry Scan

Table 2. Dynamic Group Permissions

Permission	Scope	Purpose
Allow dynamic-group registry-scan to manage buckets in tenancy	Tag-scoped (project_id)	Manage Object Storage buckets for scan artifacts/results
Allow dynamic-group registry-scan to manage objects in tenancy	Tag-scoped (project_id)	Upload/download image layers, manifests, and reports
Allow dynamic-group registry-scan to read secret-bundles in tenancy	Tag-scoped (project_id)	Retrieve registry credentials from OCI Vault



Permission	Scope	Purpose
Endorse dynamic-group registry-scan to read repos in any-tenancy	Cross-tenancy	Allow cross-tenancy image pulls for scans

Table 3. Inherited Base Permissions for Registry scanning

Permission	Scope	Purpose
Allow any-user to manage buckets in tenancy	Tag-scoped (project_id)	Create/manage buckets for scan data
Allow any-user to manage objects in tenancy	Tag-scoped (project_id)	Read/write objects (artifacts, logs, results)
Allow any-user to use keys in tenancy	Tag-scoped (project_id)	Decrypt secrets for registry access
Allow any-user to manage secret-versions in tenancy	Tag-scoped (project_id)	Rotate credentials and manage secret versions
Allow any-user to manage secrets in tenancy	Tag-scoped (project_id)	Create/update secrets for scanners
Allow any-user to manage secret-family in tenancy	Tag-scoped (project_id)	Broader secret-management rights
Allow any-user to manage vaults in tenancy	Tag-scoped (project_id)	Create/administer Vaults for key and secret storage
Allow any-user to inspect tag-family in tenancy	Global	Discover tag namespaces/definitions
Allow any-user to use tag-family (namespace=cortex_cloud, managed_by=PANW)	Restricted	Restrict tag usage to Palo Alto-managed groups
Endorse any-group to use tag-namespaces in any-tenancy	Cross-tenancy	Allow tag namespace usage across tenancies

## 2.2.7 | Onboard the Kubernetes Connector

### Abstract

To onboard your Kubernetes cluster, choose the capabilities that fit your needs and download the Helm chart values. Install the Helm charts in your Kubernetes environment to grant Cortex Cloud permissions to collect the data.

Follow this wizard to deploy your Kubernetes Connector. The Kubernetes onboarding wizard is designed to facilitate the seamless setup of Kubernetes data into Cortex Cloud. The guided experience requires minimal user input; simply select the capabilities that fit your needs and download the custom installer file. For full control of the setup, you can use the advanced settings. Based on the onboarding settings, Cortex Cloud then creates a custom installer file for running in your Kubernetes environment. This file, once executed in your Kubernetes environment, grants Cortex Cloud the necessary permissions to collect the data. The installer file must be executed in your Kubernetes environment to complete the onboarding process. The connector then appears in Kubernetes Connectors.

1. Navigate to Settings → Data Sources & Integrations.



2. On the Add Data Sources & Integrations page, click Create Integration, search for Kubernetes, then hover over it and click Add Another Instance.

3. In the Kubernetes Connect onboarding wizard, enable the solutions that fit your needs:

- Posture Management: (Enabled by default) A lightweight posture management solution for continuous discovery, policy enforcement, and proactive scanning of vulnerabilities, secrets, malware, compliance, and misconfigurations.
- Realtime Protection: A solution that monitors workloads in real time to detect and block malicious activity, instantly preventing attacks as they happen.

4. (Optional) Click Edit to configure advanced settings and then click Apply Changes:

- Posture Management:

Setting	Notes
Scan Cadence (Hours)	Define how often to scan (from every one to 24 hours). Default is 12 hours.
Policy Enforcement by the Admission Controller	Select to allow enforcement policies to be configured, ensuring that only compliant resources are admitted into the cluster.
Registry Scanning (OpenShift Only)	<p>Select this option to scan OpenShift Platform Registry images for vulnerabilities, malware, and exposed secrets.</p> <p>Select the scanning configuration option to enable security checks for your images:</p> <ul style="list-style-type: none"><li>◦ All (Default) Scans all container images, including all versions (tags), in all discovered repositories.</li><li>◦ Latest tag: Scans only images tagged 'latest' in all discovered repositories.</li><li>◦ Day modified: Scans container images created or modified in the last few days. You can select a range of up to 90 days for the scan. The default is set to 7.</li></ul> <p>Refer to OpenShift container registry for information on the instances that were automatically created by the Kubernetes deployment.</p>

- Realtime Protection:

**NOTE:**

This option is not supported for Fargate.

Setting	Notes
Node Selector	Enter node labels to have the agent run on nodes that match the node labels.
Run on all nodes (Including Master)/Run only on master node	
Deployment Platform	Select the Kubernetes deployment platform: <ul style="list-style-type: none"><li>◦ Standard</li><li>◦ Bottlerocket OS</li><li>◦ Google GCOS</li><li>◦ OpenShift</li></ul>



5. (Optional) Click Edit Profile to customize the Kubernetes Connector's profile:

Setting	Notes
Profile Name	A profile name is automatically generated, including the date and time of creation. You can manually change the profile name.
Version	Select which version of the Kubernetes Connector to install.
Cluster Resource Identifier	<p>(Optional) Enter the Kubernetes cluster resource identifier. If you do not specify the resource identifier, the installer will identify the cluster on its own.</p> <p><b>NOTE:</b></p> <p>For Fargate, you must provide the cluster resource identifier.</p> <p>The format of the identifier is <code>arn:aws:eks:&lt;region&gt;:&lt;account-id&gt;:cluster/&lt;cluster-name&gt;</code>.</p>
Namespace	<p>Enter the name for the Kubernetes namespace. The default is "panw".</p> <p>To ensure proper data parsing in an AWS Fargate environment, a Fargate Profile must be explicitly configured for the namespace where the connector is installed (typically panw) and for the kube-system namespace if the cluster is fully Fargate-based. Because the system identifies Fargate clusters by scanning for active workloads during deployment, a Fargate profile that contains no running pods will not be recognized as such. Furthermore, since this detection occurs at installation, any transition from EC2 to Fargate requires an agent update to trigger a new scan and ensure the environment is correctly identified and monitored.</p>
Proxy Gateway	<p>Enable this option if network traffic between Cortex Cloud and your Kubernetes cluster must route through a proxy gateway. Enter the following details:</p> <ul style="list-style-type: none"> <li>Proxy IP: The full IP address and port number for your HTTP proxy server. For example: <code>192.168.1.1:8080</code></li> <li>Authentication: Select None or Basic. Enter the username and password for a proxy user account that has permission to pass traffic to the Kubernetes cluster.</li> </ul> <p><b>NOTE:</b></p> <p>Basic authentication is only supported in Posture Management. If deploying Realtime Protection, select None .</p>



Setting	Notes
Auto Upgrade	<p>Enable Auto Upgrade to ensure the Kubernetes Connector and its installed capabilities are automatically updated to a newer version when available. This minimizes manual maintenance and ensures continuous access to the latest features and security patches.</p> <p>Select the Upgrade Strategy:</p> <ul style="list-style-type: none"> <li>• Latest Available Version (GA): Automatically upgrade to the newest version as soon as it is released to gain immediate access to all new features.</li> <li>• One release before the latest one (N-1): Maintain a policy to always remain one version behind the latest available release.</li> </ul> <p>Select Advanced to customize the upgrade schedule. Define whether to be upgraded immediately or to delay the upgrade by a specified number of days. You can then specify the preferred day and time for the upgrade to be applied.</p>

6. Click Generate.
7. To complete the onboarding of the Kubernetes Connector, you must download the Helm chart values `values.yaml` and run it in your Kubernetes environment: `helm repo add cortex https://paloaltonetworks.github.io/cortex-cloud --force-update`
8. Install the Helm charts in your Kubernetes environment: `helm upgrade --install konnector cortex/konnector --wait-for-jobs --create-namespace --namespace panw --values <profile-name>.values.yaml`
9. Verify the deployment succeeded when you see "Status: Deployed".

When the Kubernetes Connector is deployed, the initial discovery scan is started, and the connector appears in Data Sources & Integrations â Kubernetes â Kubernetes Connectors.

#### 2.2.7.1 | What's new in Kubernetes Connector?

This topic describes the changes, additions, known issues, and fixes for each version of the Kubernetes Connector. If Auto Upgrade is enabled in your Kubernetes Connector, you will automatically enjoy the latest released features without having to manually upgrade to the new version.

##### Kubernetes Connector releases

Cortex Cloud supports the following current Kubernetes Connector versions. Click the link to view the new features, addressed issues, and known issues per release.

Release Version	Release Notes	Release Date
1.3	Kubernetes Connector version 1.3	Nov 9, 2025
1.2	Kubernetes Connector version 1.2	July 20, 2025

##### Kubernetes Connector version 1.3

###### New features

The following section describes the new features introduced in Kubernetes Connector version 1.3.

Feature	Description
Unified Kubernetes Onboarding	Streamlined Kubernetes onboarding process in a single, easy-to-use wizard. Now you can discover all available security capabilities based on your license, configure everything in one flow, and deploy your entire solution with one consolidated installer.



Feature	Description
Kubernetes Connector	Supports AKS, EKS, GKE, managed OpenShift, self-managed Kubernetes vanilla clusters, and self-managed OpenShift with a Kubernetes Native installation method of Helm Installer. For more details, see Supported Kubernetes distributions.
KSPM Dashboard	A visual overview of your Kubernetes security posture. It includes inventory insights, protection coverage, most vulnerable clusters, malware and secrets detected, and more.
Compliance standards	Enjoy out-of-the-box CIS compliance standards for Kubernetes environments (CIS EKS, CIS GKE, CIS AKS, CIS OpenShift, and CIS Kubernetes).
Secrets, malware, and vulnerabilities	Generate secret, malware, and vulnerabilities posture issues by declaring policies on Kubernetes clusters

#### Known limitations

The following table describes known limitations in the Kubernetes Connector release.

Feature	Description
Connector onboarding and cluster identifier	<p>The Kubernetes Connector automatically calculates the Kubernetes cluster cloud identifier by using the metadata service (for EKS and GKE) and cluster resources (for AKS).</p> <ul style="list-style-type: none"> <li>For EKS and GKE, the metadata service must be enabled.</li> </ul>

Kubernetes Connector version 1.2

#### New features

The following section describes the new features introduced in Kubernetes Connector version 1.2.

Feature	Description
Kubernetes Connector Onboarding	Supports AKS, EKS, GKE, managed OpenShift, and self-managed Kubernetes Vanilla clusters, with a Kubernetes Native installation method of Helm Installer.
KSPM Dashboard	A visual overview of your Kubernetes security posture. It includes inventory insights, protection coverage, riskiest clusters, and more.
Compliance standards	Enjoy out-of-the-box CIS compliance standards for Kubernetes environments (CIS EKS, CIS GKE, CIS AKS, CIS OpenShift, and CIS Kubernetes).
Secrets, malware, and vulnerabilities	Generate secret, malware, and vulnerabilities posture issues by declaring policies on Kubernetes clusters
Kubernetes internet exposure	r



## Known limitations

The following table describes known limitations in the Kubernetes Connector release.

<b>Feature</b>	<b>Description</b>
Connector onboarding and cluster identifier	<p>The Kubernetes Connector automatically calculates the Kubernetes cluster cloud identifier by using the metadata service (for EKS and GKE) and cluster resources (for AKS).</p> <ul style="list-style-type: none"> <li>For EKS and GKE, the metadata service must be enabled.</li> </ul>

### 2.2.7.2 | Supported Kubernetes distributions

The following are the supported Kubernetes platform versions for the Kubernetes connector (Posture Management). The table shows the latest version that is supported. We support n-3 versions of each supported Kubernetes environment.

<b>Kubernetes Environment</b>	<b>Notes</b>
Managed clusters	<ul style="list-style-type: none"> <li>Amazon Elastic Kubernetes Service (EKS)</li> <li>Microsoft Azure Kubernetes Service (AKS)</li> <li>Google Kubernetes Engine (GKE)</li> </ul>
Managed OpenShift	Managed Openshift clusters, including ROSA (Red Hat OpenShift on AWS), are supported.
Self-Managed	<p>We support every CNCF-certified Kubernetes solution. We've tested our solution on:</p> <ul style="list-style-type: none"> <li>Self-managed vanilla/on-premise Kubernetes clusters.</li> <li>Self-managed OpenShift Kubernetes clusters.</li> <li>Rancher Distributions (RKE and RKE2).</li> </ul>

The following are the Kubernetes platforms that are supported with Cortex XDR agents (Real-time protection).

This table shows the Kubernetes platform versions that have been compatibility tested. The table shows the latest version that has been tested. All versions that are not EOL, up to the latest version are supported.

<b>Linux Kubernetes Platform</b>	<b>Version</b>
Unmanaged Kubernetes (k8s)	1.30
Amazon Elastic Kubernetes Service (EKS)	1.33
BottleRocket OS x86_64 User mode agent only	
BottleRocket OS aarch64 User mode agent only	



Linux Kubernetes Platform	Version
Microsoft Azure Kubernetes Service (AKS)	1.33
CBL-mariner 2 x86_64	
Google Kubernetes Engine (GKE)	1.33
Google Container-Optimized OS (COS)* x86_64 User mode agent only	
Google Kubernetes Engine (GKE) Autopilot	
Oracle Kubernetes Engine (OKE)	1.33
Red Hat OpenShift Container Platform (OCP)	4.16
RHCOS* x86_64 User mode agent only	
SUSE Rancher Kubernetes Engine 2 (RKE2)	1.28
Talos	1.8.3

**NOTE:**

In Google Container-Optimized OS release 100 and earlier, where the FANOTIFY EXEC flag is not supported, the Kernel configuration may be partial for the user mode agent to properly function. In such cases, the agent will fallback to asynchronous mode.

In RHCOS version 4.12 and earlier, the Kernel configuration may be partial for the user mode agent to properly function. In such cases, the agent will fallback to asynchronous mode.

## 2.3 | Post-deployment steps

Perform post-deployment tasks such as setting up your environment, creating automation rules, and managing user roles and access management.

### 2.3.1 | Set up your environment

Abstract

Learn more about setting up the Cortex Cloud environment based on your preferences.

To create a more personalized user experience, Cortex Cloud enables you to customize and configure the following:

- Server settings
- Security settings
- Log forwarding

#### 2.3.1.1 | Configure server settings

Abstract



Configure server settings such as keyboard shortcuts, timezone, and timestamp format.

You can configure server settings such as keyboard shortcuts, timezone, timestamp format, and custom logos for communications task emails to create a more personalized user experience in Cortex Cloud. Go to Settings → Configurations → General → Server Settings.

**NOTE:**

Keyboard shortcuts, timezone, and timestamp format are not set universally and only apply to the user who sets them.

Server Setting	Description
Keyboard Shortcuts	Enables you to change the default shortcut settings. The shortcut value must be a keyboard letter, A through Z, and cannot be the same for both shortcuts.
Timezone	Select a specific timezone. The timezone affects the timestamps displayed in Cortex Cloud, auditing logs and when exporting files.
Timestamp Format	The format in which to display Cortex Cloud data. The format affects the timestamps displayed in Cortex Cloud, auditing logs and when exporting files.  This setting is configured per user and not per tenant.
Email Contacts	A list of email addresses Cortex Cloud can be used as a distribution list. The defined email addresses are used to send product maintenance, updates, and new version notifications. These addresses are in addition to the email addresses registered with your Customer Support Portal account.
Custom Logo	By default, the Cortex Cloud logo displays on communication task emails. You can replace the default logo with a custom logo to match your organization's branding.  Supported file formats are PNG, JPEG, SVG, and GIF.  The minimum recommended image dimensions are 50px height and 50px width. The recommended maximum file size is 100 KB.
AI Configuration	<ul style="list-style-type: none"><li>• Enable or disable the Cortex Agentic Assistant (Agents &amp; LLM Experience).</li><li>• Enable or disable AI case summarization capabilities.</li></ul> <p><b>NOTE:</b> The Cortex Agentic Assistant and AI case summarization are currently available for users in limited regions. For more information, see Cortex Agentic Assistant.</p>
Password Protection (for downloaded files)	Enable password protection when downloading retrieved files from an endpoint. This prevents users from opening potentially malicious files.  Administrator permissions required. <p><b>NOTE:</b> If the Password Protection (for downloaded files) setting under Settings → Configuration → General → Server Settings is enabled, enter the password 'suspicious' to download the file.</p>
Google Maps Key	Enter the Google Maps API key to display the physical location of an entity on a Google map.



Server Setting	Description
Scope-Based Access Control (SBAC)	<p>Enforces granular scoping on users with a scoping configuration. A user can inherit scoping configurations from a user group, or have the scoping configuration applied directly on top of the role assigned from either a user group or a generated API Key.</p> <p>By default, Enable Scope Based Access Control is disabled and granular scoping is not enforced. Before enabling SBAC, we recommend that an administrator or a user with Access Management permissions first ensure that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes. For more information, see <a href="#">Manage user scope</a>.</p> <p>(Optional) If enabled, you can select the Endpoint Scoping Mode, which is defined per tenant:</p> <ul style="list-style-type: none"> <li>• Permissive: Enables users with at least one scope tag to access the relevant entity with that same tag.</li> <li>• Restrictive: Users must have all the scoped tags that are tagged within the relevant entity of the system.</li> </ul>
XQL Configuration	<p>Enables setting case sensitivity across Cortex Cloud.</p> <p>By default, this setting is set to <code>false</code> and field values are evaluated as case insensitive.</p> <p>This setting overwrites any other default configuration except for BIOCs, which will remain case-insensitive no matter what this configuration is set to.</p>
Define the cases target MTTR per issue severity	<p>Determines within how many days and hours you want issues resolved according to the issue severity Critical, High, Medium, and Low.</p> <p>The defined MTTR is used to display the Resolved Issue MTTR dashboard widgets.</p>
Impersonation Role	<p>The type of role permissions granted to the Palo Alto Networks Support team when opening support tickets. We recommend that role permissions be granted only for a specific time frame, and full administrative permissions be granted only when specifically requested by the Support team.</p> <p>Role permissions include:</p> <ul style="list-style-type: none"> <li>• Read-only: Default setting; grants read-only access to your tenant.</li> <li>• Support-related actions: Grants permissions to tech support file collection, dump file collection, investigation query, correlation rule, BIOC and IOC rule editing, alert starring, exclusion, and exception editing</li> <li>• Full role permissions: No limitations are applied; grants full permissions to all actions and content on your tenant</li> </ul> <p>Permission Reset Timeframe: Determines how long role permissions are valid.</p>
Case display modes	Allow users the access the Cases page in legacy mode.
Caching	Improve performance on the Cases and Issues pages by enabling a temporary data cache.



### 2.3.1.2 | Configure security settings

#### Abstract

Configure security settings such as session expiration, user login expiration, and dashboard expiration.

You can configure security settings such as how long users can be logged in Cortex Cloud, and from which domains and IP ranges users can log in.

Settings	Options	Description
Session Expiration	User Login Expiration	The number of hours (between 1 and 24) after which the user's login session expires. You can also choose to automatically log users out after a specified period of inactivity.
	Dashboard Expiration	Whether the Dashboard page expires at the same time as the user login session or after seven days. This is useful when you view a dashboard on a separate screen.  For example, if you select seven days for dashboards and eight hours for login expiration, and you are currently viewing the Dashboard page, the dashboard expiration takes priority (seven days). This ensures that the Dashboard page continues to display the widgets for an extended period.
Allowed Sessions	Approved Domains	The domains from which you want to allow user access (login) to Cortex Cloud. You can add or remove domains as necessary.
	Approved IP Ranges	The IP ranges from which you want to allow user access (login) to Cortex Cloud. You can also choose to limit API access from specific IP addresses.
User Expiration	Deactivate Inactive User	Deactivate an inactive user, and also set the user deactivation trigger period. By default, user expiration is disabled. When enabled, enter the number of days after which inactive users should be deactivated.
Same-Site Cookie Policy	Strict	Configure your Cortex tenant's SameSite cookie security policy by selecting between two settings to control how users log in from external links: <ul style="list-style-type: none"> <li>• Strict (Recommended): Requires users to reauthenticate when clicking a link from another site, even if they are already signed in.</li> </ul>
	Lax	<ul style="list-style-type: none"> <li>• Lax: Offers a more seamless experience by allowing users to access the tenant directly from external links without needing to log in again. Yet, we advise against this setting for security reasons.</li> </ul>
Allowed Domains	Domain Name	



### 2.3.1.3 | Log forwarding

#### Abstract

Stay informed and updated about events in your system by forwarding alerts and reports to an external service, such as a syslog receiver, a Slack channel, or an email account.

Logs provide information about events that occur in the system. These logs are a valuable tool in troubleshooting issues that might arise in your Cortex Cloud tenant.

To stay informed about important alerts and events, you can configure your notifications and specify the type of logs you want to forward. You can choose to receive these notifications through an email account, a Slack channel, or a syslog receiver.

#### 2.3.1.3.1 | Forward logs from Cortex Cloud to external services

#### Abstract

Learn how to forward logs from Cortex Cloud to external services such as email, Slack, or a syslog receiver.

You can forward logs from Cortex Cloud to an external service. This allows you to stay updated on important issues and events. Available services include the following:

- **Slack channel and/or syslog receiver:** Integrate the service with Cortex Cloud. Once the integration is complete, configure notification forwarding, specifying the log type you want to forward.
- **Email distribution list:** Configure notification forwarding, specifying the log type you want to forward.

The following table shows the log types supported for each notification type:

Log Type	Email	Slack	Syslog
Issues	â	â	â
Cases	â	â	â
Management Audit Log	â	â€	â

#### 2.3.1.3.1.1 | Integrate a syslog receiver

#### Abstract

Define syslog settings and then configure notification forwarding to receive notifications about issues and reports.

A syslog receiver can be a physical or virtual server, a SaaS solution, or any service that accepts syslog messages.

To send Cortex Cloud notifications to your syslog receiver, you first need to define the settings for the syslog receiver. After this is complete, you can configure notification forwarding.

How to send logs to a syslog receiver

Before you begin, enable access to the following Cortex Cloud IP addresses for your region in your firewall.

Region	Log Forwarding IP Addresses
United States - Americas (US)	<ul style="list-style-type: none"><li>• 35.232.87.9</li><li>• 35.224.66.220</li></ul>
Germany (DE)	<ul style="list-style-type: none"><li>• 35.234.95.96</li><li>• 35.246.192.146</li></ul>



<b>Region</b>	<b>Log Forwarding IP Addresses</b>
Netherlands - Europe (EU)	<ul style="list-style-type: none"> <li>• 34.90.202.186</li> <li>• 34.90.105.250</li> </ul>
Canada (CA)	<ul style="list-style-type: none"> <li>• 35.203.54.204</li> <li>• 35.203.52.255</li> </ul>
United Kingdom (UK)	<ul style="list-style-type: none"> <li>• 34.105.227.105</li> <li>• 34.105.149.197</li> </ul>
Singapore (SG)	<ul style="list-style-type: none"> <li>• 35.240.192.37</li> <li>• 34.87.125.227</li> </ul>
Japan (JP)	<ul style="list-style-type: none"> <li>• 34.84.88.183</li> <li>• 35.243.76.189</li> </ul>
Australia (AU)	<ul style="list-style-type: none"> <li>• 35.189.38.167</li> <li>• 34.87.219.39</li> </ul>
United States - Government	<ul style="list-style-type: none"> <li>• 104.198.222.185</li> <li>• 35.239.59.210</li> </ul>
India (IN)	<ul style="list-style-type: none"> <li>• 34.93.247.41</li> <li>• 34.93.183.131</li> </ul>
Switzerland (CH)	<ul style="list-style-type: none"> <li>• 34.65.228.95</li> <li>• 34.65.74.83</li> </ul>
Warsaw (PL)	<ul style="list-style-type: none"> <li>• 34.118.45.145</li> <li>• 34.118.126.170</li> </ul>
Taiwan (TW)	<ul style="list-style-type: none"> <li>• 35.234.2.208</li> <li>• 35.185.171.91</li> </ul>
Qatar (QT)	<ul style="list-style-type: none"> <li>• 34.18.48.182</li> <li>• 34.18.43.40</li> </ul>
France (FA)	<ul style="list-style-type: none"> <li>• 34.163.100.253</li> <li>• 34.155.72.149</li> </ul>



Region	Log Forwarding IP Addresses
Israel (IL)	<ul style="list-style-type: none"> <li>• 34.165.194.4</li> <li>• 34.165.101.105</li> </ul>
Saudi Arabia (SA)	<ul style="list-style-type: none"> <li>• 34.166.50.215</li> <li>• 34.166.55.72</li> </ul>
Indonesia (ID)	<ul style="list-style-type: none"> <li>• 34.101.248.99</li> <li>• 34.101.176.232</li> </ul>
Spain (ES)	<ul style="list-style-type: none"> <li>• 34.175.83.90</li> <li>• 34.175.230.150</li> </ul>
Italy (IT)	<ul style="list-style-type: none"> <li>• 34.154.0.173</li> <li>• 34.154.71.94</li> </ul>
South Korea (KR)	<ul style="list-style-type: none"> <li>• 34.64.198.58</li> <li>• 34.47.86.20</li> </ul>
South Africa (ZA)	<ul style="list-style-type: none"> <li>• 34.35.70.253</li> <li>• 34.35.10.167</li> </ul>

1. Select Settings → Configurations → Integrations → External Applications.

2. In Syslog Servers, click + New Server.

3. Define the following parameters:

Parameter	Description
Name	Unique name for the server profile.
Destination	IP address or fully qualified domain name (FQDN) of the syslog receiver.
Port	Port number on which to send syslog messages.
Facility	Select one of the syslog standard values. The value maps to how your syslog server uses the facility field to manage messages. For details on the facility field, see RFC 5424.
Protocol	<p>Method of communication with the syslog receiver:</p> <ul style="list-style-type: none"> <li>• TCP: No validation is made on the connection with the syslog receiver. However, if an error occurred with the domain used to make the connection, the Test connection will fail.</li> <li>• UDP: No error checking, error correction, or acknowledgment. No validation is done for the connection or when sending data.</li> <li>• TCP + SSL: Cortex Cloud validates the syslog receiver certificate and uses the certificate signature and public key to encrypt the data sent over the connection.</li> </ul>



Parameter	Description
Certificate	<p>The communication between Cortex Cloud and the syslog destination can use TLS. In this case, upon connection, Cortex Cloud validates that the syslog receiver has a certificate signed by either a trusted root CA or a self-signed certificate. You may need to merge the Root and Intermediate certificate if you receive a certificate error when using a public certificate.</p> <p>If your syslog receiver uses a self-signed CA, upload your self-signed syslog receiver CA. If you only use a trusted root CA leave the certificate field empty.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>Up to TLS 1.3 is supported.</li> <li>Make sure the self-signed CA includes your public key.</li> </ul> <p>You can ignore certificate errors. For security reasons, this is not recommended. If you choose this option, logs will be forwarded even if the certificate contains errors.</p>

4. Test the parameters to ensure a valid connection, and click Create when ready.

You can define up to five syslog receivers. Upon success, the table displays the syslog servers and their status.

#### What to do next

After you integrate with your syslog receiver, configure your forwarding settings. For more information see, [Configure notification forwarding](#).

#### Syslog receiver test message errors

When configuring a syslog message, Cortex Cloud sends a test message. If a test message cannot be sent, Cortex Cloud displays an error message to help you troubleshoot.

The following table includes descriptions and suggested solutions for the error messages:

Error Message	Description
Host Resolving Failed	The IP address or hostname you provided doesn't exist, or can't be resolved. Ensure you have the correct IP address or the hostname.
Configured Local Address	The IP address or hostname you provided is internal and can't be used. Ensure you have the correct IP address or the hostname.
Wrong Certificate Format	The certificate you uploaded is in an unexpected format and can't be used. The certificate must be an ASCII string or a bytes-like object. Re-create the certificate in the correct format, for example: <pre>-----BEGIN CERTIFICATE----- MIIDHTCCAgBgAwIBAgIQSwieRyGdh6BNRQyp406bnTANBgkqhkiG9w0BAQsFADAhMR8wHQYDVQQDEzTVVJTLUNoYXJsaWVBbHBoYS1Sb290MB4XDTHwMDQzMDE4MjEzNf0 -----END CERTIFICATE-----</pre>



Error Message	Description	
Connection Timed Out	<p>Cortex Cloud didn't connect to the syslog receiver in the expected time. This could be because your firewall blocked the connection or because the configuration of the syslog server caused it to drop the connection.</p>	Check the firewall logs and the connection using Wireshark.
Connection Refused	<p>The syslog receiver refused the connection. This could be because your firewall blocked the connection or because the configuration of the syslog server caused it to drop the connection.</p>	Check the firewall logs and the connection using Wireshark.
Connection Reset	<p>The connection was reset by the syslog receiver. This could be because your firewall blocked the connection or because the configuration of the syslog receiver caused it to drop the connection.</p>	Check the firewall logs and the connection using Wireshark.



Error Message	Description	
Certificate Verification Failed	<p>The uploaded certificate couldn't be verified for one of the following reasons.</p> <ul style="list-style-type: none"> <li>• The certificate doesn't correspond to the certificate on the syslog receiver and can't be validated.</li> <li>• The certificate doesn't have the correct hostname.</li> <li>• You are using a certificate chain and didn't merge the certificates into one certificate.</li> </ul>	<ul style="list-style-type: none"> <li>• Incorrect certificate: to check that the certificate you are uploading corresponds to the server syslog certificate, use the following command:  <pre>openssl verify -verbose -CAfile cortex_upload_certificate syslog_certificate</pre> If the certificate is correct, the result is <b>syslog_certificate: OK</b>.</li> <li>• Incorrect hostname: make sure that the hostname/ip in the certificate matches the syslog server.</li> <li>• Certificate chain: If you are using a list of certificates, merge the chain into one certificate. You can concatenate the certificates:  <pre>cat intermediate_cert root_cert &gt; merged_syslog.crt</pre> If the concatenated certificate doesn't work, change the order of the root and intermediate certificates, and try again.</li> </ul> <p>To verify that the chain certificate was saved correctly, use the following openssl command.</p> <pre>openssl verify -verbose -CAfile cortex_upload_certificate syslog_certificate</pre> <p>If the certificate is correct, the result is <b>syslog_certificate: OK</b>.</p>
Connection Terminated Abruptly	<p>The firewall or the syslog receiver dropped the connection unexpectedly. This could be because the firewall on the customer side limits the number of connections, the configuration on the syslog receiver drops the connection, or the network is unstable.</p>	<p>Check the firewall logs and the connection using Wireshark.</p>
Host Unreachable	<p>The network configuration is faulty and the connection can't reach the syslog receiver.</p>	<p>Check the network configuration to make sure that everything is configured correctly like a firewall or a load balancer which may be blocking the connection.</p>



Error Message	Description
SSL Error	Unknown SSL error. To investigate the issue, contact support.
Connection Unavailable	General error. To investigate the issue, contact support.

2.3.1.3.1.2 | [Integrate Slack for outbound notifications](#)

#### Abstract

Learn how to integrate Cortex Cloud with your Slack workspace and stay updated on important alerts and events.

Integrate Cortex Cloud with your Slack workspace to manage and highlight your issues and reports. Creating a Cortex Cloud Slack channel ensures that defined issues are exposed on laptop and mobile devices using the Slack interface. Unlike email notifications, Slack channels provide dedicated spaces where you can contact specific members regarding your issues.

#### How to integrate Slack with Cortex Cloud

1. From Cortex Cloud, select Settings → Configurations → Integrations → External Applications.
2. Select the provided link to install Cortex Cloud on your Slack workspace.

#### NOTE:

You are directed to the Slack browser to install Cortex Cloud. You can only use this link to install Cortex Cloud on Slack. Attempting to install from Slack Marketplace will redirect you to Cortex Cloud documentation.

3. Click Submit.

Upon successful installation, Cortex Cloud displays the workspace to which you connected.

#### What to do next

After you integrate with your Slack workspace, configure your forwarding settings. For more information see, [Configure notification forwarding](#).

2.3.1.3.1.3 | [Configure notification forwarding](#)

#### Abstract

Learn how to create a forwarding configuration that specifies the log type you want to forward.

After you integrate with an external service such as Slack or a syslog receiver, create a forwarding configuration that specifies the log type you want to forward. You can configure notifications for issues, agent audit logs, and management audit logs. To receive notifications about reports, see [Run or schedule reports](#).

#### PREREQUISITE:

Before you can select a syslog receiver or a Slack channel, you must integrate these external services with Cortex Cloud.

For more information, see:

- [Integrate a syslog receiver](#)
- [Integrate Slack for outbound notifications](#)

#### How to configure notifications

1. Select Settings → Configurations → General → Notifications.
2. Click + Add Forwarding Configuration.
3. Enter a name and description for the configuration.
4. Select the log type you want to forward:



- Issues: Send notifications for specific issue types.

**NOTE:**

- **Notification Forwarding by Domain:** To configure notification forwarding for issues by domain, select Log Type = Issues and filter the Issues table by Issue Domain.
- **Case IDs in Notifications:** If case matching completes before the notification is sent, the Case ID is included. If matching takes longer than the notification trigger, the notification is sent without a Case ID to prioritize timely visibility in the target system.
- **Alert vs. Issue Format:** New alert notifications are created using the notification forwarding configuration. By default, new configurations use the Issue format, but you can select the Alert format if needed.

Existing configurations are not updated automatically and will continue to send notifications in the Alert format. To use the Issue format, edit the existing configuration.

- Agent Audit Logs: Send notifications for audit logs reported by your Cortex XDR agents.
- Management Audit Logs: Send notifications for audit logs about events related to your Cortex Cloud tenant.
- Casesâ€ Send notifications for specific cases (for example, Security or Posture cases)

5. Click **Next**, and under **Scope**, filter the type of information you want included in a notification.

For example, for a filter set to **Severity = Medium, Category = Configuration**, Cortex Cloud sends the issues or events matching this filter as a notification.

6. Click **Next**.

7. (Optional) Define your email configuration:

- In the Distribution List, add the email addresses to which you want to send email notifications.
- In the Grouping Timeframe, define the time frame, in minutes, to specify how often Cortex Cloud sends notifications. Every 20 issues or 20 events aggregated within this time frame are sent together in one notification, sorted according to severity. To send a notification when one issue or event is generated, set the time frame to 0.
- Choose whether you want Cortex Cloud to provide an auto-generated subject.
- Choose the format you want to send the email. If you choose Alert, you can choose the Standard or Legacy format. For more information about the legacy format, see Log format for IOC and BIOC issues.

8. Depending on the notification integrations supported by the log type, configure the Slack channel or syslog receiver notification settings. For a list of log types supported in each notification type, see Forward logs from Cortex Cloud to external services.

- Enter the Slack channel name and select from the list of available channels. Slack channels are managed independently of Cortex Cloud in your Slack workspace. After integrating your Slack account with your Cortex Cloud tenant, Cortex Cloud displays a list of specific Slack channels associated with the integrated Slack workspace.
- Select a syslog receiver. Cortex Cloud displays the list of receivers integrated with your Cortex Cloud tenant.
- Choose the format you want to send the syslog. If you choose Alert, you can choose the Standard or Legacy format. For more information about the legacy format, see Log format for IOC and BIOC issues.

9. Click **Done** to create the forwarding configuration.

2.3.1.3.1.4 | Monitor administrative activity

## Abstract

View all Cortex Cloud administrator-initiated actions taken on issues, cases, and live terminal sessions.

From Settings â€“ Management Audit Logs, you can track the status of all administrative and investigative actions. Cortex Cloud stores audit logs for 365 days (instead of 180 days, which was the retention period in the past). Use the page filters to narrow the results or manage tables to add or remove fields as needed.

To ensure you and your colleagues stay informed about administrative activity, you can configure notification forwarding to forward your Management Audit log to an email distribution list, Syslog server, or Slack channel.

The following table describes the default and optional fields that you can view in alphabetical order.

Field	Description
Email	Email address of the administrative user



Field	Description
Description	Descriptive summary of the administrative action. Hover over this field to view more detailed information in a popup tooltip. This enables you to know exactly what has changed, and, if necessary, roll back the change.
Host Name	Name of any relevant affected hosts
ID	Unique ID of the action
Result	Result of the administrative action: Success, Partial, or Fail.
Subtype	Subcategory of action
Timestamp	Time and date of the action



<b>Field</b>	<b>Description</b>
Type	Type of activity logged, one of the following:



Field	Description
	<ul style="list-style-type: none"> <li>• Agent Configuration: Configuration of a particular Cortex XDR agent on a particular endpoint.</li> <li>• Agent Installation: Installation of the Cortex XDR agent on a particular endpoint.</li> <li>• Issue Exclusions: Suppression of particular issues from Cortex Cloud .</li> <li>• Issue Notifications: Modification of the format or timing of issues.</li> <li>• Issue Rules: Modification of issue rules.</li> <li>• API Key: Modification of the Cortex Cloud API key.</li> <li>• Authentication: User sessions started, along with the user name that started the session.</li> <li>• Broker API: Operation related to the Broker application programming interface (API).</li> <li>• Broker VM: Operation related to the Broker virtual machine (VM).</li> <li>• Dashboards: Use of particular dashboards.</li> <li>• Device Control Permanent Exceptions: Modification of permanent device control exceptions.</li> <li>• Device Control Profile: Modification of a device control profile.</li> <li>• Device Control Temporary Exceptions: Modification of temporary device control exceptions.</li> <li>• Disk Encryption Profile: Modification of a disk encryption profile.</li> <li>• Endpoint Administration: Management of endpoints.</li> <li>• Endpoint Groups: Management of endpoint groups.</li> <li>• Extensions Policy: Modification of extension policy settings, including host firewall and disk encryption.</li> <li>• Extensions Profiles: Modification of extension profile settings.</li> <li>• Global Exceptions: Management of global exceptions.</li> <li>• Host Firewall Profile: Modification of a host firewall profile.</li> <li>• Host Insights: Initiation of Host Insights data collection scan (Host Inventory and Vulnerability Assessment).</li> <li>• Case Management: Actions taken on cases and on the assets, issues, and artifacts in cases.</li> <li>• Ingest Data: Import of data for immediate use or storage in a database.</li> <li>• Integrations: Integration operations, such as integrating Slack for outbound notifications.</li> <li>• Licensing: Any licensing-related operation.</li> <li>• Live Terminal: Remote terminal sessions created and actions taken in the file manager or task manager, a complete history of commands issued, their success, and the response.</li> <li>• Managed Threat Hunting: Activity relating to managed threat hunting.</li> <li>• MSSP: Management of security services providers.</li> <li>• Policy &amp; Profiles: Activity related to managing policies and profiles.</li> <li>• Prevention Policy Rules: Modification of prevention policy rules.</li> <li>• Protection Policy: Modification of the protection policy.</li> <li>• Protection Profile: Modification of the protection profile.</li> <li>• Public API: Authentication activity using an associated Cortex Cloud API key.</li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• Query Center: Operations in the Query Center.</li> <li>• Remediation: Remediation operations.</li> <li>• Reporting: Any reporting activity.</li> <li>• Response: Remedial actions taken. For example: Isolate a host, undo host isolation, add a file hash signature to the block list, or undo the addition to the block list.</li> <li>• Rules: Modification of rules.</li> <li>• Rules Exceptions: Creation, editing, or deletion under Rules exceptions.</li> <li>• SaaS Collection: Any collected SaaS data.</li> <li>• Script Execution: Any script execution.</li> <li>• Starred Cases: Modification of starred cases.</li> <li>• Vulnerability Assessment: Any vulnerability assessment activity.</li> </ul>
User Name	The user who performed the action.

#### 2.3.1.3.2 | Data and log notification formats

##### Abstract

Cortex Cloud provides you with different formats for its log notifications.

When Cortex Cloud cases, issues, and logs are forwarded to email or a third-party system, notifications are sent in a specific format.

##### **NOTE:**

Issues can be forwarded to email, syslog servers, and Slack in the alert format, if you prefer. The alert format can be selected when you configure your forwarding notification.

#### 2.3.1.3.2.1 | Management audit log messages

##### Abstract

View the types of Cortex Cloud management audit log messages that are sent.

Cortex Cloud management audit log messages are sent based on the various log types, for example, Action Center, Issue Rules, or Authentication.

##### List of log types



- Action Center
- Agent Configuration
- Agent Exception Rules
- Issue Exclusion
- Issue Management
- Issue Notifications
- Issue Rules
- Issue Exclusions
- Allowed Domains
- API Key
- Apps
- Asset Inventory
- Asset Roles
- Asset Tag Rules
- Asset Uploads
- Authentication
- Automation Rules
- Automation Settings
- Broker API
- Broker VMs
- Business Unit Change
- SaaS Collection
- Custom Fields
- Dashboards
- Datasets
- Dataset Views
- Data Retention
- Device Control Custom Device
- Device Control Permanent Exceptions
- Extensions Policy Rules
- Device Control Profile
- Device Control Temporary Exceptions
- Agent Installation
- EDL Management
- Effective IP Ranges
- Endpoint Groups
- Endpoint Administration
- Event Forwarding
- Device Control Violations
- Device Permanent Exceptions
- Device Temp Exceptions



- Disk Encryption Visibility
- Featured Alert Fields
- Forensics
- Global Exceptions
- Host Insights
- Disk Encryption Profile
- Host Firewall
- Host Firewall Profile
- Case Domains
- Case Layout Rules
- Case Management
- Case Properties
- Case Timeline Event
- Indicator rules
- Ingest Data
- Integrations
- Layout Rules
- Licensing
- Live Terminal
- Lookups
- Managed Detection & Response
- Managed Threat Hunting
- MSSP
- Permissions
- Playbook Triggers
- Policy & Profiles
- Prevention Policy Rules
- Prisma Integration
- Extensions Profile
- Public API
- Query Center
- Query Library
- Remediation
- Remediation Path Rules
- Reporting
- Response
- Rules
- Rules Exceptions
- Scoring Rules
- XDR Collector Configuration
- XDR Collectors Groups



- XDR Collectors Policy
- XDR Collectors Profile
- Script Execution
- Security Settings
- Server Settings
- Starred Incidents
- Support
- System
- Tenant Takeover
- Vulnerability Assessment
- Vulnerability Tests
- XCloud Integration
- XDM Config
- XQL Parsing Rules
- Public API
- Cortex Automation
  - Sub Typeâ€ Command - War Room
    - Statusâ€ Success
    - Severityâ€ Informational
    - Detailsâ€ IncidentID:{ID}, IncidentType:{type}, IncidentName:{name}, Command:{command}, Arguments:{arg1}={arg1val} {arg2}={arg2val} {argn}={argnval}, ID: {num}
  - Sub Typeâ€ Command - Playground
    - Statusâ€ Success
    - Severityâ€ Informational
- XSOAR Migration

[2.3.1.3.2.2 | Issue notification format](#)

## Abstract

Learn about the formats used to forward Cortex XDR agent, BIOC, IOC, analytics, correlation, and third-party issues.

Cortex XDR agent, BIOC, IOC, analytics, correlation, and third-party issues are forwarded to external data resources according to the email, Slack, or syslog format.

### Email account

Cortex Cloud sends issue notifications to email accounts based on the settings you configure. Email messages also include an issue code snippet of the fields according to the columns in the Issue table.

The notification format is as follows:

- If only one issue exists in the queue, a single-issue email format is sent.
- If more than one issue was grouped in the time frame, all the issues in the queue are forwarded together in a grouped email format.

### Example 3.

#### Single-issue email message

```
Email Subject: Issue: <issue_name>
Email Body:
  Issue Name: Suspicious Process Creation
  Severity: High
  Source: Correlation
  Category: Malware
```



```

Action: Detected
Host: <host name>
Username:<user name>
Excluded: No
Starred: Yes
Issue: <link to the tenant issue view>
Case: <link to the tenant case view>

```

Example 4.

Grouped issue email message

```

Email Subject: Issues: <first_highest_severity_issue> + x others
Email Body:
  Issue Name: Suspicious Process Creation
  Severity: High
  Source: Correlation
  Category: MalwareAction: Detected
  Host: <host name>
  Username:<user name>
  Excluded:No
  Starred: Yes
  Issue: <link to the tenant issue view>
  Case: <link to the tenant case view>
  Issue Name: Behavioral Threat Protection
  Issue ID: 2412
  Description: A really cool detection
  Severity: Medium
  Source: Correlation
  Category: Exploit
  Action: Prevented
  Host: <host name>
  Starred: Yes
  Case: <link to the tenant issue view>
  Issue: <link to the tenant case view>
  Notification Name: ª My notification policy 2 ª
  Notification Description: ª Starred issues with medium severity ª

```

Example 5.

Email body

```
{
  "original_issue_json": {
    "uid": "<UUID Value>",
    "recordType": "threat",
    "customerId": "<Customer ID>",
    "severity": 4,
    "...",
    "is_pcap": null,
    "contains_featured_host": [
      "NO"
    ],
    "contains_featured_user": [
      "YES"
    ],
    "contains_featured_ip": [
      "YES"
    ],
    "events_length": 1,
    "is_excluded": false
  }
}
```

Slack channel

You can send issue notifications to a single Slack contact or a Slack channel. Notifications are similar to the email format.

Syslog receiver

Issue notifications forwarded to a syslog receiver are sent in a CEF format RF 5425.

Section	Description
Syslog header	<9>: PRI (considered a priority field)1: version number2020-03-22T07:55:07.964311Z: timestamp of when alert/log was sentcortexxdr: host name



Section	Description
CEF header	<pre> HEADER/Vendor="Palo Alto Networks" (as a constant string)HEADER/Device Product="Cortex XDR" (as a constant string)HEADER/Product Version= Cortex XDR version (2.0/2.1....)HEADER/Severity=(integer/0 - Unknown, 6 - Low, 8 - Medium, 9 - High)HEADER/Device Event Class ID=alert sourceHEADER/name =alert name </pre>
CEF body	<pre> end=timestamp shost=endpoint_name deviceFacility=facility cat=category externalId=external_id request=request cs1=initiated_by_process cs1Label=Initiated by (constant string) cs2=initiator_commande cs2Label=Initiator CMD (constant string) cs3=signature cs3Label=Signature (constant string) cs4=cgo_name cs4Label=CGO name (constant string) cs5=cgo_command cs5Label=CGO CMD (constant string) cs6=cgo_signature cs6Label=CGO Signature (constant string) dst=destination_ip dpt=destination_port src=source_ip spt=source_port fileHash=file_hash filePath=file_path targetprocesssignature=target_process_signature tenantname=tenant_name tenantCDLid=tenant_id CSPaccountname=account_name initiatorSha256=initiator_hash initiatorPath=initiator_path osParentName=parent_name osParentCmd=parent_command osParentSha256=parent_hash osParentSignature=parent_signature osParentSigner=parent_signer incident=incident_id act=action suser=actor_effective_username </pre>

Example 6.

```

end=timestamp shost=endpoint_name deviceFacility=facility cat=category externalId=external_id request=request cs1=initiated_by_process cs1Label=Initiated by
(constant string) cs2=initiator_commande cs2Label=Initiator CMD (constant string) cs3=signature cs3Label=Signature (constant string) cs4=cgo_name cs4Label=CGO
name (constant string) cs5=cgo_command cs5Label=CGO CMD (constant string) cs6=cgo_signature cs6Label=CGO Signature (constant string) dst=destination_ip
dpt=destination_port src=source_ip spt=source_port fileHash=file_hash filePath=file_path targetprocesssignature=target_process_signature tenantname=tenant_name
tenantCDLid=tenant_id CSPaccountname=account_name initiatorSha256=initiator_hash initiatorPath=initiator_path osParentName=parent_name osParentCmd=parent_command
osParentSha256=parent_hash osParentSignature=parent_signature osParentSigner=parent_signer incident=incident_id act=action suser=actor_effective_username

```

#### 2.3.1.3.2.3 | Management Audit log notification format

##### Abstract

An email account or a syslog receiver are the notification channels through which the Management Audit log is communicated.

Cortex Cloud forwards the Management Audit log to these external data sources:



- **Email account:** Sent according to the settings you configured. For more information, see Configure notification forwarding.
- **Syslog receiver:** Sent in a CEF format RFC 5425 according to the following mapping:

Section	Description
Syslog header	<9>: PRI (considered a priority field)1: version number2020-03-22T07:55:07.964311Z: timestamp of when issue /log was sentcortexxdr: host name
CEF header	HEADER/Vendor="Palo Alto Networks" (as a constant string)HEADER/Device Product="Cortex XDR" (as a constant string)HEADER/Device Version= Cortex XDR version (2.0/2.1....)HEADER/HEADER/Severity=(integer/0 - Unknown, 6 - Low, 8 - Medium, 9 - High)HEADER/Device Event Class ID="Management Audit Logs" (as a constant string)HEADER/name = type
CEF body	suser=user end=timestamp externalId=external_id cs1Label=email (constant string) cs1=user_mail cs2Label=subtype (constant string) cs2=subtype cs3Label=result (constant string) cs3=result cs4Label=reason (constant string) cs4=reason msg=event_description tenantname=tenant_name tenantCDLid=tenant_id CSPaccountname=csp_id

#### Example 7.

```
3/18/2012:05:17.567 PM<14>1 2020-03-18T12:05:17.567590Z cortexxdr --- CEF:0|Palo Alto Networks|Cortex XDR|Cortex XDR x.x |Management Audit Logs|REPORTING|6|suser=test end=1584533117501 externalId=5820 cs1Label=email cs1=test@palotonetworks.com cs2Label=subtype cs2=Slack Report cs3Label=result cs3=SUCCESS cs4Label=reason cs4=None msg=Slack report 'scheduled_1584533112442' ID 00 to ['CUXM741BK', 'C01022YU00L', 'CV51Y1E2X', 'CRK3VASN9'] tenantname=test tenantCDLid=11111 CSPaccountname=00000
```

#### 2.3.1.3.2.4 | Log format for IOC and BIOC issues

##### Abstract

An email account or a syslog receiver are the notification channels through which IOC and BIOC issues are communicated.

Cortex Cloud logs IOC and BIOC issues. If you configure Cortex Cloud to forward logs in the legacy format, when issue logs are forwarded from Cortex Cloud, each log record has the following format:



- **Email account:** Each field is labeled, one line per field.

Example 8.

```
edrData/action_country:  
edrData/action_download:  
edrData/action_external_hostname:  
edrData/action_external_port:  
edrData/action_file_extension: pdf  
edrData/action_file_md5: null  
edrData/action_file_name: XORXOR2614081980.pdf  
...  
xdr_sub_type: BIOC - Credential Access  
bioc_category_enum_key: null  
alert_action_status: null  
agent_data_collection_status: null  
attempt_counter: null  
case_id: null  
global_content_version_id:  
global_rule_id:  
is_whitelisted: false
```

- **Syslog format**

Example 9.

```
"/edrData/action_country","/edrData/action_download","/edrData/action_external_hostname","/edrData/action_external_port","/edrData/action_file_extension","/edrData/action_file_md5","/edrData/action_file_name","/edrData/action_file_path","/edrData/action_file_previous_file_extension","/edrData/action_file_previouus_file_name","/edrData/action_file_previous_file_path","/edrData/action_file_sha256","/edrData/action_file_size","/edrData/action_file_remote_ip","/edrData/action_file_remote_port","/edrData/action_is_injected_thread","/edrData/action_local_ip","/edrData/action_local_port","/edrData/action_module_base_address","/edrData/action_module_image_size","/edrData/action_module_is_remote","/edrData/action_module_is_replay","/edrData/action_module_path","/edrData/action_module_process_causality_id","/edrData/action_module_process_image_command_line","/edrData/action_module_process_image_extension","/edrData/action_module_process_image_md5","/edrData/action_module_process_image_name","/edrData/action_module_process_image_path","/edrData/action_module_process_image_sha256","/edrData/action_module_process_instance_id","/edrData/action_module_process_is_causality_root","/edrData/action_module_process_os_pid","/edrData/action_module_process_signature_product","/edrData/action_module_process_signature_status","/edrData/action_module_process_signature_vendor","/edrData/action_network_connection_id","/edrData/action_network_creation_time","/edrData/action_network_is_ipv6","/edrData/action_process_causality_id","/edrData/action_process_image_command_line","/edrData/action_process_image_extension","/edrData/action_process_image_md5","/edrData/action_process_image_name","/edrData/action_process_image_path","/edrData/action_process_image_sha256","/edrData/action_process_instance_id","/edrData/action_process_integrity_level","/edrData/action_process_is_causality_root","/edrData/action_process_is_replay","/edrData/action_process_is_special","/edrData/action_process_os_pid","/edrData/action_process_signature_product","/edrData/action_process_signature_status","/edrData/action_process_signature_vendor","/edrData/action_proxy","/edrData/action_registry_data","/edrData/action_registry_file_path","/edrData/action_registry_key_name","/edrData/action_registry_value_name","/edrData/action_registry_value_type","/edrData/actor_remote_ip","/edrData/action_remote_port","/edrData/action_remote_process_causality_id","/edrData/action_remote_process_image_command_line","/edrData/actor_remote_process_image_extension","/edrData/action_remote_process_image_md5","/edrData/action_remote_process_image_name","/edrData/action_remote_process_image_path","/edrData/action_remote_process_image_sha256","/edrData/action_remote_process_is_causality_root","/edrData/action_remote_process_os_pid","/edrData/action_remote_process_signature_product","/edrData/action_remote_process_signature_status","/edrData/action_remote_process_signature_vendor","/edrData/actor_effective_user_id","/edrData/action_thread_start_address","/edrData/action_thread_thread_id","/edrData/action_total_download","/edrData/action_total_upload","/edrData/action_upload","/edrData/action_user_status","/edrData/action_username","/edrData/actor_causality_id","/edrData/actor_effective_user_id","/edrData/actor_effective_username","/edrData/actor_is_injected_thread","/edrData/actor_primary_user_id","/edrData/actor_primary_username","/edrData/actor_process_causality_id","/edrData/actor_process_command_line","/edrData/actor_process_execution_time","/edrData/actor_process_image_command_line","/edrData/actor_process_image_extension","/edrData/actor_process_image_md5","/edrData/actor_process_image_name","/edrData/actor_process_image_path","/edrData/actor_process_image_sha256","/edrData/actor_process_instance_id","/edrData/actor_process_integrity_level","/edrData/actor_process_is_special","/edrData/actor_process_md5","/edrData/actor_process_signature_product","/edrData/actor_process_signature_status","/edrData/actor_thread_thread_id","/edrData/agent_content_version","/edrData/agent_host_boot_time","/edrData/agent_hostname","/edrData/agent_id","/edrData/agent_ip_addresses","/edrData/agent_is_vdi","/edrData/agent_os_sub_type","/edrData/agent_os_type","/edrData/agent_session_start_time","/edrData/agent_version","/edrData/causality_actor_causality_id","/edrData/causality_actor_effective_user_id","/edrData/causality_actor_effective_username","/edrData/causality_actor_primary_user_id","/edrData/causality_actor_primary_username","/edrData/causality_actor_process_causality_id","/edrData/causality_actor_process_command_line","/edrData/causality_actor_process_execution_time","/edrData/causality_actor_process_image_command_line","/edrData/causality_actor_process_image_extension","/edrData/causality_actor_process_image_md5","/edrData/causality_actor_process_image_name","/edrData/causality_actor_process_image_path","/edrData/causality_actor_process_image_sha256","/edrData/causality_actor_process_instance_id","/edrData/causality_actor_process_integrity_level","/edrData/causality_actor_process_is_special","/edrData/causality_actor_process_md5","/edrData/causality_actor_process_signature_product","/edrData/causality_actor_process_signature_vendor","/edrData/causality_actor_process_status","/edrData/causality_actor_process_signature_vendor","/edrData/event_id","/edrData/event_is_simulated","/edrData/event_sub_type","/edrData/event_timestamp","/edrData/event_type","/edrData/event_utc_diff_minutes","/edrData/event_version","/edrData/host_metadata_hostname","/edrData/missing_action_remote_process_instance_id","/facility","/generatedTime","/recordType","/recsize","/trapsId","/uuid","/xdr_unique_id","/meta_internal_id","/external_id","/is_visible","/is_secd0_event","/severity","/alert_source","/internal_id","/matching_status","/local_insert_ts","/source_insert_ts","/alert_name","/alert_category","/alert_description","/bioc_indicator","/matching_service_rule_id","/external_url","/xdr_sub_type","/bioc_category_enum_key","/alert_action_status","/agent_d ata_collection_status","/attempt_counter","/case_id","/global_content_version_id","/global_rule_id","/is_whitelisted"
```

Field prefixes for BIOC and IOC issue logs

Field Name	Description
/edrData/action_file*	Fields that begin with this prefix describe attributes of a file for which Traps reported activity.
edrData/action_module*	Fields that begin with this prefix describe attributes of a module for which Traps reported module loading activity.



Field Name	Description
edrData/action_module_process*	Fields that begin with this prefix describe attributes and activity related to processes reported by Traps that load modules such as DLLs on the endpoint.
edrData/action_process_image*	Fields that begin with this prefix describe attributes of a process image for which Traps reported activity.
edrData/action_registry*	Fields that begin with this prefix describe registry activity and attributes such as key name, data, and previous value for which Traps reported activity.
edrData/action_network	Fields that begin with this prefix describe network attributes for which Traps reported activity.
edrData/action_remote_process*	Fields that begin with this prefix describe attributes of remote processes for which Traps reported activity.
edrData/actor*	Fields that begin with this prefix describe attributes about the acting user that initiated the activity on the endpoint.
edrData/agent*	Fields that begin with this prefix describe attributes about the Traps agent deployed on the endpoint.
edrData/causality_actor*	Fields that begin with this prefix describe attributes about the causality group owner.

Additional fields for BIOC and IOC issue logs

Field Name	Description
/severity	<p>Severity assigned to the issue:</p> <ul style="list-style-type: none"> <li>• SEV_010_INFO</li> <li>• SEV_020_LOW</li> <li>• SEV_030_MEDIUM</li> <li>• SEV_040_HIGH</li> <li>• SEV_090_UNKNOWN</li> </ul>
/alert_source	Source of the issue: BIOC or IOC
/local_insert_ts	Date and time when Cortex Cloud â€“ Investigation and Response ingested the app.
/source_insert_ts	Date and time the issue was reported by the issue source.



Field Name	Description
/alert_name	If the issue was generated by Cortex Cloud – Investigation and Response, the issue name will be the specific Cortex Cloud rule that created the issue (BIOC or IOC rule name). If from an external system, it will carry the name assigned to it by Cortex Cloud.
/alert_category	<p>Issue category based on the issue source.</p> <ul style="list-style-type: none"> <li>• BIOC issue categories: <ul style="list-style-type: none"> <li>◦ OTHER</li> <li>◦ PERSISTENCE</li> <li>◦ EVASION</li> <li>◦ TAMPERING</li> <li>◦ FILE_TYPE_OBFUSCATION</li> <li>◦ PRIVILEGE_ESCALATION</li> <li>◦ CREDENTIAL_ACCESS</li> <li>◦ LATERAL_MOVEMENT</li> <li>◦ EXECUTION</li> <li>◦ COLLECTION</li> <li>◦ EXFILTRATION</li> <li>◦ INFILTRATION</li> <li>◦ DROPPER</li> <li>◦ FILE_PRIVILEGE_MANIPULATION</li> <li>◦ RECONNAISSANCE</li> </ul> </li> <li>• IOC issue categories: <ul style="list-style-type: none"> <li>◦ HASH</li> <li>◦ IP</li> <li>◦ PATH</li> <li>◦ DOMAIN_NAME</li> <li>◦ FILENAME</li> <li>◦ MIXED</li> </ul> </li> </ul>
/alert_description	Text summary of the event including the issue source, issue name, severity, and file path. For alerts generated by BIOC and IOC rules, Cortex Cloud displays detailed information about the rule.



Field Name	Description
/bioc_indicator	<p>A JSON representation of the rule characteristics. For example:</p> <pre data-bbox="788 294 1209 714">[{"pretty_name": "File", "data_type": null, "render_type": "entity", "entity_map": null}, {"pretty_name": "action type", "data_type": null, "render_type": "attribute", "entity_map": null}, {"pretty_name": "=", "data_type": null, "render_type": "operator", "entity_map": null}, {"pretty_name": "all", "data_type": null, "render_type": "value", "entity_map": null}, {"pretty_name": "AND", "data_type": null, "render_type": "connector", "entity_map": null}, {"pretty_name": "name", "data_type": null, "render_type": "TEXT", "entity_map": null}, {"pretty_name": "attributes", "data_type": null, "render_type": "operator", "entity_map": "attributes"}, {"pretty_name": "*", "data_type": null, "render_type": "operator", "entity_map": "attributes"}, {"pretty_name": ".pdf", "data_type": null, "render_type": "value", "entity_map": "attributes"}]</pre>
/bioc_category_enum_key	<p>Issue category based on the issue source. An example of a BIOC issue category is Evasion. An example of a Traps issue category is Exploit Modules.</p>
/alert_action_status	<p>Action taken by the issue sensor with action status displayed in parenthesis:</p> <ul style="list-style-type: none"> <li>• Detected</li> <li>• Detected (Download)</li> <li>• Detected (Post Detected)</li> <li>• Detected (Prompt Allow)</li> <li>• Detected (Reported)</li> <li>• Detected (Scanned)</li> <li>• Prevented (Blocked)</li> <li>• Prevented (Prompt Block)</li> </ul>
/case_id	<p>Unique identifier for the incident.</p>
/global_content_version_id	<p>Unique identifier for the content version in which a Palo Alto Networks global BIOC rule was released.</p>
/global_rule_id	<p>Unique identifier for an issue generated by a Palo Alto Networks global BIOC rule.</p>
/is_whitelisted	<p>Boolean indicating whether the issue is excluded or not.</p>

2.3.1.3.2.5 | Analytics log format

## Abstract

Learn about the syntax and different variables that are used in the analytics log format.

Cortex Cloud Analytics logs issues as analytics issue logs. If you configure Cortex Cloud to forward logs in the legacy format, each log record has the following format:



- Syslog format:

Example 10.

```
sub_type,time_generated,id,version_info/document_version,version_info/magnifier_version,version_info/detection_version,alert/url,alert/category,alert/type,alert/name,alert/description/html,alert/description/text,alert/severity,alert/state,alert/is_whitelisted,alert/ports,alert/internal_destinations/single_destinations,alert/internal_destinations/ip_ranges,alert/external_destinations,alert/app_id,alert/schedule/activity_first_seen_at,alert/schedule/activity_last_seen_at,alert/schedule/first_detected_at,alert/schedule/last_detected_at,user/user_name,user/url,user/display_name,user/org_unit,device/id,device/url,device/mac,device/hostname,device/ip,device/ip_ranges,device/owner,device/org_unit,files
```

- Email account: Each field is labeled, one line per field.

Example 11.

```
sub_type: Update
time_generated: 1547717480
id: 4
version_info/document_version: 1
version_info/magnifier_version: 1.8
version_info/detection_version: 2019.2.0rc1
alert/url: https://ddc1...
alert/category: Recon
alert/type: Port Scan
alert/name: Port Scan
alert/description/html: <ul>\n<li>The device...
alert/description/text: The device ...
...
device/id: 2-85e40edd-b2d1-1f25-2c1e-a3dd576c8a7e
device/url: https://ddc1 ...
device/mac: 00-50-56-a5-db-b2
device/hostname: DCIENV3APC42
device/ip: 10.201.102.17
device/ip_ranges: [{"max_ip": "...", "name": "...", "min_ip": "...", "asset": ""}])
device/owner:
device/org_unit:
files: []
```

Fields for analytics issue logs

Field Name	Definition
sub_type	Issue log subtype. Values are: <ul style="list-style-type: none"> <li>• <b>New:</b> First log record for the issue with this record <b>id</b>.</li> <li>• <b>Update:</b> Log record identifies an update to a previously logged issue.</li> <li>• <b>StateOnlyUpdate:</b> Issue state is updated. For internal use only.</li> </ul>
time_generated	Time the log record was sent to the Cortex Cloud tenant. Value is a Unix Epoch timestamp.
id	Unique identifier for the issue. Any given issue can generate multiple log records— one when the issue is initially generated, and then additional records every time the issue status changes. This ID remains constant for all such issue records.  You can obtain the current status of the issue by looking for log records with this id and the most recent <b>alert/schedule/last_detected_at</b> timestamp.
version_info/document_version	Identifies the log schema version number used for this log record.
version_info/magnifier_version	The version number of the Cortex Cloud Analytics instance that wrote this log record.
version_info/detection_version	Identifies the version of the Cortex Cloud Analytics detection software used to generate the issue.



Field Name	Definition
alert/url	Provides the full URL to the issue page in the Cortex Cloud Analytics user interface.
alert/category	<p>Identifies the issue category, which is a reflection of the anomalous network activity location in the attack life cycle. Possible categories are:</p> <ul style="list-style-type: none"> <li>• <b>C&amp;C:</b> The network activity is possibly the result of malware attempting to connect to its Command &amp; Control server.</li> <li>• <b>Exfiltration:</b> A large amount of data is being transferred to an endpoint that is external to the network.</li> <li>• <b>Lateral:</b> The network activity is indicative of an attacker who is attempting to move from one endpoint to another on the network.</li> <li>• <b>Malware:</b> A file has been discovered on an endpoint that is probably malware or riskware. Malware issues can also be generated based on network activity that is indicative of automated malicious traffic generation.</li> <li>• <b>Recon:</b> The network activity is indicative an attacker that is exploring the network for endpoints and other resources to attack.</li> </ul>
alert/type	Identifies the categorization to which the issue belongs. For example Tunneling Process, Sandbox Detection, Malware, and so forth.
alert/name	The issue name as it appears in the Cortex Cloud Analytics user interface.
alert/description/html	The issue textual description in HTML formatting.
alert/description/text	The issue textual description in plain text.
alert/severity	<p>Identifies the issue severity. These severities indicate the likelihood that the anomalous network activity is a real attack.</p> <ul style="list-style-type: none"> <li>• <b>High:</b> The issue is confirmed to be a network attack.</li> <li>• <b>Medium:</b> The issue is suspicious enough to require additional investigation.</li> <li>• <b>Low:</b> The issue is unverified. Whether the issue is indicative of a network attack is unknown.</li> </ul>



Field Name	Definition
alert/state	<p>Identifies the issue state.</p> <ul style="list-style-type: none"> <li>• <b>Open:</b> The issue is currently active and should be undergoing triage or investigation by the network security analysts.</li> <li>• <b>Reopened:</b> The issue was previously resolved or dismissed, but new network activity has caused Cortex Cloud Analytics to reopen the issue.</li> <li>• <b>Archived:</b> No action was taken on the issue in the Cortex Cloud Analytics user interface, and no further network activity has occurred that caused it to remain active.</li> <li>• <b>Resolved:</b> Network personnel have taken enough action to end the attack.</li> <li>• <b>Dismissed:</b> The anomaly has been examined and deemed to be normal, sanctioned, network activity.</li> </ul>
alert/is_whitelisted	<p>Indicates whether the issue is whitelisted. Whitelisting indicates that anomalous-appearing network activity is legitimate. If an issue is whitelisted, then it is not visible in the Cortex Cloud Analytics user interface. Issues can be dismissed or archived and still have a whitelist rule.</p>
alert/ports	<p>List of ports accessed by the network entity during its anomalous behavior.</p>
alert/internal_destinations/single_destinations	<p>Network destinations that the entity reached, or tried to reach, during the course of the network activity that caused Cortex Cloud Analytics to generate the issue. This field contains a sequence of JSON objects, each of which contains the following fields:</p> <ul style="list-style-type: none"> <li>• <b>ip:</b> The destination IP address.</li> <li>• <b>name:</b> The destination name (for example, a host name).</li> </ul>
alert/internal_destinations/ip_ranges	<p>IP address range subnets that the entity reached, or tried to reach, during the course of the network activity that caused Cortex Cloud Analytics to generate the issue. This field contains a sequence of JSON objects, each of which contains the following fields:</p> <ul style="list-style-type: none"> <li>• <b>max_ip:</b> Last IP address in the subnet.</li> <li>• <b>min_ip:</b> First IP address in the subnet.</li> <li>• <b>name:</b> Subnet name.</li> </ul>
alert/external_destinations	<p>Provides a list of destinations external to the monitored network that the entity tried to reach, or actually reached, during the activity that generated this issue. This list can contain IP addresses or fully qualified domain names.</p>
alert/app_id	<p>The App-ID associated with this issue.</p>
alert/schedule/activity_first_seen_at	<p>Time when Cortex Cloud Analytics first detected the network activity that caused it to generate the issue. Be aware that there is frequently a delay between this timestamp, and the time when Cortex Cloud Analytics generates an issue (see the <code>alert/schedule/first_detected_at</code> field).</p>



Field Name	Definition
alert/schedule/activity_last_seen_at	Time when Cortex Cloud Analytics last detected the network activity that caused it to generate the issue.
alert/schedule/first_detected_at	Time when Cortex Cloud Analytics first alerted on the network activity.
alert/schedule/last_detected_at	Time when Cortex Cloud Analytics last alerted on the network activity.
user/user_name	The name of the user associated with this issue. This name is obtained from Active Directory.
user/url	Provides the full URL to the user page in the Cortex Cloud Analytics user interface for the user who is associated with the issue.
user/display_name	The user name as retrieved from Active Directory. This is the user name displayed within the Cortex Cloud Analytics user interface for the user who is associated with this issue.
user/org_unit	The organizational unit of the user associated with this issue, as identified using Active Directory.
device/id	A unique ID assigned by Cortex Cloud Analytics to the device. All issues generated due to activity occurring on this endpoint will share this ID.
device/url	Provides the full URL to the device page in the Cortex Cloud Analytics user interface.
device/mac	The MAC address of the network card in use on the device.
device/hostname	The device host name.
device/ip	The device IP address.
device/ip_ranges	<p>Identifies the subnet or subnets that the device is on. This sequence can contain multiple inclusive subnets. Each element in this sequence is a JSON object with the following fields:</p> <ul style="list-style-type: none"> <li>• <b>asset:</b> The asset name assigned to the device from within the Cortex Cloud Analytics user interface.</li> <li>• <b>max_ip:</b> Last IP address in the subnet.</li> <li>• <b>min_ip:</b> First IP address in the subnet.</li> <li>• <b>name:</b> Subnet name.</li> </ul>
device/owner	The user name of the person who owns the device.
device/org_unit	The organizational unit that owns the device, as identified by Active Directory.



Field Name	Definition
files	<p>Identifies the files associated with the issue. Each element in this sequence is a JSON object with the following fields:</p> <ul style="list-style-type: none"> <li>• <b>full_path</b>: The file full path (including the file name).</li> <li>• <b>md5</b>: The file MD5 hash.</li> </ul>

## 2.3.2 | Cortex MCP server

Learn how to install, configure, and use the Cortex MCP Server with Cortex Cloud.

### 2.3.2.1 | Cortex MCP server overview

#### Abstract

The Cortex MCP server enables you to leverage Cortex's powerful capabilities directly through natural language. Use built-in tools to manage cases and issues and conduct investigations, with the flexibility to create and customize new tools to fit specific use cases and workflows.

The Cortex MCP Server enables you to access Cortex's powerful features directly within your Large Language Model (LLM) apps. Built on the Model Context Protocol (MCP), a standard for connecting AI models to work with other applications and tools, enabling you to query your Cortex tenant and conduct investigations using natural language.

**NOTE:**

This feature is in **Beta**.

#### Key capabilities

- Investigate
- Use the built-in tools to manage cases and issues, and conduct investigations.
- Customize
- Create, customize, and fine-tune tools to fit specific use cases and workflows.
- Flexible client

The Cortex MCP Server is provided as a downloadable file that can be installed on a local machine or a container. While these instructions use Claude Desktop as the MCP client, you can use any client that supports MCP. More detailed setup instructions are provided in a README file included in the download.

**NOTE:**

The Cortex MCP Server empowers you to integrate AI into your security workflows using natural language. When using LLM-based suggestions, always review and approve actions suggested by the AI before they're executed. We recommend deploying the Cortex MCP server in a secure environment where access is limited to authorized users.

To install, configure, and use the Cortex MCP server:

1. Install the Cortex MCP server
2. Configure the MCP client
3. (Optional) Create custom Cortex MCP server tools
4. Use the Cortex MCP server

#### 2.3.2.1.1 | Install the Cortex MCP server

#### Abstract

Download, install, and configure the MCP server on your local machine or a container.

With the Cortex MCP Server, you can use natural language in your MCP client to investigate and manage cases and issues. The MCP Server can be run within a Docker container or a Poetry virtual environment.

This documentation contains instructions for configuring and using the Cortex MCP server. More detailed setup instructions are provided in a README file included in the download.

These instructions use Claude Desktop, but you can use any client that supports MCP.



## **PREREQUISITE:**

If you are running the Cortex MCP server in a Poetry virtual environment, you must have Python 3.13 or higher.

If you plan to run the Cortex MCP server in a Docker container, you must have Docker installed.

Step 1: Create an API key

### **NOTE:**

The MCP Server uses public APIs to communicate and is limited by the license quotas available in your tenant. This is particularly relevant when running XQL queries. For more information on running XQL query APIs, see Run XQL query APIs.

1. Select Settings → Configurations → Integrations → API Keys → New Key.

2. In the Role tab, perform for the following:

a. Under Security Level, select Standard.

b. Under Role, select the desired level of access for this key. You can select from predefined roles or custom roles. Roles are available according to what was defined in either the Cortex Gateway or the tenant's Access Management. You can view the configuration of the role selected by expanding the sections under Components.

### **NOTE:**

It is critical to avoid assigning excessive permissions when creating an API key for the Cortex MCP Server. Since the key has both read and write capabilities, overly broad permissions can lead to unintended actions and potentially compromise your environment. Ensure the key follows the principle of least privilege and is granted only the minimum required access.

c. (Optional) Under Comment, provide a comment that describes the purpose of the API key.

d. (Optional) If you want to define a time limit on the API key authentication, select Enable Expiration Date, and select the expiration date and time. You can track the expiration date of each API key in the API Keys page. In addition, a API Key Expiration notification appears in the Notification Center one week and one day prior to the defined expiration date.

3. (Optional) If Scope-Based Access Control (SBAC) is enabled for the tenant, click Scope, and under Scope Definition, select the scope areas that you want to limit the user role to access for this API.

4. Click Generate to generate the API key.

5. Copy the generated API key and click Done.

### **IMPORTANT:**

To configure the Cortex MCP Server, you need the Cortex API URL, Cortex API key, and Cortex API key ID. You will not be able to view the API key again after you complete this step. Ensure that you copy the API key before closing the notification.

Step 2: Download and install the Cortex MCP server

1. Go to Settings → Configurations → Integrations → Cortex MCP Server.

2. Download MCP File

3. (Optional) Download the checksum file and run a command such as `shasum` (Linux/macOS) or `certutil` (Windows) to verify the integrity and authenticity of the file. For example: `shasum -a 256 -c cortex-checksum.zip.sha256`.

4. Extract the .zip file.

5. Follow the detailed instructions in the README.md file located in the top directory. Instructions are provided for both Docker and Poetry and include the following:

Docker

- Create an .env file with the environment variables.

### **NOTE:**

When using Docker, we recommend using an .env file to set the Cortex API credentials as environment variables. While the credentials can be provided in the MCP client configuration settings, the .env file provides safer handling of API credentials and makes your configuration easily reproducible.

- Build and run the Docker container.

Poetry

- Install Poetry.
- Create and activate a virtual environment.
- Install project dependencies.
- Provide the required variables in the Python runtime environment.



#### NOTE:

By default, stdio (standard input/output) is used. You can also configure Streamable HTTP, to send requests directly to the tenant instead of through the MCP client. Streamable HTTP can be useful for testing in the browser without a MCP client and to bypass limits that may be in place for your MCP client. For Docker, you can include the Streamable HTTP variables in the .env file. You can also include it as a flag when you start the server in the Python virtual environment.

Docker

```
docker run --env-file .env -it cortex-mcp
```

Poetry virtual environment

```
python src/main.py
```

When using the Poetry virtual environment, you can also start the server using the CLI command `python src/cli.py start [OPTIONS]`, where [OPTIONS] includes the API key id, API key, the Cortex PAPI server URL, and the log level.

Use the CLI

From the CLI, you can run three commands.

- **start**: Start the Cortex MCP server. Relevant only for the Poetry virtual environment.
- **update**: Any new or updated components provided by Cortex are automatically downloaded into the `remote_components` folder. During each update, the folder is fully replaced and all existing contents are recreated. Do not add custom tools to this directory, as it is managed entirely by Cortex and is overwritten at every update.
- **version**: Display the current version of the Cortex MCP Server.

Additional information about the CLI is available in the README file located in the `src` directory.

#### 2.3.2.1.1 Configure the MCP client

Abstract

Configure your local MCP client to communicate with the Cortex MCP server.

After you have downloaded and installed the Cortex MCP server, you need to configure your local MCP client to communicate with the Cortex MCP server. The instructions below use Claude Desktop, but any MCP client can be used.

1. In the Claude Desktop app, navigate to Settings → Developer → Edit Config. The configuration file opens in your default text editor.

For reference, the file is located at:

- macOS: `~/Library/Application Support/Claude/cladev_desktop_config.json`
- Windows: `%APPDATA%\Claude\cladev_desktop_config.json`

2. Add the `mcpServers` configuration to the file. The examples below are provided for local client (Poetry virtual environment) and container (Docker). The exact details of your `mcpServers` configuration depend on your specific installation.

Poetry virtual environment

```
{
  "mcpServers": {
    "Cortex MCP Server": {
      "command": "python",
      "args": [
        "/path/to/cortex-mcp/src/main.py"
      ],
      "env": {
        "CORTEX_MCP_PAPI_URL": "https://api.cortex.example.com",
        "CORTEX_MCP_PAPI_AUTH_HEADER": "<your_api_key>",
        "CORTEX_MCP_PAPI_AUTH_ID": "<your_api_key_id>",
        "MCP_TRANSPORT": "stdio/streamable-http"
      }
    }
  }
}
```

Docker Container

```
{
  "mcpServers": {
    "Cortex MCP Server": {
      "command": "docker",
      "args": [
        "run",
        "--env-file",
        ".env"
      ]
    }
  }
}
```



```

        "/path/to/.env",
        "-i",
        "--rm",
        "cortex-mcp"
    ]
}
}
}

```

3. Save the changes to the configuration file and restart Claude Desktop for the changes to take effect.

4. Verify the connection to the Cortex MCP server. You should see the Cortex MCP server running in the Developer settings and a hammer icon may appear in the input box, indicating the MCP tools are available.

#### 2.3.2.1.3 | Use the Cortex MCP server

##### Abstract

Use the MCP server to investigate and manage cases and issues from your local MCP client.

The Cortex MCP server provides built-in tools to manage cases and issues and conduct investigations.

Built-in tools include, but are not limited to:

- **get\_assets**: Fetch all assets, or a filtered subset of assets, based on criteria such as category, region or provider.
- **get\_assets\_by\_id**: Fetch detailed information about the asset specified by the asset ID.
- **get\_cases**: Fetch all cases, or a filtered subset of cases matching specific criteria such as domain, status, severity or specific case ID.
- **get\_issues**: Fetch all issues, or a filtered subset of issues matching specific criteria such as domain, severity, detection method or specific issue ID.
- **get\_assessment\_results**: Fetch the results of all or filtered compliance assessments from the Cortex platform.
- **get\_filtered\_endpoints**: Fetch a filtered list of endpoints managed by the XDR agents based on their status, XDR agent status, and other filters.

When you run the `update` command in the Cortex MCP server, new or updated tools provided by Cortex are automatically downloaded.

You also have the flexibility to create and customize your own tools to fit specific use cases and workflows. For more information, see Create custom Cortex MCP server tools.

##### Use case examples

##### **NOTE:**

The built-in tools retrieve information, but do not write to the tenant. You can create your own tools that include write actions. The examples below include both.

- Show me the top ten most critical cases and create a graphical representation for my manager to review.
- Give me the details for case ID 12345 and create a visual timeline.
- Isolate endpoint WIN-123 because it may be compromised.
- Retrieve full details for endpoint XXXX.
- Add a note to case 12345 saying “Escalated to Tier 2 for further investigation.”

#### 2.3.2.1.4 | Create custom Cortex MCP server tools

##### Abstract

Create your own customized tools to manage cases and issues.

You can build your own tools using OpenAPI or Python to manage cases, handle issues, and conduct investigations. More detailed information can be found in the README file located in the `src/usecase` directory. Tools are based on Cortex API endpoints.

To view the Cortex Cloud API documentation, see Cortex Cloud Platform APIs.

##### **NOTE:**

Any new or updated components provided by Cortex are automatically downloaded into the `remote_components` folder. During each update, the folder is fully replaced and all existing contents are recreated. Do not add custom tools to this directory, as it is managed entirely by Cortex and is overwritten at every update.

##### OpenAPI

You can create an OpenAPI specification for a specific API endpoint.



1. Create a YAML file in the `/custom_components/openapi` directory with the name of the MCP component. For example: `custom_cortex_component.yaml`.
2. Base your custom OpenAPI component on the Cortex API documentation structure for a specific endpoint. We recommend viewing the built-in tools, located at `/builtin_components/openapi`, as a reference.
3. After you define the OpenAPI specification, the Cortex MCP server collects it automatically and it is ready for use.
4. Test your new MCP component by running the Cortex MCP server and writing a prompt that uses your new component.

#### Python

We recommend using Python for more complex MCP components that require custom logic. MCP components in Python are defined in a module.

1. Create a new Python file in the `/custom_components` directory.
2. Define a class that inherits from the `BaseModule` class with the required methods. We recommend viewing the built-in modules, located at `/builtin_components`, as a reference.
3. After you define a class, the Cortex MCP server collects it automatically and it is ready for use.
4. Test your new MCP component by adding an end-to-end test in the `tests/e2e` directory or run the MCP server and write a prompt that uses your new component.

### 2.3.3 | Manage user roles and access management

#### Abstract

Learn how to manage access for users, user roles, user groups, and Single Sign-On (SSO) for users on a specific Cortex Cloud tenant.

#### PREREQUISITE:

Managing users, roles, scopes, user groups, authentication settings in Cortex Cloud Access Management requires View/Edit RBAC permissions for Access Management (under Configurations). Account Admin and Instance Administrator roles are granted this permission by default. For more information, see *Predefined user roles* in Set up users and roles.

Access management enables you to control who can access the different parts of your organization's resources. It ensures only authorized users can interact with sensitive data.

Cortex Cloud uses a combination of Role-Based Access Control (RBAC) and Scope-Based Access Control (SBAC) to ensure scalability and granular control.

What is the difference between RBAC and SBAC?

RBAC assigns permissions based on a user's organizational role, such as Investigator or Responder, establishing a clear hierarchy and set of capabilities for each role and simplifying management by linking access to job functions. RBAC does this by helping to manage access to Cortex Cloud components and Cortex Query Language (XQL) datasets, so that users, based on their roles, are granted minimal access required to accomplish their tasks.

SBAC refines RBAC by granting access only to the relevant data that the user requires for their designated role. Users with Access Management permission apply scopes to limit the data and content that users can be granted access to in Cortex Cloud, which are divided into different scoping areas. The scoping areas include Assets, Cases and Issues, and Endpoints, which can be applied as relevant to the enforcement area or entity.

For example, an Investigator role might have access to asset information based on the RBAC permissions, but SBAC granular scoping could limit that investigator's view and control to only assets within a particular scoping area. This hybrid approach ensures scalability and granular control, significantly strengthening system security.

Understanding more about access management concepts

You can manage access for users, and create and assign user roles and user groups for a specific tenant. When Single Sign-On (SSO) is enabled, you can manage SSO for users.

#### Users

You can manage access permissions and activities for users allocated to a specific Customer Support Portal account and tenant. All users must belong to a user group or have an assigned role.

#### User roles

User roles enable you to define the type of access and actions a user can perform. User roles are assigned to users, user groups, or API keys.

#### NOTE:

For more information on assigning user roles when generating an API key, see [Manage API keys](#).

#### Predefined user roles



Cortex Cloud provides predefined built-in user roles that provide specific access rights that cannot be modified. You can also create custom, editable user roles. To view the predefined permissions for each default role, go to Settings → Configurations → Access Management → Roles.

#### Dataset access permissions

You can also set dataset access permissions using user roles or set specific permissions using role-based access control (RBAC). Configuring administrative access depends on the security requirements of your organization. Dataset permissions control dataset access for all components, while RBAC controls access to a specific component. By default, dataset access management is disabled, and users have access to all datasets. If you enable dataset access management, you must configure access permissions for each dataset type, and for each user role. When a dataset component is enabled for a particular role, the Issues and Cases pages include information about datasets. For more information on how to set dataset access permissions, see [Manage user roles](#).

#### NOTE:

Some features are license-dependent. Accordingly, users may not see a specific feature if the feature is not supported by the license type or if they do not have access based on their assigned role or scope.

#### User groups and scoping areas

You can use user groups to streamline configuration activities by grouping together users whose access permission requirements are similar. Import user groups from Active Directory, or create them from scratch in Cortex Cloud.

Users with Access Management permission can further restrict access of these user groups, specifically for the designated role and list of users configured in the user group by granting access only to the relevant data that the user requires for their designated role. This is performed by applying scopes to limit the data and content that users can be granted access to in Cortex Cloud, which are divided into different scoping areas. The scoping areas include Assets, Cases and Issues, and Endpoints, which can be applied as relevant to the enforcement area or entity. This enables you to adhere to your company's security policies of limiting user access by specifying, for example, which groups of assets users can access and what actions they can perform.

#### NOTE:

For features where scoping is not applicable, Role-Based Access Control (RBAC) is used and can be configured when managing user roles. For more information, see [Manage user roles](#).

#### Single Sign-On

Manage your SSO integration with the Security Assertion Markup Language (SAML) 2.0 standard to securely authenticate system users across enterprise-wide applications and websites, with one set of credentials. This configuration allows system users to authenticate using your organization's Identity Provider (IdP), such as Okta or PingOne. You can integrate any IdP with Cortex Cloud supported by SAML 2.0.

SSO with SAML 2.0 configuration activities are dependent on your organization's IdP. Some of the field values need to be obtained from your organization's IdP, and some values need to be added to your organization's IdP. It is your responsibility to understand how to access your organization's IdP to provide these fields, and to add any fields from Cortex Cloud to your IdP.

After SSO configuration is complete, when you sign in as an SSO user, the Cortex Cloud permissions granted to you after logging in, either from the group mapping or from the default role configuration, are effective throughout the entire session for the defined maximum session length. Maximum session length is defined in your Cortex Cloud Session Security Settings. This applies even if the default role configuration is updated, or the group membership settings were changed.

#### 2.3.3.1 | Manage user roles

##### Abstract

Manage user roles that are assigned to Cortex Cloud users or user groups in Cortex Cloud Access Management.

#### PREREQUISITE:

Managing user roles in Cortex Cloud Access Management requires View/Edit RBAC permissions for Access Management (under Configurations). Account Admin and Instance Administrator roles are granted this permission by default. For more information, see [Predefined user roles](#) in Set up users and roles.

Review the following topics:

- Set up users and roles
- User group management
- Assign user roles and groups
- Manage user roles and access management

Manage user roles that are assigned to Cortex Cloud users, user groups, or API keys. User roles enable you to define the type of access and actions a user can perform.

You can only set dataset access permissions from a user role in Cortex Cloud Access Management for the tenant. When creating user roles from the Cortex Gateway, these settings are disabled. By default, dataset access management is disabled, and users have access to all datasets. If you enable dataset access management, you must configure access permissions for each dataset type, and for each user role. When a dataset component is enabled for a particular role, the Issues and Cases pages include information about datasets.

[Create a user role](#)



1. Select Settings → Configurations → Access Management → Roles.
2. Click New Role.
3. Under Role Name, enter a name for the user role.
4. (Optional) Under Description, enter a description for the user role.
5. Under Components, expand each list and select the permissions for each of the components.
6. Under Datasets (Disabled), you have two options for setting the Cortex Query Language (XQL) dataset access permissions for the user role:
  - Set the user role with access to all XQL datasets by leaving the dataset access management as disabled (default).
  - Set the user role with limited access to certain XQL datasets by selecting the Enable dataset access management toggle and selecting the datasets under the different dataset category headings.
7. Click Save.

#### Edit a user role

1. Select Settings → Configurations → Access Management → Roles.
2. Right-click the relevant user role, and select Edit Role.
3. (Optional) Under Role Name, modify the name for the user role.
4. (Optional) Under Description, enter a description for the user role or modify the current description.
5. Under Components, expand each list and select the permissions for each of the components.
6. Under Datasets, you have two options for setting the Cortex Query Language (XQL) dataset access permissions for the user role:
  - Set the user role with access to all XQL datasets by disabling the Enable dataset access management toggle.
  - Set the user role with limited access to certain XQL datasets by selecting the Enable dataset access management toggle and selecting the datasets under the different dataset category headings.
7. Click Save.

#### Create new role based on an existing role

1. Select Settings → Configurations → Access Management → Roles.
2. Right-click the relevant user role, and select Save As New Role.
3. (Optional) Under Role Name, modify the name for the user role.
4. (Optional) Under Description, enter a description for the user role or modify the current description.
5. Under Components, expand each list and select the permissions for each of the components.
6. Under Datasets, you have two options for setting the Cortex Query Language (XQL) dataset access permissions for the user role:
  - Set the user role with access to all XQL datasets by disabling the Enable dataset access management toggle.
  - Set the user role with limited access to certain XQL datasets by selecting the Enable dataset access management toggle and selecting the datasets under the different dataset category headings.
7. Click Save.

### 2.3.3.2 | Manage user access

#### Abstract

Manage access permissions for Cortex Cloud users.

#### **PREREQUISITE:**

Managing users, roles, scopes, user groups, authentication settings in Cortex Cloud Access Management requires View/Edit RBAC permissions for Access Management (under Configurations). Account Admin and Instance Administrator roles are granted this permission by default. For more information, see *Predefined user roles* in Set up users and roles.

Review the following topics:



- Set up users and roles
- User group management
- Assign user roles and groups
- Manage user roles and access management
- Manage user scope

Manage access permissions for Cortex Cloud users.

#### [Edit user permissions](#)

Update a user's role and scope, add a user to a user group, and view permissions based on the role, scope, and user groups assigned to the user.

You can configure granular scoping for Scope-Based Access Control (SBAC) by granting access only to the relevant data that the user requires for their designated role. Administrators apply scopes to limit the data and content that users can be granted access to in Cortex Cloud, which are divided into different scoping areas. The scoping areas include Assets, Cases and Issues, and Endpoints, which can be applied as relevant to the enforcement area or entity. For more information, see [Manage user scope](#).

#### **NOTE:**

You can only reduce the permissions of an Account Admin user via Cortex Gateway.

1. Select Settings → Configurations → Access Management → Users.
2. Right-click the relevant user, and select Edit User Permissions.

#### **TIP:**

To apply the same settings to multiple users, select them, and then right-click and select Edit User Permissions.

3. In the Role tab, under Role, select the default or custom role.
4. (Optional) Under User Groups, add the user to a group.
5. (Optional) Under Show Accumulated Permissions:
  - a. Do one of the following:
    - Select all to view the combined permissions for every role and user group assigned to the user.
    - Select a specific role assigned to the user to view the available permissions for that role.
  - b. Under Components, expand each list to view the permissions to the various Cortex Cloud components.
  - c. Under Datasets, there are two possibilities for viewing a user's dataset access permissions:
    - When dataset access management is enabled and the user has access to certain Cortex Query Language (XQL) datasets, the datasets are listed.
    - When dataset access management is disabled and users have access to all XQL datasets, the text No dataset has been selected is displayed.

#### **NOTE:**

User permissions for components and datasets are based on the access permissions set in the user role. For more information on editing these user role permissions, see [Manage user roles](#).

6. (Optional) You can configure granular scoping:

- a. Click the Scope tab.
- b. Under Scope Definition, expand the scoping areas that you want to grant the user role access to in the tenant by clicking the chevron icon (>) beside the scoping area title, and make any changes required. The following table explains the options available to configure:

#### **IMPORTANT:**

Before configuring, ensure that you review [Understand scoping](#) in the [Manage user scope](#) section.



Scoping Area    Granular Scoping Configurations	
Assets	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• No assets: No asset is accessible.</li> <li>• All assets: Defines access to all assets.</li> <li>• Select asset groups: Defines access to the specific assets associated with the Asset Groups selected, and to view all their related cases, issues, and findings for these specific assets and Asset Groups. Under Select asset groups, define the specific asset groups that you want to grant access. Only Asset Groups relevant for scoping are listed, which are asset groups that are using only the asset attributes listed in Manage user scope (under Understand scoping â Scoping Areas â Assets).</li> </ul> <p>The scoping of assets also affects the scoping of cases, issues, and findings.</p> <p><b>NOTE:</b></p> <p>Visibility of Security domain Issues that refer to assets with agents is controlled by the Endpoints scoping configuration.</p>
Cases and Issues	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• No cases and issues: Defines access to no cases and issues.</li> <li>• All cases and issues: Defines access to all cases and issues. Users can view cases or issues referencing assets within their scope. Use the Assets section to define which assets are in scope.</li> <li>• Select domains: Defines access to the domains selected to view their related cases and issues. Under Select domains, define the specific domains that you want to grant access.</li> </ul> <p>Users can only view cases or issues referencing assets and endpoints within their scope. Use the Assets section to define which assets are in scope.</p> <p>When selecting All cases and issues or Select domains, you can separately configure access to issues and cases that lack an asset reference or where the referenced asset is not in All Assets and All Endpoints inventories. To provide access, select the Allow access to cases and issues that are not referencing known assets or endpoints checkbox.</p>
Endpoints	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• No endpoints: Defines access to no endpoints with no ability to view their related agent management and enterprise policies.</li> <li>• All endpoints: Defines access to all endpoints with the ability to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> <li>• Select specific (at least one required): Defines specific access to all endpoint groups by selecting Endpoint Groups or all endpoint tags by selecting Endpoint Tags to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> </ul>

#### IMPORTANT:

By default, Enable Scope Based Access Control is disabled in Settings â Configurations â General â Server Settings, and granular scoping is not enforced. Before enabling SBAC, we recommend that an administrator or a user with Access Management permissions first ensures that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes. For more information, see [Manage user scope](#).

7. Click Save.

#### Import multiple users

Use a CSV file to import users who belong to a Customer Support Portal account, and assign them roles that are defined in Cortex Cloud. You can use the CSV template provided in Cortex Cloud, or prepare a CSV file from scratch.

1. Select Settings â Configurations â Access Management â Users.
2. Click Import Multiple User Roles.
3. Do one of the following:



- To use the CSV template, click Download example file, and replace the example values with your values.
- Prepare a CSV file from scratch. Make sure the file includes these columns:
  - User email: Email address of the user belonging to a Customer Support Portal account, for example, john.smith1@exampleCompany.com.
  - Role name: Name of the role that you want to assign to this user, for example, Privileged Responder. The role must already exist in Cortex Cloud.
  - Is an account role: A boolean value that defines whether the user is designated with an Account Admin role in Cortex Gateway. Set the value to TRUE; otherwise, the value is set to FALSE (default).

4. Locate the file and drag it to the dialog box.

5. Click Import.

#### [View user permissions](#)

View all of the permissions currently assigned to a user.

1. Select Settings → Configurations → Access Management → Users.

2. Right-click the relevant user, and select Edit User Permissions.

#### **TIP:**

To apply the same settings to multiple users, select them, and then right-click and select Edit User Permissions.

3. In the Role tab, under Show Accumulated Permissions, do one of the following:

- Select all to view the combined permissions for every role and user group assigned to the user.
- Select a specific role assigned to the user to view the available permissions for that role.

4. Under Components, expand each list to view the permissions to the various Cortex Cloud components.

5. Under Datasets, there are two possibilities for viewing a user's dataset access permissions:

- When dataset access management is enabled and the user has access to certain Cortex Query Language (XQL) datasets, the datasets are listed.
- When dataset access management is disabled and users have access to all XQL datasets, the text No dataset has been selected is displayed.

6. To view the granular scoping configurations granted to the user role, click the Scope tab, and under Scope Definition, expand the scoping areas to view the settings by clicking the chevron icon (>) beside the scoping area title. The scoping areas include Assets, Cases and Issues, and Endpoints.

#### [Hide user](#)

There might be instances where you want to hide a user from the list of users, for example, a user that has a Customer Support Portal Super User role but isn't active on your Cortex Cloud tenant. After you hide a user, they will no longer be displayed in the list of users when Show User Subset is selected on the Users page.

1. Select Settings → Configurations → Access Management → Users.

2. Right-click the relevant user, and select Hide User.

#### [Add user to a user group](#)

1. Select Settings → Configurations → Access Management → Users.

2. Right-click the relevant user, and select Edit User Permissions.

#### **TIP:**

To apply the same settings to multiple users, select them, and then right-click and select Edit User Permissions.

3. Under User Groups, add the user to a group.

4. Click Save.

#### [Deactivate user](#)

You cannot deactivate a user who has an Account Admin role.

1. Select Settings → Configurations → Access Management → Users.

2. Right-click the relevant user, and select Deactivate User.

3. Click Deactivate.



#### Remove role assigned to user

You cannot remove a user who has an Account Admin role.

1. Select Settings â Configuration â Access Management â Users.
2. Right-click the relevant user, and select Remove User Role.
3. Click Remove.

#### 2.3.3.2.1 | User access reference information

The following is a list of common fields on the Users page:

Field	Description
Show User Subset	Displays all users except for hidden users.
User Type	Indicates whether a user was defined in Cortex Cloud using the Customer Support Portal, SSO (single sign-on) using your organization's IdP, or both Customer Support Portal/SSO.
Direct XDR Role	Name of the role specifically assigned to a user. When a user does not have any Cortex Cloud access permissions assigned specifically to them, the field displays No-Role.
Groups	Lists the groups to which a user belongs. Any group that was imported from Active Directory displays AD beside the group name. If a user group has scoping permissions, the users in the group are granted permissions according to the user group settings, even if the user does not have configured scope settings.
Group Roles	Lists the group roles based on the groups to which a user belongs. Hovering over the group role displays the group associated with this role.
Scope	Lists a summary of the granular scoping configured for the user.
Groups Scope	Lists a summary of the granular scoping configured in the user groups that the user belongs to

#### 2.3.3.3 | Manage user scope

##### Abstract

Learn about Scope-Based Access Control (SBAC) and how to assign users to specific scoping areas in your organization.

##### PREREQUISITE:

- Configuring user scopes in Cortex Cloud Access Management requires View/Edit RBAC permissions for Access Management (under Configurations). Account Admin and Instance Administrator roles are granted this permission by default. For more information, see *Predefined user roles* in Set up users and roles.
- By default, Enable Scope Based Access Control is disabled in Settings â Configuration â General â Server Settings, and granular scoping is not enforced. Before enabling SBAC, we recommend that you first ensure that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes.

Review the following topics:

- Set up users and roles
- User group management
- Assign user roles and groups
- Manage user roles and access management



Cortex Cloud enables you to use Scope-Based Access Control (SBAC) in combination with Role-Based Access Control (RBAC) to define precise access controls according to your organization's security policies. While RBAC defines what a role can access and the actions that can be performed, SBAC determines the specific data and content displayed when accessing these areas and performing those actions.

Users with Access Management permission apply scopes to limit the data and content that users can be granted access to in Cortex Cloud, which are divided into different scoping areas. The scoping areas include Assets, Cases and Issues, and Endpoints, which can be applied as relevant to the enforcement area or entity. For example, an Investigator role might have access to asset information based on the RBAC permissions, but the SBAC granular scoping configuration could limit that investigator's view and control to only assets within a particular scoping area. This hybrid approach ensures scalability and granular control, significantly strengthening system security by ensuring only authorized users are granted access to the relevant data that the user requires for their designated role.

Granular scoping for all scoping areas is configured in users, user groups, or API Keys according to the designated user role. Users are granted granular scoping access based on the user role assigned to them either in a user group or directly.

#### Things to consider before configuring SBAC

Before you begin setting Scope-Based Access Control (SBAC) granular scoping, consider the following information:

- SBAC is disabled by default, which means that users have access to all content and data in the areas they have access to according to the RBAC permissions defined in their role.
- To best address Cases that span across all scopes, we recommend that there always be designated users with full access to all cases, issues, assets, and findings.
- Policies and playbook execution can affect items outside the user's scope, even though scoped users can't view them. As a result, we recommend that users who write policies be granted access to all relevant policy assets, so they can review the effects of the policies.
- Some areas and features in Cortex Cloud do not comply with SBAC. In these cases, use RBAC permissions to restrict access. For more information, see Functional areas that respect and don't respect SBAC.
- Respecting SBAC has some performance overhead when opening the Cases, Issues, Findings, and Assets tables, which can take more time.
- In Reports, SBAC applies when a report is manually generated, not when it is accessed in any other way. Scheduled reports do not run in any user context and are not subject to SBAC.
- For users who upgraded from a previous version of Cortex Cloud to the current version, see the What's New in Cortex XSIAM 3.x Guide for specific changes that you should know about.

#### Understand scoping

##### Scoping areas

User Groups, Users, and API Keys can be scoped according to the following scoping areas:

- **Assets:** Provides access to the assets associated with asset groups, and enables you to access their related cases, issues, and findings. When using asset groups, you can limit access based only on this list of attributes: Asset Class, Category, Provider, Region, Organization, Realm, Business Application Names, Kubernetes Cluster, Kubernetes Namespace, Code Repository, and Asset Tags.
  - When you create or edit an Asset Group, the changes are applied immediately to new assets and to existing assets that have been updated. Yet, it can take a few hours for the changes to appear on existing assets that have not been updated.
- **Cases and Issues:** Provides access to domains to view their related cases and issues.
- **Endpoints:** Applies scoping on an endpoint as an entity and provides access to Endpoint Groups and Endpoint Tags to view their related agent management and enterprise policies.

#### NOTE:

This configuration can impact the visibility of the related Security domain in the Cases and Issues scope area, but will not affect asset visibility.



## Scoping Behaviors

- When applicable, all conditions must be met to apply the scope configuration. For example, an issue with an affected asset is accessible only if the asset is in scope and the issue's domain is in scope.
- SBAC allows viewing cases and issues with no affected assets or endpoints, or when at least one affected asset is in the user's scope. The user can see all affected assets, including those not in scope, but won't be able to see more details about the assets not in scope, including opening their card.
- Cases and Issues of deleted assets do not have affected assets and so are not affected by asset-led SBAC or Endpoints, and are only based on the Cases and Issues domain.
- SBAC allows viewing cases where at least one of its issue domains is in the user's scope. The user can see all issues, including those not in scope, but won't be able to see more details about the issues not in scope, including opening their card.
- The behavior of cases and issues with affected endpoints depends on the Endpoint Scoping mode.
- XQL queries that use the `cases`, `issues`, `findings`, and `asset_inventory` datasets respect only the Assets scoping area configurations.

## Functional areas that respect and don't respect SBAC

It is important to review both the functional areas and features in Cortex Cloud that are respected and not fully respected so you can decide what actions to take in your tenant.

### Functional areas respected

Scope-Based Access Control (SBAC) applies to the following functional areas in Cortex Cloud:

#### **IMPORTANT:**

Some areas and features in Cortex Cloud do not respect SBAC. In these cases, use RBAC permissions to restrict access.

Functional Area	Description	Related Scoping Area
Cases, Issues, Findings, and Assets tables	View and manage cases, issues, findings, and assets, and take actions in these tables.	<ul style="list-style-type: none"><li>Assets</li><li>Cases and Issues</li><li>Endpoints</li></ul>
Dashboard and Reports	Scoping takes place only on the following: <ul style="list-style-type: none"><li>XQL-related widgets based on XQL queries that use the <code>cases</code>, <code>issues</code>, <code>findings</code>, and <code>asset_inventory</code> datasets, and respect only the Assets scoping area configurations.</li><li>Agent-related widgets.</li></ul> <p><b>NOTE:</b> XQL-based dashboard widgets may require a few hours to initially reflect changes to the list or definitions of asset groups used for scoping. To view the most current data immediately, refresh the dashboard or its XQL widgets.</p>	<ul style="list-style-type: none"><li>Assets</li><li>Cases and Issues</li><li>Endpoints</li></ul>
Public APIs	Public APIs that access Cases, Issues, Findings, and Assets information respect Scope-Based Access Control (SBAC).	<ul style="list-style-type: none"><li>Assets</li><li>Cases and Issues</li></ul>
Cortex Query Language (XQL)	When using XQL with <code>cases</code> , <code>issues</code> , <code>findings</code> , and <code>asset_inventory</code> datasets, keep in the mind the following: <ul style="list-style-type: none"><li>XQL respects asset-led SBAC when accessing these datasets, including when using XQL queries and XQL widgets.</li><li>XQL queries that use these datasets, respect only the Assets scoping area configurations.</li></ul> <p><b>NOTE:</b> For Cases and Issues domains, a workaround is to create a Dataset View for each required combination of domains, and allow the relevant entity access only to this Dataset View, not to the underlying <code>cases</code> and <code>issues</code> datasets.</p>	Assets



Functional Area	Description	Related Scoping Area
Endpoint Administration table	View endpoints and take actions on endpoints.	Endpoints
Policy Management	Create and edit Prevention policies and profiles, Extension policies and profiles, and global and device Exceptions that are within the scope of the user.	Endpoints
Action Center	View and take actions only on endpoints that are within the scope of the user.	Endpoints
Identity Security	View and manage identity assets, permissions, and issues that are within the scope of the user. For more information, see Manage RBAC and SBAC in Cortex Cloud Identity Security.	<ul style="list-style-type: none"> <li>• Assets</li> <li>• Cases and Issues</li> </ul>
Cloud Workload Policies	View Cloud Workload Policies when user access is scoped to any of the available options: All assets, No assets, or Select asset groups. When no SBAC restriction is applied, the user's access is determined solely by their RBAC permissions. For more information, see Cloud Workload Policies and Rules.	Assets

#### SBAC not fully respected functional areas

Ensure that you review the points below that explain the main functional areas with limitations with respecting SBAC, so you can decide how to handle this in your tenant. A suggested action is provided when applicable.

- Access to datasets: Access to the **alerts** and **incidents** datasets do not support SBAC. As a result, consider limiting users from accessing these datasets by excluding access to the datasets mentioned above using Dataset Views, and only enabling access to **cases** and **issues** datasets that respect SBAC.
- Graph Search: Graph Search does not support SBAC. It is currently a Beta feature and is only available in the tenant using a feature flag.
- Command Centers: Aggregate numbers in Command Centers can also sum up data that is not in the user scope. When pivoting from Command Centers to the Cases, Issues, Findings, and Assets tables, these tables do respect SBAC. We recommend limiting the users who access Command Centers, and these users should be granted a broader scope. For all other users, disable access in RBAC settings (Dashboards & Reports â> Command Center Dashboards).
- Host Inventory

We recommend disabling access in RBAC settings (Investigation & Response â> Search â> Host Insights).

- Timeline widget

As a workaround, you can disable access through RBAC permissions by disabling Dashboards (Dashboards & Reports â> Dashboards).

- Notification Center
- Agent Installation widget: This widget is not available for scoped users.
- Drop-downs of cases and issues domains: Drop-downs of these domains display all domains.
- KSPM dashboard: Users can access all information on the dashboard when their user access is scoped to view All assets or assigned to the Instance Administrator role. Otherwise, users with granular scoping set to No assets or Select asset groups will have limited access to the dashboard. For more information on the KSPM dashboard, see KSPM dashboard.
- Cloud Workload Policies: Users with SBAC granular scoping (in addition to the RBAC permissions required for Cloud Workload Policies) can only view Cloud Workload Policies when their access is scoped to any of the available options: All assets, No assets, or Select asset groups. When no SBAC restriction is applied, the user's access is determined solely by their RBAC permissions. As a result, if you want users to be able to edit and modify Cloud Workload Policies, use the RBAC permissions. For more information on Cloud Workload Policies, see Cloud Workload Policies and Rules.

[Feature Change] Visibility for cases and issues without Inventory Assets

#### IMPORTANT:

Action Required: Recent security enhancements enforce stricter default permissions for cases and issues that lack specific asset or endpoint references. This notice explains how to include access to these items if your users' visibility has been impacted.

To improve data security, Cortex Cloud now restricts access by default for cases and issues that do not reference a specific asset or that involve assets not found in your standard inventories.



If your users previously relied on broad access to these items, an administrator or a user with access management permissions must manually enable the new setting to to include access to these cases and issues:

1. Choose one of the following:

- To edit the role for a user or user group, select Settings → Configurations → Access Management.
- To edit the role of an API key, select Settings → Configurations → Integrations → API Keys.

2. Edit the relevant User, User Group, or API Key.

3. In the Scope tab, under Cases and Issues, enable the checkbox: Allow access to cases and issues that are not referencing known assets or endpoints.

4. Save your changes.

Once enabled, an (Extended) label appears next to the scope level.

[How to configure granular scoping](#)

Granular scoping is configured in users, user groups, or API keys, and applied to the user roles assigned. Users are then granted granular scoping access according to the user roles assigned to them in a user group or directly. The instructions below explain how to configure granular scoping according to Palo Alto Networks best practices.

Granular scoping is disabled and not enforced in Cortex Cloud by default. Before enabling SBAC, we recommend that an administrator or a user with Access Management permissions first ensure that the users, user groups, and API Keys defined in Cortex Cloud are granted the required access by assigning the relevant scopes. This user can then assign a scoping area to a Cortex Cloud user (non-administrator), so the non-administrator user can manage only the specific scoping areas that are predefined within that scope.

Any changes made to the granular scoping of a user, user group, or API key are recorded on the Management Audit Logs page (Settings → Management Audit Logs). These events are categorized with the Type set to Permissions and the Subtype set to Scope Edit.

**NOTE:**

Make sure to assign the required default granular scoping for users. This depends on the structure and divisions within your organization and the particular purpose of each organizational unit to which scoped users belong.

1. Ensure that you have the necessary administrator-level permissions.

2. Verify that the users, user groups, and API keys defined in Cortex Cloud are assigned the relevant scopes.

- To verify the granular scoping of a user, select Settings → Configurations → Access Management → Users, right-click the user name, and select Edit User Permissions.
- To verify the granular scoping of a user group, select Settings → Configurations → Access Management → User Groups, right-click the user group, and select Edit Group.
- To verify the granular scoping of an API key, select Settings → Configurations → Integrations → API Keys, right-click the API key, and select Edit.

3. In the Scope tab, expand the scoping areas to review the current granular scoping definitions by clicking the chevron icon (>) beside the scoping area title, and make any changes required. The following table explains the options available to configure:

**IMPORTANT:**

Before configuring, ensure that you review the Understand scoping section.

Scoping Area	Granular Scoping Configurations
Assets	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"><li>• No assets: No asset is accessible.</li><li>• All assets: Defines access to all assets.</li><li>• Select asset groups: Defines access to the specific assets associated with the Asset Groups selected, and to view all their related cases, issues, and findings for these specific assets and Asset Groups. Under Select asset groups, define the specific asset groups that you want to grant access. Only Asset Groups relevant for scoping are listed, which are asset groups that are using only the asset attributes listed in Manage user scope (under Understand scoping → Scoping Areas → Assets).</li></ul> <p>The scoping of assets also affects the scoping of cases, issues, and findings.</p> <p><b>NOTE:</b></p> <p>Visibility of Security domain Issues that refer to assets with agents is controlled by the Endpoints scoping configuration.</p>



Scoping Area	Granular Scoping Configurations
Cases and Issues	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No cases and issues: Defines access to no cases and issues.</li> <li>All cases and issues: Defines access to all cases and issues. Users can view cases or issues referencing assets within their scope. Use the Assets section to define which assets are in scope.</li> <li>Select domains: Defines access to the domains selected to view their related cases and issues. Under Select domains, define the specific domains that you want to grant access.</li> </ul> <p>Users can only view cases or issues referencing assets and endpoints within their scope. Use the Assets section to define which assets are in scope.</p> <p>When selecting All cases and issues or Select domains, you can separately configure access to issues and cases that lack an asset reference or where the referenced asset is not in All Assets and All Endpoints inventories. To provide access, select the Allow access to cases and issues that are not referencing known assets or endpoints checkbox.</p>
Endpoints	<p>Set the Scope by selecting one of the following:</p> <ul style="list-style-type: none"> <li>No endpoints: Defines access to no endpoints with no ability to view their related agent management and enterprise policies.</li> <li>All endpoints: Defines access to all endpoints with the ability to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> <li>Select specific (at least one required): Defines specific access to all endpoint groups by selecting Endpoint Groups or all endpoint tags by selecting Endpoint Tags to view their related agent management and enterprise policies. This configuration can impact the visibility of related Security domain Cases and Issues, but will not affect asset visibility.</li> </ul>

4. Click Save.

5. Repeat steps 2 to 4 until you have configured all users, user groups, and API keys with the correct granular scoping access.

6. Enable granular scoping in Cortex Cloud.

a. Select Settings → Configurations → General → Server Settings, and select the Enable Scope Based Access Control toggle.

b. (Optional) You can select the Endpoint Scoping Mode, which is defined per tenant:

- Permissive: Enables users with at least one scope tag to access the relevant entity with that same tag.
- Restrictive: Users must have all the scoped tags that are tagged within the relevant entity of the system.

c. Click Save.

When you are finished, all the users in Cortex Cloud are now able to use Cortex Cloud only within the granular scoping granted according to their assigned user roles.

#### 2.3.3.4 | Manage access to objects

##### Abstract

Learn more about managing access to objects in Cortex Cloud.

Cortex Cloud enforces least-privileged access by allowing you to manage access for individual instances of custom (user-defined) and system Dashboards and Saved Queries. Access management for these items is handled through a common experience for per-object access, which allows you to treat these tools as distinct objects with their own access settings.

- Custom objects:** User-defined objects that can be fully managed, shared, or deleted by the Owner or an authorized Editor.
- System objects:** Out-of-the-box objects provided by Palo Alto Networks. These are available to any user with access to Dashboards or to Saved Queries and cannot be deleted or have their ownership changed, though they can often be duplicated to create a custom version.

##### Key concepts

Before configuring access, it is important to understand the different states and roles that define an object's security access.

##### General access states



The General access setting determines the baseline visibility for an object:

- **Restricted** (default): The object is visible only to the Owner and those specifically shared with.
- **Public**: The object is visible to all users who have that component enabled in their role permissions. Any user with access to the component can view both Public and System objects, and those with the required role permissions can also edit the Public custom objects.

#### Per-object roles

- **Owner**: The person who created the object. Every object has an assigned Owner responsible for managing its lifecycle and access. Owners have full control, including the ability to edit content, delete the object, and, depending on tenant-level settings, share the object with other principals (users, user groups, or API keys) as an Editor or Viewer.
- **Editor**: Can view and modify the object. If authorized by tenant-level settings, they can also manage access for others.
- **Viewer**: Can view the object and its data but cannot make any changes to the object's configuration or access settings.

**Administrative access**: Account and Instance Administrators have inherent visibility into all objects (including Restricted ones) regardless of whether they have been explicitly shared with them. They can also Change Owner for any object.

Keep in mind the following

While Per-object access controls the visibility of the dashboard or saved query, the underlying data remains governed by Scope-Based Access Control (SBAC). A user must have the appropriate SBAC permissions to view the data available through an object.

#### Sharing icons

The following icons indicate the sharing status and origin of an object in management tables:

- : A Restricted object you created that is not shared with anyone else.
- : An object you created that is currently shared with other users, groups, or API keys.
- : An object created by another user that has been shared with you.
- : A Palo Alto Networks object provided out-of-the-box. These are Public, cannot be deleted, and ownership cannot be transferred.

#### How to configure access to objects?

Configuring access follows a top-down workflow:

1. Tenant-level settings: Establish the "rules of engagement" for the entire instance.
2. Role permissions: Enable specific components and define additional capabilities for those roles.
3. Per-object access: Manage visibility and access levels for specific dashboards and queries.
4. Scope-Based Access Control (SBAC): Ensure the user has the required permissions to view the underlying data available through the object.

#### Step 1: Configure tenant-level access settings

Administrators first establish the "rules of engagement" for all objects. These settings are located under Settings → Configurations → Access Management → Objects:

- Owners can Share objects they created: Allows the creator (Owner) of an object to share it with users, user groups, or API keys.
  - Editors can also Share objects with others: Allows users with Editor access to further share the object with additional principals (users, user groups, and API keys).
- Owners and editors can change the general access (default): Allows the object owner and any user with Editor access to modify the object's General access settings (Restricted or Public) using the drop-down menu in the object's sharing settings.

#### Step 2: Set role permissions

Once tenant-level policies are established, configure individual roles to allow users to interact with specific components:

1. Select Settings → Configurations → Access Management → Roles.
2. Right-click the relevant user role, and select Edit Role.
3. Under Components, expand each list, set the applicable component to one of the following:
  - **Disabled**: The component is hidden from the user's navigation menu. The user cannot access any objects associated with this component, even if they were previously shared with them.
  - **Enabled**: The component is visible in the user's navigation menu. The user can view Public objects and any Restricted objects shared with them.
4. Define additional capabilities.

If enabled, refine capabilities using the following checkboxes:



- Create [Object]: Allows the user to create new instances; the user is automatically designated as the Owner, which grants the inherent right to edit, delete, and manage sharing for that specific object.
- Edit Public [Object]: Allows the user to modify custom objects that have been set to Public General access, even if they are not the owner.

Once a component is enabled using role permissions, sharing is managed at the individual object level. Owners and authorized editors can share with other principals (users, user groups, or API keys) directly on the object.

#### Step 3. Configuring per-object access

For more information on managing visibility and access levels for specific dashboards and saved queries, see the following topics:

- Manage access to custom dashboards
- Manage access to saved queries

#### Step 4. Configure SBAC permissions

For more information on managing user scope so users have the permissions necessary to view the data available through the object, see Manage user scope.

How to change an object owner

To ensure continuity when personnel changes occur or a user leaves the organization, the ownership of an object (a dashboard or a saved query) can be changed.

- **Administrative privilege:** Only Account and Instance Administrators can change the owner of an object. Other users who are Owners and Editors cannot perform this action.
- **Change Owner:** Using the Change Owner action in the management table of the specific object, administrators can select a new user to take over full control. Once changed, the new user assumes all Owner-level rights, including the ability to edit, delete, and share with other principals (users, user groups, and API keys).

Access examples

Granular per-object access supports various organizational security requirements:

1. **Use only by SOC team:** A "flat" structure where all analysts can see all objects. This is the default setting for the tenant. By default, newly created custom objects, such as a specific investigation dashboard or a complex XQL saved query, are Restricted and visible only to the creator; the owner can then make them Public to allow the entire team to view or edit them based on their role permissions.
2. **Both SOC team and Internal threat:** Specific objects, such as sensitive dashboards and saved queries, are created by a member of the Internal Threat team and made accessible only to the Internal Threat user group. First, an administrator must enable the tenant-level access settings that allow users to share objects. Members of the Internal Threat team then create these objects and share them only with their peers or their specific user group. Members of the SOC team do not have access to these dashboards and saved queries, as they are not visible or accessible to any users who have not been explicitly granted access.
3. **Both SOC team and Cloud team:** Provides department isolation. Each team only accesses its own saved queries and dashboards; the SOC team cannot see Cloud team objects, and vice versa.

##### 2.3.3.4.1 | Manage access to custom dashboards

Abstract

Learn more about managing access to custom dashboards in Cortex Cloud.

The Dashboard Manager serves as the central repository for your visualizations. By using object-level access, you can ensure that custom (user-defined) dashboards, such as those used for sensitive executive reporting or specialized department views, are only accessible to authorized users and user groups. The permissions assigned to your role, combined with the ownership of specific objects, directly determine the content available to you; you can only access dashboards where you are the Owner, dashboards that have been explicitly shared with you (or your user group), or dashboards marked as Public.

#### **PREREQUISITE:**

- **Configure tenant-level settings:** An administrator must first establish the sharing framework under Settings → Configurations → Access Management → Objects.

The configuration of these settings defines the authorized sharing workflows for custom dashboards:

- **Enable "Owners can Share objects they created":** Grants owners the ability to share dashboards with specific users and user groups. In the Dashboard Manager, this enables the Share option.
- **Disable "Owners can Share objects they created":** Restricts owners to managing only General access (Public vs. Restricted). In the Dashboard Manager, this replaces the Share option with the Manage Access option.
- **Define Scope-Based Access Control (SBAC):** While object-level sharing grants access to the dashboard's layout and configuration, users must also have the appropriate SBAC permissions to view the actual data populated within the widgets. If a user has access to a shared dashboard but lacks the required data scope for the underlying datasets, the dashboard will load, but the widgets may appear empty or display an error.

For more information on these prerequisites, see Manage access to objects.

Understanding widget behavior



Because dashboards are composed of multiple widgets, it is important to understand how access is applied to these individual components:

- **Widgets are not objects:** Unlike dashboards, individual widgets are not treated as independent objects. They do not have their own "Share" dialog and cannot be shared independently. Within the Widget Library, a widget is set to either Restricted (visible only to the creator) or Public (visible to all with Widget Library access).
- **Inherited access:** Any user who has been granted access to a custom dashboard (as a Viewer or Editor) can see all the widgets contained within that dashboard, including those marked as Restricted. This means you may see a widget on a shared dashboard that you cannot see in the Widget Library even if you have access to it.
  - **Dashboard Editors:** Can edit the dashboard layout, but the widget is only available in their Widget Library for editing when the widget is Public.
  - **Dashboard Viewers:** Can't make any changes to dashboards or widgets that are Restricted.

How to configure access to custom dashboards

#### Step 1: Set role-level permissions

Role permissions define the functional capabilities for dashboards and the Widget Library, and determine what actions a user can take.

1. Select Settings → Configurations → Access Management → Roles.
2. Right-click the relevant user role, and select Edit Role.
3. Under Components, expand Dashboards & Reports, and locate Dashboards.
4. Configure access state:
  - Disabled: Users cannot navigate to Dashboards & Reports → Dashboard Manager or Dashboards & Reports → Widget Library. Dashboards cannot be shared with this role. If the user previously owned or had access to shared dashboards, they are no longer available.
  - Enabled: Allows dashboards to be accessed and managed according to defined sub-permissions. Grants access to the Widget Library as explained below in Manage the Widget Library.
5. If Enabled, assign specific capabilities to control the UI:
  - Create Dashboards: Enables the New Dashboard button on the Dashboard Manager page, allowing the user to create new custom dashboard objects. The user who performs this action becomes the Owner of the object and is granted the inherent right to edit, delete, and manage sharing for that specific object.
  - Edit Public Dashboards: Allows the user to modify custom dashboards set to Public, even if they are not the owner.
6. Click Save.

#### Step 2: Manage the widget library

The Widget Library is the central repository for predefined and custom widgets and is intended for browsing and selecting widgets to add to a dashboard. Access to and visibility within the Widget Library is determined by role-level permissions and your specific access level to the dashboards where those widgets reside:

- **Access to the Widget Library:** To access the Widget Library, your role must have the Create Dashboards or Edit Public Dashboards capability. Users who only have "View" permissions for dashboards cannot access the Widget Library.
- **Widget Library visibility:** Visibility within the Widget library depends on ownership and inherited dashboard and widget permissions:
  - **Public and personal widgets:** You can always see widgets you created (Restricted) and widgets marked as Public.
  - **Inherited access via dashboards:** If a Restricted widget was created by another user but is part of a dashboard shared with you, you won't see it in the Widget Library and it can't be edited (unless you are an administrator).

#### NOTE:

If you're designated as an Editor, you can always duplicate the widget and make your changes on the copy.

#### Step 3: Manage sharing for a custom dashboard

Once a custom dashboard exists in the Dashboard Manager, the Owner (or an authorized Editor) defines who can see or edit it.

1. Select Dashboards & Reports → Dashboard Manager.
2. Locate the custom dashboard that you want to share in the table.
3. Right-click the custom dashboard and select the available access option. The menu option you see depends on your tenant-level settings:
  - Share: Use this if your admin enabled sharing. It allows you to invite specific users/groups and change the General access (Public/Restricted).
  - Manage Access: Use this if sharing is disabled. It is a restricted view that only allows you to toggle the General access between Public and Restricted. You cannot invite specific individuals.
4. (If sharing is enabled) Search for the User or User Group, and assign the access level: Viewer (read-only) or Editor (can modify and share).



5. Set the General access state:

- Restricted: Private to the Owner and invited guests.
- Public: Visible to all users with the Dashboard component enabled in their role.

6. Click Save.

Sharing icons in the Dashboard Manager

The following icons help you identify the security access of your custom dashboards:

- A Restricted custom dashboard you created that is not shared with anyone else.
- A custom dashboard you created that is currently shared with other users or user groups.
- A custom dashboard created by another user that has been shared with you.
- A standard system dashboard provided by Palo Alto Networks. These are always Public and cannot be deleted or edited, and their ownership cannot be transferred. Yes, you can Duplicate a system dashboard to create a custom version that you can then modify and share.

Change owner of a dashboard

To ensure continuity when personnel changes occur or to hand off management of a resource, only administrators can change the ownership of a custom dashboard.

#### **NOTE:**

Only Account Administrators and Instance Administrators have the authority to change the owner of an object.

1. Select Dashboards & Reports â Dashboard Manager.
2. Right-click the custom dashboard in the table and select Change owner.
3. Select the new owner from the list of users, and click Change.

#### 2.3.3.4.2 | Manage access to saved queries

Abstract

Learn more about managing access to saved queries in Cortex Cloud.

Review the following:

- Manage access to objects

The Query Library serves as the central repository for your team's investigation logic. By using object-level access, you can ensure that specific Cortex Query Language (XQL) queries, such as those used for sensitive internal investigations or executive reporting, are only accessible to authorized users, user groups, and API keys.

#### **PREREQUISITE:**

**Configure tenant-level settings:** An administrator must first establish the sharing framework under Settings â Configurations â Access Management â Objects.

The configuration of these settings defines the authorized sharing workflows for saved queries in the Query Library, including the options that appear to users when clicking the three dot, vertical ellipsis (â ⑧) for a query in the Query Library:

- **Enable "Owners can Share objects they created":** Grants owners the ability to share saved queries with specific users, user groups, and API keys to the query's access list. In the Query Library, this enables the Share option.
- **Disable "Owners can Share objects they created":** Restricts owners to managing only General access (Public vs. Restricted). In the Query Library, this replaces the Share option with the Manage Access option.

For more information on these tenant-level configurations, see [Manage access to objects](#).

How access impacts the Query Builder

The permissions assigned to your role, combined with the ownership of specific objects, directly change the tools available to you while working in the Query Builder:

- **Restricted versus Public visibility:** Your Query Library view is personalized. You will only see queries where you are the Owner, queries that have been explicitly shared with you (or your user group or API key), or queries marked as Public.
- **Context-sensitive functionality:** The permissions assigned to your role, combined with the ownership of specific objects, directly change the tools available to you while working in the Query Builder and the Query Library. UI elements like the Save as menu or the Share action only appear if you have the required functional capabilities.



## How to configure access to saved queries

Setting up access involves a two-part process: enabling the user interface (UI) elements in the role settings, and then defining the audience for individual saved query objects.

### Step 1: Define role capabilities

Role-level permissions act as the "master switch" for Query Builder functionality and determine what actions a user can take.

1. Select Settings → Configurations → Access Management → Roles.

2. Right-click the relevant user role, and select Edit Role.

3. Under Components, expand Investigation & Response.

4. Ensure Query Library is set to Enabled.

5. Define functional capabilities to control the UI:

- Create Queries: Selecting this enables the Save as drop-down menu in the Query Builder. This allows users to select Save as → Query to Library or Save as → Widget to Library. The user who performs this action becomes the Owner of the object and is granted the inherent right to edit, delete, and manage sharing for that specific object..
- Edit Public Queries: This allows a user to modify queries marked as Public by others.

#### NOTE:

If the role of a user is set to Edit Public Queries but not Create Queries, they can update existing public queries, but the Save as drop-down menu will be hidden, preventing them from creating new Query Library entries.

### Step 2: Manage sharing for a specific query

Once a query exists in the Query Library, the Owner (or an authorized Editor) can define who has permission to view (and run) or edit it.

1. Select Investigation & Response → Search → Query Builder → XQL.

2. Under the Query Library tab, locate the query that you want to share in the table.

3. Click the three dot, vertical ellipsis (⋮) and select the available action:

- Share: This option appears when Owners can Share objects they created is enabled in tenant-level settings. It allows you to manage both General access and specific principals (users, user groups, and API keys).
- Manage Access: This option appears when Owners can Share objects they created is disabled. It only allows you to change the General access state.

4. (If sharing is enabled) To share with specific entities (for Restricted queries):

- Search for the User, User Group, or API Key.
- Assign the access level: Viewer (can run/view) or Editor (can modify and, if permitted by tenant-level settings, share).

5. Set the General access drop-down menu (if authorized by tenant-level settings):

- Restricted: The query is private. It is only visible to the Owner and the specific principals added to the list.
- Public: The query is visible to every user who has the Query Library enabled in their role.

#### NOTE:

When the tenant-level setting Owners and editors can change the general access is unselected, the drop-down is disabled and only an administrator can configure this option.

6. Click Save.

### Sharing icons in the Query Library

The following icons in the Query Library table help you identify the security access of your queries:

- A Restricted query you created that is not shared with anyone else.
- A query you created that is currently shared with other users, user groups, or API keys.
- A query created by another user that has been shared with you.
- A standard system query provided by Palo Alto Networks. These are always Public and can't be deleted, or have their ownership transferred.

## 2.3.4 | Configure the Cortex Agentic Assistant



## Abstract

Create and manage agents and actions in the Agents Hub and configure access to the Cortex Agentic Assistant.

Create and manage agents and actions in the Agents Hub, configure access to the Cortex Agentic Assistant to create an AI agent workforce.

### 2.3.4.1 | Agentic Assistant components and concepts

#### Abstract

Learn about the key components and concepts, such as agents and actions in the Cortex Agentic Assistant

The Cortex Agentic Assistant uses the following components and concepts:

Name	Description
Actions	Actions wrap diverse capabilities (such as playbooks, scripts, and commands) to make them accessible and executable by an agent. You can use out-of-the-box system actions or register new actions.
Agent	<p>An agent is a virtual persona that creates and executes domain-specific plans, at your request, to assist in your day-to-day SOC operations. An agent has roles and permissions that provide guardrails. Each agent is assigned a collection of actions that it can use as part of plans.</p> <p>The agent chooses the most relevant actions to fulfill a user's request. Agents process user requests, create plans, and orchestrate actions based on their goals and permissions (RBAC and SBAC).</p> <p>You can use the following types of agents:</p> <ul style="list-style-type: none"><li>• System agents that are provided by Cortex Cloud for specific use cases.</li><li>• Custom agents that users have created.</li></ul> <p>Some agents provide relevant chat conversation starters under the chat prompt. For examples of conversation starters, see Agentic Assistant use cases.</p> <p><b>NOTE:</b></p> <p>Agents are bound by the same rules and robust permissions as a human user. In addition, you can mark actions that make real-world changes in production systems as sensitive, requiring a quick manual review and confirmation, ensuring peace of mind before critical system changes are made.</p>
Plan	A sequence of actions that run in parallel or sequentially to satisfy a user request. The agent dynamically chooses relevant actions to resolve the prompt.
Conversation	A sequence of user requests that maintains context across interactions.
Request	A user request from the agent with an end goal, triggering a plan.

### 2.3.4.2 | Agents Hub

#### Abstract

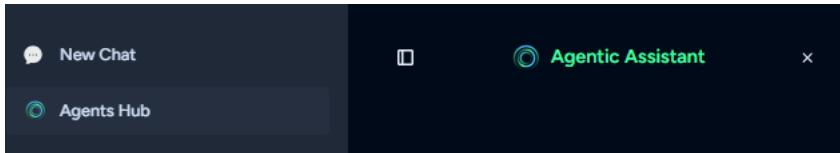
Learn about personal and system agents in the Agents Hub

In Cortex Cloud, you can interact with agents in the Agentic Assistant chat to automate case and issue investigation and response. Agents create and execute plans, which are sequences of actions (such as playbooks, scripts, and commands) designed to fulfill your requests.



Actions and agents are managed in the Agents Hub. To open the Agents Hub, click on the agent chat icon in the upper right hand corner, click the side panel icon to expand the menu if needed, and then click the Agents Hub menu item.





#### NOTE:

To manage agents in the Agents Hub, you must have the proper permissions. For more information, see [Agentic Assistant role-based access control](#).

A screenshot of the Agents Hub interface. The title 'Agents Hub' is at the top. Below it, there are two tabs: 'Agents' (which is selected) and 'Actions'. A search bar with placeholder 'Search in All Agents' and a 'Build a New Agent' button are also present. The main area displays four agent cards: 'Threat Intel' (By Cortex), 'Network Security' (By Cortex), 'IT' (By Cortex), and 'Endpoint Investigation' (By Cortex). Each card includes a brief description and a 'Actions' count.

Agent Type	Provider	Description	Actions
Threat Intel	By Cortex	Gathers fresh threat data, enriches indicators and vulnerabilities, links them to past or current incidents, and...	22 Actions
Network Security	By Cortex	Manages Palo Alto Networks Panorama and Firewalls, as well as third-party network security products. Streamlines work...	26 Actions
IT	By Cortex	Automates identity lifecycle enforcement, real-time containment on endpoints and networks, vulnerability and...	22 Actions
Endpoint Investigation	By Cortex	Unifies host-level containment, forensic collection, and remediation across all major EDR/XDR platforms while...	29 Actions

The Agents Hub includes the following components:

- **Actions**

Actions wrap diverse content items (such as playbooks, scripts, AI prompts, and commands) to make them accessible and executable by an agent. Cortex Cloud provides system actions, and you can also create your own actions. Custom actions can be created from scripts, commands, and AI prompts.

You can register new actions through the Agents Hub or from the Scripts or AI Prompts page. Actions can include functionality such as sending emails, extracting data, enriching information, or opening support cases. Multiple actions can be created from a single script, command, or AI prompt, if needed. An action can be added to multiple agents.

- **Agents**

An agent is a virtual persona that creates and executes domain-specific plans, at your request, to assist in your day-to-day SOC operations. An agent has roles and permissions that provide guardrails. Each agent is assigned a collection of actions that it can use as part of plans.

The agent chooses the most relevant actions to fulfill a user's request. Agents process user requests, create plans, and orchestrate actions based on the user's goals and permissions (RBAC and SBAC).

Cortex Cloud provides system agents, and you can also create custom agents. In the Agentic Assistant chat, you can select any system agent, any agent you created, or any public agent.

- From the Agents tab of the Agents Hub, you can hover over any agent card to see the View option. Click View to see all the actions assigned to the agent and their status.

In the Agents Hub, you can do the following:



- Register scripts, commands, and AI prompts as custom actions. After a script, command, or AI prompt is registered as a custom action, it can be assigned to agents and used in plans. For more information, see [Manage actions](#).
- View system actions and edit existing custom actions.
- Build agents and assign actions to agents.
- Enable and disable system agents. System agents have access to system actions that are assigned to the agent.
- Start a chat with any agent, by clicking the more options icon on the agent card and clicking Start chat.

#### 2.3.4.2.1 | [Manage actions](#)

##### Abstract

Manage actions that can be used by agents.

Actions wrap diverse capabilities (such as playbooks, scripts, AI prompts, and commands) to make them accessible and executable by an agent. You can use out-of-the-box system actions or register new actions.

##### **NOTE:**

To manage actions in the Agents Hub, you must have the correct permissions. For more information, see [Agentic Assistant role-based access control](#).

There are two types of actions in the Agents Hub:

- **System actions:** Cortex Cloud contains more than 50 out-of-the-box system actions that can be disabled or enabled, but cannot be edited or deleted. To find and install additional content packs that include actions, go to Marketplace and select Content pack includes and Actions.
- **Custom actions:** Users can register existing or new scripts, commands, and AI prompts as actions. Custom actions can be edited, deleted, enabled, or disabled.

Any action marked as sensitive to require user approval requires explicit user approval before execution. This is particularly crucial for operations that might alter system reality or affect an organization's budget, such as revoking user access. System actions are marked sensitive if they affect system reality. When creating custom actions, you decide which actions should be marked as sensitive for your organization.

##### Manage existing actions

From the Actions tab of the Agents Hub, click  for an action to edit, delete, or disable an existing custom action. System actions can only be enabled or disabled.

##### Search, filter, and sort actions

You can use the dropdown filter to search all actions, custom actions, system actions, enabled actions, or disabled actions.

You can sort actions by most used, creation time, or update time.

#### 2.3.4.2.1 | [Register actions](#)

##### Abstract

Register custom actions that can be used by agents.

You can register scripts, commands, and AI prompts as actions in the Agents Hub. After a script, command, or AI prompt is registered as an action, it can be added to one or more agents. The agents can then execute the action as part of plans.

##### **NOTE:**

To register actions, ensure you have the correct permissions. For more information, see [Agentic Assistant role-based access control](#).

When you register an action, you provide a description, goal, and, optionally, a few-shot examples. This information helps agents understand how the action should be used.

When registering or editing an action, you can choose which specific inputs and outputs are visible to the LLM. For example, a script might have two inputs and five outputs, but for this action, only one input and two outputs are required, and only those are included in the action. This helps to create more focused actions and reduces unnecessary complexity.

##### **IMPORTANT:**

A single content item can be registered as different actions, with each action using different inputs and outputs from the same script. Only register the same script, command, or AI prompt as a new action if it is required for your use case, as providing an agent with many actions with overlapping abilities can reduce the ability of the agent to choose the most appropriate action.

While you can create multiple actions from a single content item, each action must have a different name.

If you try to register a script, command, or AI prompt that is already registered, you are presented with a list of the actions already using it, and you can review and decide if any of them are relevant for your current use case. If not, you can register the script, command, or AI prompt again as a different action.



## How to register an action

1. Do one of the following:
  - Click the Agentic Assistant icon in the upper right hand corner and expand the side panel  to access the Agents Hub menu item. From the Actions tab of the Agents Hub, click Register new action.
  - Within the script creation or editing screen, click  when viewing or editing a script and select Register as action.
  - Within the AI Prompts library, select a prompt and click the more options icon to Register as action.
2. If you clicked Register as action from the Scripts or AI Prompts page, the name is prepopulated in the Content chosen field. If you clicked Register action from the Agents Hub, select script, command, or AI prompt for the Type of content and select the content you want to register.
3. Enter an action Name, a short description of what the action does. Example: `Extract_email`.
4. Describe the Goal of the action.
5. (Optional) By default, Mark action as sensitive to require user approval is selected, and the agent prompts the user to approve before executing the action. If you do not want the action marked as sensitive, clear the checkbox.
6. (Optional) Provide Few-shot examples to help the agent understand the context and the appropriate situations to invoke a specific action.
7. Click Next.
8. Choose your Action Parameters:

**NOTE:**  
Mandatory arguments cannot be deselected.

  - a. Choose which arguments and inputs to include in the action. If a content item contains descriptions of the inputs, the descriptions are prepopulated. If not, you can provide short descriptions. The descriptions help the agent understand the purpose of each input.
  - b. (Optional) Enter a default value for each input. The default value is used when the user does not specify the input.
  - c. Choose which script outputs to include in the action. If the content item contains descriptions of the outputs, the descriptions are prepopulated. If not, you can provide short descriptions. The descriptions help the agent understand the purpose of each output.
9. Save changes.

### 2.3.4.2.3 | Manage agents

#### Abstract

Edit, disable, or delete existing agents.

Agents create and execute step-by-step plans dynamically, choosing relevant actions based on a user's request. Each agent has a model, a user context, a conversation context, and a set of actions that it can perform. Users engage with agents through conversations in the chat interface.

Permissions for the Agentic Assistant and the Agents Hub can be found under CORTEX AGENTIC ASSISTANT in the role permissions when creating or edit a role. For more information, see Agentic Assistant role-based access control

There are two types of agents in the Cortex Agentic Assistant:

- **Custom agents:** Each user can create one or more agents that have the same or fewer permissions as the user, ensuring agents operate with the least necessary privileges required. These permissions automatically update if the user's roles or permissions change. When users create custom agents, they can create a private agent only they can access, or a public agent all users can access.
- **System agents:** System agents come out-of-the-box and are not linked to a specific user; instead, they possess their own defined roles and permissions. A system agent may include actions that the user does not have permission to execute. All users have access to all system agents, but plan execution is limited by the permissions of the individual user.

#### Agent management

You can edit, delete, disable, or enable custom agents by clicking the more options  icon for the agent.

You can edit, enable, or disable system agents by clicking the more options  for the agent. The edit option for system agents is limited to adding specific instructions for the agent such as tone, style, format, and priorities.

You can click on an Agent to view all actions assigned to the agent. There are three possible statuses for actions assigned to an agent:



- **Enabled** (green circle with a check mark): The action is enabled and available for the agent to use.
- **Disabled** (grey circle with an x): The action has been disabled and is not available for the agent to use.
- **Unavailable content** (grey circle with a horizontal line): The content the action is based on is not available. To use the action, the content item must be installed and configured.

**NOTE:**

In some cases, an agent may include actions with content items that are not relevant for all licenses. If that occurs, the grey circle appears, but you are not able to install the related content.

Search, filter, and sort existing agents

You can use the dropdown filter to search all agents, custom agents, enabled agents, or disabled agents.

You can sort agents by most used, creation time, or update time.

2.3.4.2.4 | [Build agents](#)

Abstract

Build new agents.

You can build custom agents in Cortex Cloud to execute plans and assist in investigations. Custom agents have the same or fewer permissions as the user who creates them. For example, you might want to create an agent with all of your permissions to use for certain investigations, but also create a read-only agent that provides you with information, but does not execute actions on real-world systems. You can create custom agents that are private or that are shared for all users.

When you build an agent, it should contain all actions that you require for your workflow. Agents are self-contained and cannot communicate with other agents or access actions that are not assigned to the agent.

**NOTE:**

To build agents in the Agents Hub, you must have view/edit permissions. For more information, see [Agentic Assistant role-based access control](#).



1. Click on the agent chat icon in the upper right hand corner, click the side panel icon to expand the menu if needed, and then click the Agents Hub menu item.
2. From the Agents tab of the Agents Hub, click Create agent.
3. Complete the following agent detail fields:

Field	Description	Required
Agent Name	A short description name for the agent. Each agent must have a different name.	Yes
Color	The color for the icon that appears in the agent list.	No
Description	A description of the agent's purpose or area.	Yes



Field	Description	Required
Specific Instructions	<p>Provide the agent with detailed customized instructions. You can include a wide range of directives, from describing the agent's role and preferred terminology to step-by-step processes and structure of the output.</p> <ul style="list-style-type: none"> <li><b>Role:</b> What the agent is supposed to be or act as. Defines its identity and primary function. Example A: SOC tier 1 analyst. As a tier 1 analyst you are responsible for triaging alerts and concluding if an alert is a true or false positive.</li> <li><b>Instructions:</b> The specific rules and behavioral guidelines that tell the agent how to operate and respond. Example: Follow the NIST framework, provide clear and concise recommendations, use critical thinking when conducting analysis.</li> <li><b>Structure:</b> How the agent should format and organize its responses. Examples of possible formats: JSON, Markdown, Array, enum.</li> </ul>	No
Agent access	Choose whether to make the agent a Public Agent. Public agents can be accessed by all users with View/Edit permissions to Interact with Agents. By default, custom agents are only available for the users who created them.	No
Conversation starters	Include up to four prompts that appear under the prompt bar when the user interacts with the agent. Conversation starters help users understand what the agent can do and how to initiate a request.	No

4. Click Next to proceed to the Access Control page.

5. Define which roles and actions the agent can access. To save an agent, there must be at least one role or action selected.

**NOTE:**

If you clear the checkbox for a role, all actions associated with that role are also cleared. The exception is if another role is also selected, which is associated with the same actions.

If you clear the checkbox for an action, all roles associated with that action are cleared. For example, if you select the Investigator role, and Send Mail and Tavily Extract are both actions associated with that role, clearing the check box for Investigator also clears the check box for Send Mail and Tavily Extract. If you then reselect the Send Mail action, the Investigator role is not automatically selected.

Not all actions are associated with a role.

For an agent to be able to run XQL queries, you must add the Cortex - Run XQL Query action. This action is included by default for all system agents.

6. If needed, register one or more new actions by clicking New Action and following the steps in Manage actions.



## 7. Save Agent.

### 2.3.4.2.5 | Expand agent capabilities with MCP integrations

#### Abstract

Learn how Agentic agents can leverage tools on third-party MCP servers.

Cortex Agentic Assistant supports native interaction with external environments via the Model Context Protocol (MCP). Agentic Assistant agents can use tools from third-party MCP servers to retrieve data and perform tasks in external systems. For example, an agent can open a Jira issue or check GitHub to see if security scans in a workflow are being bypassed..

The Cortex Agentic Assistant connects to external MCP servers using streamable HTTP and supports both OAuth-based and Authless servers. The MCP server must be accessible via a URL. To communicate with third-party MCP servers, you install the relevant content pack from Marketplace and configure an integration instance. The integration connects to the third-party MCP server to discover available tools and automatically generate agentic actions.

#### MCP integrations

To find MCP content packs, filter for MCP under Types in Marketplace. Examples of MCP content packs include Cloudflare MCP, GitHub MCP, and Atlassian Cloud MCP. You can also use the Generic MCP content pack to connect to MCP servers that do not have their own specific content pack. Each MCP integration includes instructions for providing the required parameters, such as the URL and authentication details.

You can create multiple integration instances for each MCP integration. For example, you might configure one instance of the GitHubMCP integration to connect to a environment with read tools and another instance to connect to an environment with both read and write tools. In addition, the GenericMCP integration can be used to connect to multiple MCP servers, each with a separate integration instance.

When you Test the integration instance, Cortex Cloud verifies server connectivity.

#### NOTE:

If you are using OAuth-based authentication, the Test button returns an error containing the command to run in the playground in order to test the connection.

All configured MCP integration instances can be viewed in the Settings → Data Sources & Integrations page. You can view each integration instance and verify the status of the connection, Test the connection, enable or disable the integration instance, and view the last discovery timestamp.

#### MCP tool actions

The integration instance checks hourly for new or changed tools exposed by the third-party MCP server. The same checks are also performed every time an integration instance is saved. All discovered tools are automatically registered as AI actions, with the type MCP Tool. Actions are created once per MCP integration instance. If you have multiple integration instances for the same MCP server, multiple actions are created for the same tools. The server name, the tool name, and the name of the integration instance are all included in the name of the action. Actions created through tool discovery are system actions. The actions cannot be edited, but you can enable and disable them and also select or clear the checkbox to mark the action as a sensitive action that requires manual approval. By default, all actions registered from MCP servers are marked as sensitive.

#### NOTE:

- If an MCP tool is removed from the MCP server, the action will be unavailable due to missing content. If the tool is restored on the MCP server, the action is automatically reenabled.

#### Agents and permissions

To use MCP tool actions, they must be added to custom agents in the Agents Hub. By default, all users with access to the custom agent can use all of the available tools. To restrict access to MCP tools, go to Settings → Configurations → Data Collection → Integration Permissions. You can restrict access for MCP integration instance commands to one or more roles. If you restrict access, only users in the permitted roles can use these actions.

### 2.3.4.3 | Agentic Assistant role-based access control

#### Abstract

Configure permissions to access Cortex Agentic Assistant features.

Instance and Account admins have full control over the permissions and access that users have to the Cortex Agentic Assistant. Cortex Cloud uses role-based access control (RBAC) to manage access to the chat, as well as access to view, create, edit, delete, disable, and enable Agents and Actions in the Agents Hub.

By default, Instance and Account admins have full view/edit permissions enabled. When editing or creating other roles, in the Cortex Agentic Assistant → Agents section, you can select the following:



Permission	Description
View/Edit	<p>When selected (and nothing else is checked in this section), the user role can only see actions and public agents in the Agents Hub, but cannot interact with agents.</p> <p>You can also select the following permissions:</p> <ul style="list-style-type: none"> <li>Interact with agents: Users can trigger Agents in the Cortex Agentic Assistant. Users can access their own agents, public agents and system agents.</li> <li>Manage actions: Users can view, create, update, and delete actions.</li> <li>Manage agents: Users can view, create, update, and delete their own custom agents.</li> <li>Agents admin: Users can view, create, update, and delete all actions and agents. Users can enable or disable system actions and agents.</li> </ul>
View	N/A
None	The user role does not see any agents and can't use the chat. The Agents Hub is not visible to the user. Cortex Agentic Assistant is only available for navigation and insights.

### 2.3.5 | XQL query management

#### Abstract

Administrators can set controls on running XQL queries.

You can find Query Management options under Settings → Configurations → General → Query Management. These options enable administrators to set controls on running queries.

#### Set query limits

##### **PREREQUISITE:**

Setting query limits requires View/Edit permissions for Configurations → Query Management.

Administrators can set query limits that control user-generated XQL queries within a tenant. Setting query limits helps to prevent resource strain and optimize tenant performance. You can control the following query settings:



- Concurrent queries per user

Prevent system overload by setting a maximum number of concurrent queries that a user can run.

The concurrent query limit is applied per user.

If a user is running a high number of queries and is approaching the concurrent query limit, a system message warns that a high query load is impacting their performance. If a user exceeds the defined limit of concurrent queries, new queries are blocked until the number of active queries drops below the limit.

The user can view all of their In Progress queries from the Query Center, and cancel active queries to avoid being blocked and improve query performance. For more information, see [Edit and run queries in Query Center](#).

If a user is blocked, other users of the tenant can continue to run queries. By default, query limits apply to all users of the tenant, but you can exclude specific roles and groups from these limits.

Queries that are included in the concurrent queries calculation include:

- Cortex Query Language (XQL) investigation queries, including cold and hot storage, XDM templates, XDR templates, free text search, and queries from the query library.
- Scheduled queries and scheduled reports.

**NOTE:**

A scheduled query or report is run on behalf of the user that originally created it, even if it is edited and run by another user.

- XQL widget queries in dashboards and reports
- XQL public API queries (cold and hot storage)
- BIOC test queries.
- Correlation rule test queries.
- XQL queries run from playbook tasks.

**NOTE:**

- Queries run by correlation rules are not restricted by the query limit.
- Very short queries do not count towards concurrent queries.

- Query duration timeout

Prevent long running queries by setting a timeout duration for queries to automatically stop long running queries and reserve tenant resources.

Only integer values are supported for this field. In addition, the query timeout is an approximate value.

**NOTE:**

To ensure optimal system performance, all queries (user-generated and otherwise) adhere to a default timeout limit of 60 minutes that is defined by Palo Alto that takes priority over the administrator defined value. Therefore, regardless of the value specified in this field, queries will be stopped after 60 minutes.

You can override the default timeout limit by including the `config max_runtime_minutes` stage in your query to increase the query timeout value, up-to the administrator defined value. For more information about this stage, see [max\\_runtime\\_minutes](#).

How to set a query limit

1. Go to Settings → Configurations → General → Query Management.

2. Under Query Limits select Enabled.

3. Under Concurrent Queries Per User, specify the maximum number of queries a user is allowed to run concurrently. Queries exceeding this limit will be blocked.

Important considerations:

- A value of 0 will prevent all queries from running.
- Setting a very low or very high limit could adversely affect overall query execution speed and system resources.

4. Under Query Timeout specify the maximum duration (in minutes) that any query can run.

By default, the query duration timeout is set to 60 minutes for all queries regardless of the value specified in this field. For more information, see the explanation above regarding [Query timeout duration](#).

5. Under Excluded User Groups or Roles, choose specific user groups or roles that should be excluded from the query limits.

6. Click Save.



7. Changes to the query limit settings are recorded in the Management Audit Logs.

#### Restrict query visibility

Administrators can restrict non-admin users and API keys to viewing and managing only their own query history, which enhances tenant privacy and reduces operational noise. By limiting access to users' own search activities, you can secure sensitive investigations and ensure that API usage adheres to strict visibility controls.

The following areas in the Query Builder are affected when you restrict query visibility:

- Query History tab: Users and API keys see an access only the queries they initiated. Queries which are run implicitly on their behalf, such as background reports, BIOCs, or dashboards, are hidden from this view to reduce noise and maintain focus.
- Active Queries tab: Users and API keys view and manage any query they initiated, regardless of the source, including dashboards and widgets, allowing them to cancel operations they triggered.
- Scheduled Queries tab: Users see only the queries they personally scheduled.

#### Query restriction use cases

Restricting the access of users and APIs to only their own queries addresses specific operational and security needs:

- Reduce operational noise: Restricting visibility to only user-initiated Investigation or Simple Search sources in Query History makes the view more relevant to the analyst's immediate workflow.
- Prevent insider threat visibility: When investigating another user within the same tenant, restricting visibility prevents the individual being examined from seeing queries about themselves. Enabling this restriction protects the integrity of internal investigations.
- Secure API keys: Restricting API key access to their own queries prevents users from retrieving results using execution ID guessing. This aligns API privacy standards with the User Interface.

#### NOTE:

Query visibility is subject to Role-Based Access Control (RBAC); users can't see queries for datasets they do not have permission to access.

How to enable query visibility restrictions

1. Go to Settings → Configurations → General → Query Management.
2. Under Enforce query privacy for non-admins,
  - Enable: Non-admin users can only see and manage their own query activity.
  - Disable: Non-admin users can view all queries in the tenant.
3. Click Save.

Changes to the query visibility settings are recorded in the Management Audit Logs.

### 2.3.6 | Customize cases and issues

#### 2.3.6.1 | Customize cases and issues

Abstract

Customize your cases and issues for specific requirements.

While cases and issues are configured to work OOTB, users with specific requirements can customize them for specific needs or scenarios.

##### 2.3.6.1.1 | Set up case scoring

Abstract

Set up case scoring and define scoring rules.

To set up case scoring you need to define scoring rules.

#### Enable and define scoring rules

1. Select Cases & Issues → Case Configuration → Case Scoring → Scoring Rules and enable User Scoring Rules.

The Scoring Rules table displays the user-defined rules and sub-rules.

2. Click Add Scoring Rule.

3. In the Create New Scoring Rule dialog, define the rule criteria:



1. Under Rule Name, enter a unique name for your rule.
2. Under Score, define the score that Cortex Cloud should apply to issues that matching the rule criteria.
3. Under Base Rule, select whether to create a top-level rule (labeled Root) or a sub-rule (labeled *Rule Name (ID:#)*). By default, rules are defined at the root level.
4. Select or deselect Apply score only to first issue of case.

By selecting this option you choose to apply the score only to the first issue that matches the defined rule. Subsequent issues of the same case will not receive a score from this rule. By default, a score is applied only to the first issue that matches the defined rule and sub-rule.

5. In the issue table, use the filters to define the attributes you want to include in the rule match criteria. For example, you can select issues with High severity, issues by category, or issues associated with certain assets or asset providers.

**TIP:**

Right-click an issue field to add it as match criteria.

#### Example 12. Example

With this rule, Cortex Cloud assigns a score of 30 to any XDR BIOC issues with a severity level of Critical:

- Score = 30
- Base Rule = Root
- Filters:

```
Issue Source=XDR BIOC AND Severity=Critical
```

#### 4. Click Create.

You are automatically redirected to the Scoring Rules table.

#### 5. In the Scoring Rules table, click Save to save your scoring rule.

**NOTE:**

For scoped users, a small lock icon indicates that you don't have permissions to edit a rule.

[Revise existing scoring rules](#)

In the Scoring Rules table, take the following actions to review your rules and sub-rules:

- Use the arrows to rearrange rule priorities. Make sure to click Save after any changes.
- Select one or more rules and right-click to see the available actions.

[Scope-Based Access Control considerations](#)

Case Scoring supports Scope-Based Access Control (SBAC). If you're a scoped user, a small lock icon indicates that you don't have permissions to edit a rule. The following parameters are considered when editing a scoring rule:

- If Scope-Based Access Control (SBAC) is enabled and Endpoint Scoping Mode is set to restrictive mode, you can edit a rule if you are scoped to all tags in the rule.
- If Scope-Based Access Control (SBAC) is enabled and Endpoint Scoping Mode is set to permissive mode, you can edit a rule if you are scoped to at least one tag listed in the rule.
- To change the order of a rule, you must have permissions to the other rules of which you want to change the order.
- If a rule was added when set to restrictive mode, and then changed to permissive (or vice versa), you will only have view permissions.

[2.3.6.1.2 | Create a starring configuration](#)

You can proactively star issues and the cases to which they are linked by creating a starring configuration:

1. Select Cases & Issues â Case Configuration â Starred Issues.
2. Select Add Starring Configuration.
3. Under Configuration Name, enter a name to identify your starring configuration.
4. (Optional) Under Comment, enter a descriptive comment.



- In the issue table, use the filters to define the issue attributes you want to include in the match criteria. For example, you can select issues with High severity, issues by category, or issues associated with certain assets or asset providers.

**TIP:**

Right-click an issue field to add it as match criteria.

- Click Create.

Scope-Based Access Control considerations

Case starring supports Scope-Based Access Control (SBAC). The following parameters are considered when editing a starring configuration:

- If Scope-Based Access Control (SBAC) is enabled and the Endpoint Scoping Mode is set to restrictive mode, you can edit a configuration if you are scoped to all tags in the configuration.
- If Scope-Based Access Control (SBAC) is enabled and the Endpoint Scoping Mode is set to permissive mode, you can edit a configuration if you are scoped to at least one tag listed in the configuration.
- If a policy was added when set to restrictive mode, and then changed to permissive (or vice versa), you will only have view permissions.

2.3.6.1.3 | [Create custom case statuses and resolution reasons](#)

Abstract

You can create custom case status and resolutions that are tailored to your workflow.

**NOTE:**

Before you create a custom status, please review the built-in options. For more information, see [Resolution reasons for cases and issues](#).

We recommend using the built-in statuses and resolution reasons where possible. Custom statuses and resolution reasons might not be supported by all content, and status syncing can take time.

In addition, custom statuses affect Cortex Cloud's ability to learn, correctly identify, and score future cases.

You can create custom cases statuses and custom resolution reasons that are tailored to your workflow. Custom case statuses and resolution reasons apply to case and issue statuses, and can also be used in playbooks.

Adding custom ,case statuses and resolution reasons requires a View/Edit RBAC permission for Case Properties (under Configurations → Object Setup).

**NOTE:**

After creation, custom statuses and resolution reasons cannot be deleted or modified.

How to create custom case statuses

- Go to Configurations → Object Setup → Cases → Properties.

The existing statuses and resolution types are listed.

- In the Add another status field, type a new status and click Save.
- Click Edit to rearrange the order of the statuses. This order is presented when you set a status or select a resolution type.

2.3.6.1.4 | [Create a sync profile](#)

Abstract

You can set up inbound and outbound sync profiles to define field mapping between Cortex Cloud issues and an external application.

Sync profiles provide a blueprint for how information is exchanged between Cortex Cloud issues and external applications, by defining field mapping. This ensures that relevant data, such as Status or Description, is accurately transferred and maintains consistency, even if the systems use different terminology.

When you link an issue with an external application (such as Jira), or set up an automation, you can select the sync profile you want to use. Cortex Cloud provides default outbound and inbound sync profiles, or you can create custom sync profiles as described in the following procedure.

How to create a sync profile

- Go to Settings → Configurations → Object Setup → Issues → Sync Profiles.
- Click New Profile.
- Type a profile name and description.
- Under Integration, select the external application with which you want to map fields, such as Jira V3 or ServiceNow V2.



5. Under Sync Direction, select Inbound or Outbound.

If you select Inbound, you will define field mapping from the external application to Cortex Cloud. If you select Outbound, you will define field mapping from Cortex Cloud to the external application.

**NOTE:**

If an issue is using bi-directional syncing, you need to provide both an Inbound and an outbound sync profile.

6. Under Field Mapping, select a field to map and select the corresponding field. For example, Jira: Priority, Cortex: Severity.

7. Define one or more values for each field that you want to map.

**NOTE:**

- Blank fields are skipped.
- You must define exact values.
- Custom status values are not currently supported.
- Support is currently limited to a specific set of fields.

8. Click Save.

Example 13.

In this example, the sync profile specifies Inbound mapping from Jira v3 fields to Cortex fields.

New Sync Profile

* Sync Template Name <i>Jira priority and status map</i>	Description <i>Inbound Jira priority and status fields</i>												
* Integration <i>Jira V3</i>	* Sync Direction <i>Inbound</i>												
<b>Field Mapping</b> For accurate syncing, match your ticketing system fields to Cortex fields. Blank fields are ignored; map at least one value. Values must match exactly to enable syncing.													
<table border="1"><thead><tr><th>Jira V3 Fields</th><th>Cortex Fields</th></tr></thead><tbody><tr><td>* Priority</td><td>→ * Severity</td></tr><tr><td>Highest   x</td><td>→ Critical</td></tr><tr><td>High   x</td><td>→ High</td></tr><tr><td>Medium   x</td><td>→ Medium</td></tr><tr><td>Low   x</td><td>→ Low</td></tr></tbody></table>		Jira V3 Fields	Cortex Fields	* Priority	→ * Severity	Highest   x	→ Critical	High   x	→ High	Medium   x	→ Medium	Low   x	→ Low
Jira V3 Fields	Cortex Fields												
* Priority	→ * Severity												
Highest   x	→ Critical												
High   x	→ High												
Medium   x	→ Medium												
Low   x	→ Low												
<table border="1"><thead><tr><th>Status</th><th>→</th><th>Status</th></tr></thead><tbody><tr><td>To Do   x</td><td>→</td><td>New</td></tr><tr><td>In Progress   x</td><td>→</td><td>In Progress</td></tr><tr><td>Done   x</td><td>→</td><td>Resolved</td></tr></tbody></table>		Status	→	Status	To Do   x	→	New	In Progress   x	→	In Progress	Done   x	→	Resolved
Status	→	Status											
To Do   x	→	New											
In Progress   x	→	In Progress											
Done   x	→	Resolved											
<a href="#">+ Add Mapping</a>													

### 2.3.7 | Dashboards and reports

Dashboards consist of visualized data powered by fully customizable widgets, which enable you to analyze data from inside or outside Cortex Cloud, in different formats such as graphs, pie charts, or text. Cortex Cloud displays the predefined dashboards when you log in. You can also create custom dashboards that are based on the predefined dashboards, or built to your specifications, and you can save any of your dashboards as reports.

From the Dashboard & Reports menu, you can view and manage your dashboards and reports from the dashboard and incidents table, and view alert exclusions.



- Dashboard: Provides dashboards that you can use to view high-level statistics about your agents and incidents.
- Reports: View all the reports that Cortex Cloud administrators have run.
- Customize: Create and manage a new dashboard and reports.
  - Dashboards Manager: Add new dashboards with customized widgets to surface the statistics that matter to you most.
  - Reports Templates: Build reports using pre-defined templates, or customize a report. Reports can be generated on-demand scheduled.
  - Widget Library: Search, view, edit, and create widgets based on predefined widgets and user-created custom widgets.

## 3 | Review inventory and explore your cloud environment

### 3.1 | Inventory management

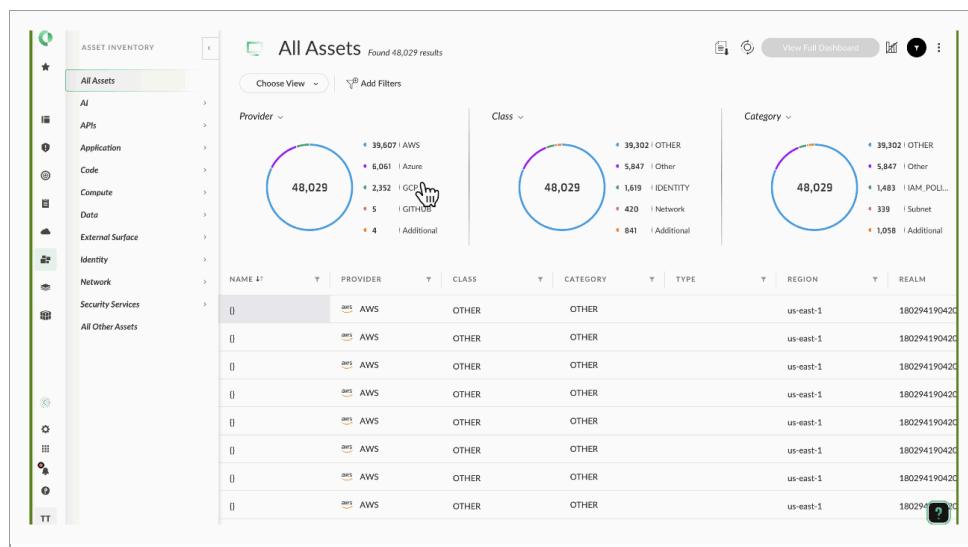
#### 3.1.1 | Asset management

##### 3.1.1.1 | All Assets

###### Abstract

Learn about the All Assets page, under Asset Inventory.

The All Assets page provides a centralized repository containing information about all assets within your environment, including enterprise, multi-cloud, code, and external surfaces. Dedicated asset modules allow multi-method asset coverage, such as agent, agentless, logs, from various sources. Having full visibility of assets allows for timely incident response, effective threat hunting, and attack surface reduction.



The asset card provides a unified view of an asset, consolidating attributes, enhancements, and related cases, issues, or findings. The Highlights section provides an overview of the security risks associated with the asset. When you click an asset, the asset card opens in a tab, enabling users to easily switch between multiple asset cards at the same time.

On each Asset card, you can perform the following actions:

- Leave comments for collaboration, and perform actions on the asset, depending on the type.
- Share links for easy access.
- View asset data: see all relevant data and raw information connected to the asset.
- Use Cortex Assistant/Cortex Agentic Assistant for insights and recommendations.

Category, class, and type are terms used to facilitate the organization and classification of assets.



- **Class:** represents the highest-level grouping of assets based on their general purpose or domain. It is a broad classification that defines the overall function of the assets.
  - Examples: Compute, Network, Data
- **Category:** represents a more detailed grouping within a class. It categorizes assets based on their normalized function or common type, regardless of the provider or implementation.
  - Examples: For Compute: Virtual Machine, Container
  - For Data: Bucket, Database
- **Type:** the most specific level of classification and represents the provider-specific name for a particular asset within a category. This level directly refers to the specific implementation of an asset.
  - Examples: For the Virtual Machine category: EC2 Instance (AWS), Compute Engine Instance (GCP).

**NOTE:**

When working with the Asset Inventory page, consider the following:

- To maintain an accurate and clutter-free asset inventory, an automated cleanup process periodically removes outdated assets in the background.

Fields on the All Assets page

The following is a list of the fields displayed on the All Assets page. The assets shown, and their data, depend on your system's licensing.

Column	Description
Name	Displays the name that describes the asset.
Provider	The provider that hosts cloud assets, such as GCP, AWS, or Azure.
Class	Grouping of assets according to industry standards. For example, Compute, Network, and Storage.
Category	Asset types given by each cloud vendor are normalized into this field.
Type	A type is the most specific level of classification and represents the provider-specific name for a particular asset within a category. <p><b>NOTE:</b></p> <p>The options available are dependent on your license.</p>
Region	Displays the region as provided by the Cloud provider.
Realm	Account ID.
Tags	Users can add information about the asset by adding tags.
Cases breakdown	The Cases attached to the asset.
Critical cases	When a critical Case is attached to an asset, the number of High or Critical cases appears in brackets.
Issues breakdown	The Issues attached to the asset.
Critical issues	When a critical Issue is attached to an asset, the number of high or critical cases appears in brackets.
Groups	Users can group assets using asset groups. The asset group indicates which assets are grouped together.



Column	Description
First observed	Timestamp of when the asset was first observed by the source that reported it.
Last observed	Timestamp of when the asset was last observed by the source that reported it.

#### Asset tabs

Assets are separated by their respective classes. The following table describes the tabs shown under All Assets.

Tab	Description
AI	Provides a detailed view of AI-related assets, their attributes, and associated risks. Key metrics at the top summarize the number of Assets at Risk, AI resources across cloud environments like AWS, Azure, and GCP, and the presence of AI Assets With Sensitive Data.
All Cloud	Asset inventory of cloud accounts and applications.
APIs	Provides a comprehensive view of APIs in your organization, including their distribution across cloud platforms, exposure status, and detailed attributes. Key metrics at the top summarize: <ul style="list-style-type: none"> <li>• APIs per Cloud</li> <li>• APIs per Service</li> <li>• Internet Exposed APIs</li> </ul>
Application	The Application Inventory provides a high-level summary and detailed insights into the applications within your environment, including their classification, providers, and categories.  Click <a href="#">View Dashboard</a> to navigate to a detailed dashboard for deeper analysis.
Code	This section provides an overview of code assets, including all code repositories, Infrastructure as Code (IaC) resources, CI/CD pipelines, and software packages.  Click <a href="#">View Dashboard</a> to navigate to a detailed dashboard for deeper analysis.
Compute	The Compute Inventory provides a detailed overview of compute resources, including virtual machines, containers, serverless functions, Kubernetes clusters, general devices, and other compute assets across your environment.  Click <a href="#">View Dashboard</a> to navigate to a detailed dashboard for deeper analysis.
Data	The Data Inventory provides an overview of data assets and their associated risks, including the number of Assets at Risk, data stored in AWS, Azure, and GCP, Sensitive Assets, and assets marked as Open to the World.



<b>Tab</b>	<b>Description</b>
Device	Overview of assets with devices that have a Cortex XDR agent installed.
External Surface	The All External Surface Inventory provides an overview of external-facing assets, including services versus websites, domains versus certificates, and their distribution across providers.
Identity	<p>The Identity section provides an overview of identity-related assets, including All Identity Assets, Human Identities, Non-Human Identities, Cloud Service Accounts, IAM Groups, and IAM Policies, giving visibility into both user and service-based identities and their associated permissions.</p> <p>Click <a href="#">View Dashboard</a> to navigate to a detailed dashboard for deeper analysis.</p>
Network	<p>The Network section provides an overview of network-related assets, including All Network resources, Load Balancers, Network Interfaces, Security Groups, and Subnets, offering visibility into the network infrastructure and security configurations within your environment.</p> <p>Click <a href="#">View Dashboard</a> to navigate to a detailed dashboard for deeper analysis.</p>
Security Services	This section provides a complete overview of the security services being actively managed within your environment.
All Other Assets	All assets that are uncategorized.

#### 3.1.1.1 | Container Images

##### Overview

Container Images are fundamental, immutable assets that package applications and their dependencies for consistent deployment across cloud environments. Each image is uniquely identified by a SHA256 digest, ensuring content verifiability throughout its lifecycle across build, deploy, and run stages. You can assign multiple names and tags to a single container image, allowing you to reference the same image in various contexts and versions within container registries.

##### Container Image Types

Understanding the different types of container images helps you manage assets, investigate findings, and resolve related issues more efficiently. You can also use this information to:

- query assets by image Type using graph searches or XQL
- group assets based on image classification
- apply cloud workload policies to monitor and protect your environment

The following table summarizes each container image type, its purpose, and key characteristics to help you effectively manage container images.



Image Type	Description	Key Characteristics
Core Image	<p>Represents the immutable content of the container image itself.</p>	<p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>Forms the foundation for other image types: Build, Registry, and Runtime Images.</li> </ul> <p><b>Properties:</b></p> <ul style="list-style-type: none"> <li>Identified by a unique SHA256 digest.</li> <li>Contains file-related findings (for example, vulnerabilities, secrets, malware).</li> <li>Has no scope and cannot directly be part of an asset group or policy, as it purely represents the image's content.</li> <li>Does <b>not</b> include issues.</li> </ul> <p><b>Relationships with other image types:</b></p> <ul style="list-style-type: none"> <li>Can reference another Core Image as its base, establishing a hierarchical relationship between images.</li> <li>Can be the "base of" another Core Image.</li> </ul> <p><b>User Interaction:</b></p> <ul style="list-style-type: none"> <li>You can query Core Image assets through XQL.</li> <li>Find Core Images listed under Inventory âœ All Assets âœ Compute âœ Container Images</li> </ul>
Build Image	<p>Represents a container image created from a CI/CD pipeline or build processes.</p>	<p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>Exists when discovered through CLI scanning in the platform.</li> <li>Helps with build traceability and integrity verification.</li> </ul> <p><b>Properties:</b></p> <ul style="list-style-type: none"> <li>Includes build metadata such as build time, source code repository, and build environment.</li> <li>Contains findings and issues related to the build image.</li> </ul> <p><b>Relationships with other image types:</b></p> <ul style="list-style-type: none"> <li>A Build Image represents a Core Image, and a Core Image can be represented by a Build Image.</li> </ul> <p><b>User Interaction:</b></p> <ul style="list-style-type: none"> <li>You can query Build Image assets through XQL.</li> <li>Find Build Images listed under Inventory âœ All Assets âœ Compute âœ Container Images</li> </ul>



Image Type	Description	Key Characteristics
Registry Image	<p>Represents a container image stored within a container registry (for example, AWS ECR, Azure ACR, Google GAR, JFrog Artifactory, Docker).</p>	<p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>Exists only when discovered through cloud discovery or registry scanning for onboarded registries.</li> <li>Helps manage images within registries and ensures compliance with registry policies.</li> </ul> <p><b>Properties:</b></p> <ul style="list-style-type: none"> <li>Includes registry-specific findings (for example, retention policy, FQDN, repository name, image tags, manifest digests).</li> </ul> <p><b>Relationship with other image types:</b></p> <ul style="list-style-type: none"> <li>The container image registry contains an image repository, and a Registry Image resides within the image repository.</li> <li>A Registry Image represents a Core Image, and a Core Image can be represented by a Registry Image.</li> </ul> <p><b>User Interaction:</b></p> <ul style="list-style-type: none"> <li>You can query Registry Image assets through XQL.</li> <li>Find Registry Images listed under Inventory â All Assets â Compute â Container Images</li> </ul>
Runtime Image	<p>Represents container images stored, running, or defined in a workload asset (such as VMs, Kubernetes workloads).</p>	<p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>Exists when discovered through Agentless Disk scan and XDR agent scan.</li> <li>Ensures that runtime images adhere to security policies and provides visibility into their deployment and operational state.</li> </ul> <p><b>Properties:</b></p> <ul style="list-style-type: none"> <li>Contains findings related to its deployment and operational state, such as configuration deviations and security policy violations. File-related findings are derived from the connected Core Image.</li> </ul> <p><b>Relationships with other images:</b></p> <ul style="list-style-type: none"> <li>A Runtime Image "represents" a Core Image, linking the runtime state to the immutable content of the image.</li> <li>A Core Image is "represented by" a Runtime Image, ensuring that any findings related to the image files are considered during runtime evaluations.</li> </ul> <p><b>User Interactions:</b></p> <ul style="list-style-type: none"> <li>You can query Runtime Image assets through XQL.</li> <li>Find Runtime images listed under Inventory â All Assets â Compute â Container Images</li> </ul>

#### Container Images asset inventory

The Container Images asset inventory provides a centralized view of all scanned container images and their details across your environments. The platform enables efficient tracking and management of your container images, ensuring compliance with security and governance standards.

You can directly access container image issues and findings within the inventory, which allows you to prioritize and remediate them without navigating to a separate remediation section.

To access container image assets:

1. Go to Inventory.



## Explore the container images inventory

The Container Image assets inventory includes a dashboard with OS Distro, OS Version, and Base Image widgets displayed by default, and an inventory table. Selecting a widget automatically filters the inventory table based on the widget's criteria.

The inventory table includes the following fields. You can filter results by any heading and value:

Fields	Description
Asset ID	A unique identifier assigned to the image.
Provider	The provider that hosts cloud assets, such as AWS, Azure, Docker, GCP, JFrog Artifactory, OCI, and Not Applicable (for core images).
Asset Type	<p>Types of container images:</p> <ul style="list-style-type: none"> <li>Core Image: Represents the immutable content of the container image itself. It is identified by a unique SHA256 digest, ensuring that any alteration to its content results in the creation of a new Core Image.</li> <li>Build Image: Represents the image created from a pipeline or build process, capturing the context of the build environment and time.</li> <li>Registry Image: Represents the container image stored in an artifact repository within a container registry. It exists only when discovered as part of cloud discovery or registry scan for onboarded registries.</li> <li>Runtime Image: Represents container images stored, running, or defined in a workload asset (VMs, Kubernetes workloads), identified by its name and digest in the runtime environment.</li> </ul>
Name	The container image name.
Image Type	Image file format. For example, Docker and OCI formats.
Image Identifier	A unique identifier assigned to a specific version of a container image, used to distinguish it from other images and ensure consistency across deployments.
Names	Aggregation of all the observed image names over time.
Realms	Indicates which connector the registry belongs to. For managed registries (such as ECR, GAR, and ACR), this field shows the CSP account.
SDLC Stages	Shows the SDLC stage when the image was created. For example, Runtime.
Base Image	Indicates whether an image is a base image (Yes) or a non-base (derived or application-specific) image (No).
Base Image	<p>Displays the number of images derived from the base image.</p> <p>For example, Base image  2 indicates there are two images derived from it.</p>
Tags	Labels assigned to container images to identify and reference specific versions or variants.
Digest	A unique, content-based SHA256 hash that immutably identifies a specific container image version.
Architecture	The CPU architecture for which the container image is built. For example, amd64, arm64, x86



Fields	Description
Image OS	The base operating system environment version the container image uses. For example, 12.10
OS Distribution	The operating system (OS) distribution name. For example, Debian.
Operating System	Operating system details of the image. For example, Linux.
OS Version	The version or release number of that OS distribution. For example, 20.04 for Ubuntu)
OS Concat	Shows combined values of OS distribution and OS version. For example, Debian 11 or Debian bookworm.
Size	Size of the container image in bytes.
First Observed	Timestamp of when the image was first observed by the source that reported it.
Last Observed	Timestamp of when the image was last observed by the source that reported it.
Scanners	List of scanners that have scanned the container image. As the container image can be scanned by multiple scanners, the values are stored as a concatenated string of all scanner types. If no scanner data exists for an asset in the database, the default value is an empty array. This column is hidden from the default view.
Last Scan	Timestamp of the most recent scan time for the container image, considering all scanners that have scanned it. If no scan data exists in the database for the container image, the default value is 0. This column is hidden from the default view.

#### Expanded Container Images asset information

On the Container Image page, select an asset in the inventory table to open a detailed Asset card, which provides additional, in-depth information about the asset. The information is organized into tabs, including an Overview tab (displayed by default) that provides highlights and a general summary, while contextual tabs focus on particular properties of the asset. The card also includes details about detected risks, allowing you to explore them directly from the asset inventory. You can also perform actions on the asset using the Actions menu.

#### Container Image summary

The Container Image Summary, displayed at the top of the card, provides concise details about the image, such as its type, cloud provider, and name.

#### Overview

The Overview tab summarizes container image Highlights, Properties, Scan information details, and Relationships between the current image and its Core Image.

Highlights include:

- Critical/High issues: An aggregation of critical and high issues associated with the container image. Clicking on this property redirects you to the Issues page, filtered by specific asset and severity level.
- Visibility timeline: When the container image was first and last detected.
- Risk summary: The risks associated with the container image, grouped by category (cases, issues, and findings). Each category includes the total number of associated risks, as well as a specific count for each severity level.

Properties include:



- Includes identifying information and cloud location of the container image: Name, ID (such as ARN in AWS), cloud Provider, cloud Region, and Account ID.
- Additional details: Includes Asset category, Asset Groups, Image Digest, Base image name along with its URL (if present), and Image name.

OS/ARCH includes:

OS information: Includes OS related information for that container image, such as OS distro, OS release, size in bytes, operating system, Docker Labels, and the type of architecture the image is compatible with.

Scan management includes:

Information about the last scan, including scanner name, version, and scan status for vulnerabilities, compliance, secrets, and malware.

Relationships include:

Information about how each logical image (Build, Registry, Runtime) is linked to the Core Image it represents, ensuring that any findings related to the Core Image are contextualized within the scope of the logical images.

This feature enables you to precisely identify the registry and repository source of any running image, directly linking runtime security findings to their origin. As a result, you can rapidly answer complex audit and security questions, such as determining which registry images are currently deployed in runtime.

#### SBOM

The SBOM tab displays details about the Software Bill of Materials (SBOM) generated by the scanning process. Exposed properties include Type, Name, Binary Packages, Version, Path, and License.

Export SBOM: You can export the entire SBOM, or selected attributes from any of the tabs in the expanded card:

Select menu → file format. Supported formats: **XML**, **json**

#### Vulnerabilities

The Vulnerabilities tab provides inventories for Findings, Packages, and Layers, enabling you to assess potential risks and prioritize remediation efforts.

**Findings:** Displays a list of findings, along with their associated CVE ID and description, EPSS score, CVSS score and severity, CVE risk factors, affected software, and fix versions, when available.

**Packages:** Displays a list of packages, their name and version, the total number of vulnerabilities found within each package, a breakdown of vulnerabilities by severity level and count, their EPSS (Exploit Prediction Scoring System), which estimates the likelihood of exploitation; CVSS (Common Vulnerability Scoring System), which rates the technical severity of the vulnerability; location; base image vulnerability; and whether a fix is available.

**Layers:** Displays the various layers and their contents within a container image.

#### Applications

The Applications tab identifies any embedded applications within the image, helping you assess security risks associated with the bundled software.

##### 3.1.1.1.2 | Kubernetes Cluster

#### Abstract

Learn about the Kubernetes Cluster feature, under the Asset Inventory page.

Navigate to Inventory → All Assets → Compute → Kubernetes Cluster for a Kubernetes Clusters assets overview. Reference the assets overview page to comprehensively assess the overall security posture of your Kubernetes (K8s) environment.

Select any cluster, to view all resources within it and any connected clusters. The Cluster details panel provides a detailed breakdown of assets, and the nodes within each cluster. Choose any of the following tabs for additional information:

- Click Resource Explorer to view the clusters components and identify any security breaches. Disconnected clusters do not show any data. Ensure all clusters are connected for maximum protection.
- Select the Vulnerabilities tab to see a list of all cluster nodes. Click on any cluster to further analyze the vulnerability. You can also find specific container images in the vulnerability list and view the container images, namespaces, and associated K8s deployment. Options include:
  - Container Image Vulnerability Findings: Displays all the vulnerabilities found in the container images running within the cluster. Select any cluster to view vulnerability details such as Max CVSS Severity, Associated K8s Resource Type, etc.
  - Kubernetes Nodes Vulnerability Findings: Provides a detailed view of vulnerabilities effecting the Kubernetes worker and master nodes. Select any node from the table view to see more information, such as Node type, associated Vulnerabilities, and Max CVSS Severity.

#### NOTE:

The Vulnerabilities tab is only available if the cluster you wish to analyze has a K8s connector.



Select Kubernetes Connectivity Management to manage the connector-connectivity of cluster assets, including connector versions, upgrades, statuses, and more. Here, you can check if a cluster is connected, view the status, and see the connector version. You can also update to a new connector version when one is released.

### 3.1.1.3 | External Surface assets

#### Abstract

The External Surface inventory provides a searchable, filterable view of all your internet-facing assets.

The External Surface inventory provides a searchable, filterable view of the internet-facing assets that Cortex Cloud has discovered and attributed to your organization, including certificates, domains, and services.

#### **NOTE:**

Cloud ASM data must be enabled before the External Surface asset inventory will populate. See [Enable Cloud ASM](#).

The following sections provide information about each External Surface asset type.

#### Certificates

Certificates (also known as digital or public key certificates) are used when establishing encrypted communication channels to identify and authenticate a trusted party. Certificates are typically used for SSL/TLS, HTTPS, FTPS, SSH, and VPN connections. The most common use of certificates is for HTTPS-based websites, which enable a web browser to validate that an HTTPS web server is an authentic website.

Cortex XSIAM tracks information for each certificate, such as Issuer, Public key, Public Key Algorithm, Subject, Subject Alternative Names, Subject Organization, Subject Country, and Subject State. Cortex XSIAM also tracks the following “cryptographic health” checks for each certificate:

- Is it self-signed?
- Is wildcard?
- Is domain control validated?
- Expired when scanned?
- Public key bits
- Signature algorithm

These health checks are referred to in the asset details as Certificate Classifications.

#### Domains

The External Surface inventory includes all domains that Cortex XSIAM has attributed to your organization and whether each domain has a recent resolution. Root domains and subdomains are displayed as separate entries in the inventory. However, if an organization owns a wildcard DNS entry, we group all subdomains of that wildcard that resolve to the same IP address under that one wildcard domain asset entry. We also collapse subdomains under the parent domain if we observe more than 1,000 subdomains.

Cortex XSIAM collects domains and DNS data from a combination of active and passive global collection techniques. For DNS scanning, Cortex XSIAM sends a BIND version query as the payload. This approach still identifies DNS servers that are not BIND compliant as their response informs us of a DNS server’s existence.

#### Services

The External Surface inventory includes all internet-facing services attributed to your organization. A service can be any internet-facing device or software that communicates on a *domain:port* or *IP:port* pair that responds to scanners on an application-level protocol over the public internet.

Services include classifications which are fingerprint-based identifiers of software, technologies, and behaviors observed on the service. Classifications can be either active or inactive based on the most recent observations of a service. In addition to classifications, services will also include banner, response, and header information from Cortex Cloud data collection.

#### Services field descriptions

The Services table includes the fields.



Field	Description
Active classifications	<p>Facts that have been inferred about each of your services by examining a response for fingerprints. Classifications cover a variety of details including:</p> <ul style="list-style-type: none"> <li>• Identifying specific software and versions.</li> <li>• Configuration details of note.</li> <li>• Identifying when the services do not implement best practices like web security headers or certificate security standards.</li> </ul> <p>Some Classifications merely note that a fact is true or false, like Missing Cache Control Header. Other Classifications provide additional information, such as a version number for “nginx Server”. These details are viewable in the services table and on the details page for the service by clicking the name of the service in the All External Services table.</p>
Business units	<p>A Business Unit is a designation to classify assets. Cortex Cloud tracks business units as a means to identify owning organizations of these assets. Business units become extremely important when an organization has subsidiaries and groups established through M&amp;A activities.</p>
Discovery type	<p>Services are identified with one of the following two discovery types, depending on the level of confidence Cortex Cloud has in attributing it to your organization.</p> <ul style="list-style-type: none"> <li>• Directly Discovered: services that are definitively associated with an asset that belongs to your organization. Examples include: <ul style="list-style-type: none"> <li>◦ It is hosted on one of your on-prem IP ranges.</li> <li>◦ The service advertises one of your organization's certificates.</li> <li>◦ It is on a managed cloud resource that is known to be yours.</li> </ul> </li> <li>• Colocated with your Services: the service is running on the same IP as a different directly-discovered service. In a multi-tenant hosting environment, these co-located services may belong to other organizations but can sometimes pose adjacency risks to your services hosted on that IP. If your organization has a single-tenant environment only policies with 3rd party hosting providers, you can use this functionality to identify possible violations of that policy.</li> </ul>
Domain	<p>The most recent domain on which the service is running.</p>
Externally detected providers	<p>The provider of the asset is determined by an external assessment.</p>
Externally inferred CVEs	<p>Externally Inferred CVEs are identified by comparing the product name and version of active service, if identifiable, with CVES for those products in the National Vulnerability Database. Additional investigation may be required to confirm if the CVE is present.</p> <p>Click on the service to view the service details, which include the complete list of all the externally inferred CVEs.</p>
Externally inferred vulnerability score	<p>This score is based on the highest CVSSv3 score for Externally Inferred CVEs on this service. If there is no CVSSv3 score for the CVE, then the CVSSv2 score is used.</p> <p>This field applies only to services with Externally Inferred CVEs.</p>
First observed	<p>When the asset was first observed via any of the sources.</p>
Inactive Classifications	<p>Previously observed classifications that are no longer observed.</p>
IP addresses	<p>Array column specifying a list of IPs associated with this asset.</p>



Field	Description
Is active	<ul style="list-style-type: none"> <li>Yes – indicates the service is active, which means that the service has been observed recently.</li> <li>No – indicates the service is inactive, which means Cortex Cloud no longer sees it on the internet.</li> </ul>
Last observed	When the asset was last observed via any of the sources.
Port	The most recent port for the service.
Protocol	The application-level protocol on the public internet over which Cortex XSIAM validated the service.
Service name	The service type along with the specific domain:port or IP:port pair for the service.
Service type	The type of server or software for the service.

### 3.1.1.2 | Serverless function assets

#### 3.1.1.2.1 | Overview

The Serverless Functions asset inventory provides a centralized view of all serverless functions and their details across your environments. The platform enables efficient tracking and management of your serverless function resource, ensuring compliance with security and governance standards. You can directly access serverless function issues and findings within the inventory, allowing you to prioritize and remediate them without having to navigate to a separate remediation section.

How to access serverless function assets

To access serverless function assets, under Inventory, select All Assets â Compute â Serverless Functions.

#### 3.1.1.2.2 | Explore the serverless functions inventory

The Serverless Functions assets inventory includes a dashboard with provider, class, and category widgets displayed by default, and an inventory table. Selecting a widget will automatically filter the inventory table based on the widget's criteria.

Serverless functions asset inventory

The inventory table includes general asset properties, as well as these unique attributes:

Property/Attribute	Description
Category	Serverless Functions
Type	<ul style="list-style-type: none"> <li>Lambda Function - for AWS</li> <li>Google Cloud Function - for GCP</li> <li>Azure App Service Web App Function - for Azure</li> </ul>
Class	Serverless functions belong to the Compute asset class

#### 3.1.1.2.3 | Expanded serverless function asset information



Click an asset in the inventory table to open its side card, providing in-depth information organized into several tabs. The Overview tab (default display) offers highlights and a general summary. Additional contextual tabs provide specific details, including a Code to Cloud tab (providing context on the asset's path to production), an Applications tab (displaying the applications associated with this asset), and tabs focusing on specific issue types detected within the asset, such as Secrets and Vulnerabilities.

#### Serverless function summary

The serverless function summary, displayed at the top of the card, provides concise details about the serverless function including cloud provider, category, region and account ID.

#### Overview

The Overview tab summarizes serverless function highlights, properties, scan management details and provides a list of entities with access to the serverless function.

Highlights include:

- **Critical/High issues:** An aggregation of critical and high issues associated with the serverless function. Clicking on this property redirects to the Issues page, filtered by specific asset and severity level
- **Visibility timeline:** When the serverless function was first and last detected
- **Risk summary:** The risks associated with the serverless function, grouped by category (cases, issues and findings). Each category includes the total number of associated risks, as well as a specific count for each severity level

Properties include:

- **Identification and Location:** Includes identifying information and cloud location of the serverless function: Name, ID (such as ArN in AWS), cloud provider, cloud region and account ID
- **Configuration and Environment:** Includes the fundamental setup and execution context of the serverless function. It includes the function category, type (the specific serverless compute service being used such as AWS Lambda, Azure Functions, Google Cloud Functions) and runtime (such as Python and Node.js)

**Scan management:** Includes information about the last scan, including date, scanner name, version and scan status.

**Identities with access to this asset:** Lists the top most privileged identities on the asset, ranked by their recent activity and highlighting those who have recently used their high-level permissions.

#### SBOM

The SBOM tab displays details about the Software Bill of Materials (SBOM) that was generated by the scanning process. Exposed properties include Type, Name, Binary Packages, Version, Path and License.

**Export SBOM:** You can export the entire SBOM, or selected attributes from any of the tabs in the expanded card: Select menu  $\square$  file format. Supported formats: **XML**, **json**.

#### Access

The Access tab includes two inventories:

- **Access permissions** (Who can access this asset): Exposed properties include Source, Grantor, Access Levels, Access to Data Labels, Last Used, Permission Scope and Excessive Policies
- **Identity access scope** (Where can this identity access): Exposed properties include Grantor, Destination, Access Level, Last Used, Access to Data Labels, Configured By and Destination ID

#### Vulnerabilities

The Vulnerabilities tab provides inventories for Findings and Packages, enabling you to assess potential risks and prioritize remediation efforts.

- **Findings:** Displays a list of findings, along with their associated CVE ID and description, EPSS score, CVSS score and severity, CVE risk factors, affected software and fix versions, when available
- **Packages:** Displays a list of packages, their name and version, the total number of vulnerabilities found within each package, a breakdown of vulnerabilities by severity level and count, their EPSS (Exploit Prediction Scoring System), which estimates the likelihood of exploitation, CVSS (Common Vulnerability Scoring System), which rates the technical severity of the vulnerability, location, base image vulnerability, and whether a fix is available

#### NOTE:

For details of all serverless function issues generated by Cortex Cloud from vulnerability findings, refer to [Serverless function usage](#).

#### 3.1.1.3 | Network configuration

#### Abstract



Cortex Cloud Network Configuration provides a representation of your network assets by collecting and analyzing your network resources.

Network asset visibility is a crucial investigative tool for discovering rogue devices and preventing malicious activity within your network. The number of managed and unmanaged assets in your network provides vital information for assessing security exposure and tracking network communication effectively.

Cortex Cloud Network Configuration accurately represents your network assets by collecting and analyzing the following network resources:

- User-defined IP Address Ranges and Domain Names associated with your internal network.
- EDR data collected by Firewall Logs.
- Cortex Cloud Agent Logs.
- ARP Cache
- Broker VM Network Mapper

In addition to the network resources, Cortex Cloud allows you to configure a Windows Agent Profile to scan your endpoints using Ping. This scan provides updated identifiers of your network assets, such as IP addresses and OS platforms. The scan is automatically distributed by Cortex Cloud to all the agents configured in the profile and cannot be initiated by request.

With the data aggregated by Cortex Cloud Network Configuration, you can locate and manage your assets more effectively and reduce the amount of research required to:

- Distinguish between assets managed and unmanaged by a Cortex Cloud agent.
- Identify assets that are part of your internal network.
- Monitor network data communications both within and outside your network.

#### 3.1.1.3.1 | Configure your network parameters

##### Abstract

Define the IP address ranges and domain names used by Cortex Cloud to identify your network assets.

Internal IP address ranges and domain names must be defined in order to track and identify assets in the network. This enables Cortex Cloud to analyze, locate, and display your network assets.

##### Define internal IP address ranges

1. In Cortex Cloud, select Assets Network Configuration.
2. Define an IP address range.

By default, Cortex Cloud creates Private Network ranges that specify reserved industry-approved ranges. These ranges can only be renamed.

To Add New Range, select either:

- Create New.
  1. In the Create IP Address Range dialog box, enter the IP address Name and IP Address, Range or CIDR values.
- Upload from File
  1. In the Upload IP Address Range dialogue box, drag and drop or search for a CSV file listing the IP address ranges. Download example file to view the correct format.
  2. Click Add.

##### NOTE:

You can add a range that is fully contained in an existing range, however, you cannot add a new range that partially intersects with another range.

##### Define domain names

1. In Cortex Cloud , select Assets → Network Configuration → Internal Domain Suffixes.
2. In the Internal Domain Suffixes section, +Add the domain suffix you want to include as part of your internal network. For example, acme.com.
3. Select ↗ to add to the Domains List.

##### IP address ranges fields



FIELD	DESCRIPTION
Range Name	Name of the IP address range defined.
First IP Address	First IP address value of the defined range.
Last IP Address	Last IP address value of the defined range.
Active Assets	Number of assets within the defined range that have reported Cortex Agent logs or appeared in your Network Firewall Logs.
Active Managed Assets	Number of assets within the defined range reported Cortex Cloud Agent logs.
Modified By	Username of the user who last changed the range.
Modification Time	The timestamp shows when this range was last changed.

#### 3.1.1.4 | Asset Groups

##### Abstract

Learn about the Asset Groups feature, under the Asset Inventory.

By grouping assets based on shared attributes, you can address them collectively. This enables more efficient bulk actions and simplifies both filtering and scoping within the inventory and across the platform.

To create an Asset Group:

1. Navigate to Inventory → Assets → Groups → Add Group.
2. Define a meaningful Group Name that represents the group's purpose to improve usability. You can choose between two types of Asset Groups:
  - Dynamic Groups: Use the filters Provider or Realm, to group current and future assets that meet the defined criteria. Click Create Dynamic Group to save.
  - Static Groups: Manually select individual assets to include in a group. After selection, click Create Static Group.
3. Add an optional Description to further clarify.

##### Use cases

Once your Asset Group has been defined, you can use it in specific areas of the platform for the following:

- Enrich asset data: Add information to a set of assets that isn't directly stored on the asset itself.
- Reuse asset groups: Reference the same group across different areas of Cortex Cloud, for example, in Policies and Rules.

##### NOTE:

When you create or edit an Asset Group, the changes are applied immediately to new assets and to existing assets that have been updated. However, it may take a few hours for the changes to appear on existing assets that have not been updated.

#### 3.1.1.5 | Vulnerability Assessment

##### Abstract

Perform a vulnerability assessment of all endpoints in your network using Cortex Cloud. This includes CVE, endpoint, and application analysis.

Cortex Cloud vulnerability assessment enables you to identify and quantify the security vulnerabilities on an endpoint. After evaluating the risks to which each endpoint is exposed and the vulnerability status of an installed application in your network, you can mitigate and patch these vulnerabilities on all the endpoints in your organization.



## Legacy Vulnerability Assessment

For a comprehensive understanding of the vulnerability severity, Cortex Cloud retrieves the latest data for each Common Vulnerabilities and Exposures (CVE) from the NIST National Vulnerability Database, including CVE severity and metrics.

### PREREQUISITE:

The following are prerequisites for Cortex Cloud to perform a vulnerability assessment of your endpoints.

Requirement	Description
Licenses and Add-ons	<ul style="list-style-type: none"><li>Host Insights Add-on.</li></ul>
Supported Platforms	<ul style="list-style-type: none"><li><b>Windows</b><ul style="list-style-type: none"><li>Cortex Cloud lists only CVEs relating to the operating system, and not CVEs relating to applications provided by other vendors.</li><li>Cortex Cloud retrieves the latest data for each CVE from the NIST National Vulnerability Database as well as from the Microsoft Security Response Center (MSRC).</li><li>Cortex Cloud collects KB and application information from the agents but calculates CVE only for KBs based on the data collected from MSRC and other sources</li><li>For endpoints running Windows Insider, Cortex Cloud cannot guarantee an accurate CVE assessment.</li><li>Cortex Cloud does not display open CVEs for endpoints running Windows releases for which Microsoft no longer fixes CVEs.</li></ul></li><li><b>Linux</b><ul style="list-style-type: none"><li>Cortex Cloud collects all the information about the operating system and the installed applications, and calculates CVE based on the the latest data retrieved from the NIST.</li></ul></li><li><b>MacOS</b><ul style="list-style-type: none"><li>Cortex Cloud collects only the applications list from MacOS without CVE calculation.</li></ul></li></ul> <p>If Cortex Cloud doesn't match any CVE to its corresponding application, an error message is displayed, No CVEs Found.</p>
Setup and Permissions	Ensure Host Inventory Data Collection is enabled for your Cortex XDR agent.
Limitations	Cortex Cloud calculates CVEs for applications according to the application version, and not according to application build numbers.

## Enhanced Vulnerability Assessment

The Enhanced Vulnerability Assessment mode uses an advanced algorithm to collect extensive details on CVEs from comprehensive databases and to produce an in-depth analysis of the endpoint vulnerabilities. Turn on the Enhanced Vulnerability Assessment mode from Settings → Configurations → Vulnerability Assessment. This option may be disabled for the first few days after updating Cortex Cloud as the Enhanced Vulnerability Assessment engine is initialized.

### PREREQUISITE:

The following are prerequisites for Cortex Cloud to perform an Enhanced Vulnerability Assessment of your endpoints.

Requirement	Description
Licenses and Add-ons	<ul style="list-style-type: none"><li>Host Insights Add-on.</li></ul>



Requirement	Description
Supported Platforms	<ul style="list-style-type: none"> <li>• <b>Windows</b> <ul style="list-style-type: none"> <li>◦ Cortex XDR agent 8.3 or a later release.</li> <li>◦ Cortex Cloud collects all the information about the operating system and the installed applications, and calculates CVE based on the latest data retrieved from the NIST.</li> <li>◦ CVEs that apply to applications that are installed by one user aren't detected when another user without the application installed is logged in during the scan.</li> </ul> </li> <li>• <b>MacOS</b> <ul style="list-style-type: none"> <li>◦ Cortex XDR agent 8.3 or a later release.</li> <li>◦ Cortex Cloud collects all the information about the operating system and the installed applications, and calculates CVE based on the latest data retrieved from the NIST.</li> </ul> </li> </ul>
Setup and Permissions	Ensure Host Inventory Data Collection is enabled for your Cortex XDR agent.
Certificates for Windows and macOS	<p>When Advanced Vulnerability and Assessment is enabled, these certificates are a prerequisite for Windows and macOS.</p> <p>Download the certificates from here.</p> <ul style="list-style-type: none"> <li>• Import the <i>Digicert Trusted Root G4</i> certificate into the Trusted Root Certification Authorities store in the local machine.</li> <li>• In some environments, if the scan does not initialize, the <i>DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1</i> certificate, may also be required.</li> </ul> <p>Import the signed certificate into the Intermediate Certification Authorities store in the local machine.</p>
Limitations	<ul style="list-style-type: none"> <li>• Some CVEs may be outdated if the Cortex XDR agent wasn't updated recently.</li> <li>• Application versions which have reached end-of-life (EOL) may have their version listed as 0. This doesn't affect the detection of the CVEs.</li> <li>• Some applications are listed twice. One of the instances may display <code>invalid version</code>, however, this doesn't affect the functionality.</li> <li>• The scanning process may impact performance on the Cortex XDR agent during scanning. The scan may take up to two minutes.</li> </ul>

You can access the Vulnerability Assessment panel from Inventory+Endpoints → Host Inventory → Vulnerability Assessment.

After enabling the feature for the first time, it may take up to a week to get the updated data into the platform. Re-collecting the data from all endpoints in your network could take up to 6 hours. After that, Cortex Cloud initiates periodical recalculations to rescan the endpoints and retrieve the updated data. If at any point you want to force data recalculation, click Recalculate. The recalculation performed by any user on a tenant updates the list displayed to every user on the same tenant.

#### CVE Analysis

To evaluate the extent and severity of each CVE across your endpoints, you can drill down into each CVE in Cortex Cloud and view all the endpoints and applications in your environment that are impacted by the CVE. Cortex Cloud retrieves the latest information from the NIST public database. From Inventory → Endpoints → Host Inventory → Vulnerability Assessment, select CVEs on the upper-right bar. This information is also available in the `va_cves` dataset, which you can use to build queries in XQL Search.

If you have the Identity Threat Module enabled, you can also view the CVE analysis in the Host Risk View. To do so, from Inventory → Assets → Asset Scores, select the Hosts tab, right click on any endpoint, and select Open Host Risk View.

For each vulnerability, Cortex Cloud displays the following default and optional values.

Value	Description
Affected endpoints	The number of endpoints that are currently affected by this CVE. For excluded CVEs, the affected endpoints are N/A.



Value	Description
Applications	The names of the applications affected by this CVE.
CVE	<p>The name of the CVE.</p> <p><b>TIP:</b></p> <p>You can click each individual CVE to view in-depth details about it on a panel that appears on the right.</p>
Description	The general NIST description of the CVE.
Excluded	Indicates whether this CVE is excluded from all endpoint and application views and filters, and from all Host Insights widgets.
Platforms	The name and version of the operating system affected by this CVE.
Severity	The severity level (Critical, High, Medium, or Low) of the CVE as ranked in the NIST database.
Severity score	The CVE severity score is based on the NIST Common Vulnerability Scoring System (CVSS). Click the score to see the full CVSS description.

You can perform the following actions from Cortex Cloud as you analyze the existing vulnerabilities:

- View CVE details:** Left-click the CVE to view in-depth details about it on a panel that appears on the right. Use the in-panel links as needed.
- View a complete list of all endpoints in your network that are impacted by a CVE:** Right-click the CVE and then select View affected endpoints.
- Learn more about the applications in your network that are impacted by a CVE:** Right-click the CVE and then select View applications.
- Exclude irrelevant CVEs from your endpoints and applications analysis:** Right-click the CVE and then select Exclude. You can add a comment if needed, as well as Report CVE as incorrect for further analysis and investigation by Palo Alto Networks. The CVE is grayed out and labeled Excluded and no longer appears on the Endpoints and Applications views in Vulnerability Assessment, or in the Host Insights widgets. To restore the CVE, you can right-click the CVE and Undo exclusion at any time.

**NOTE:**

The CVE will be removed/reinstated to all views, filters, and widgets after the next vulnerability recalculation.

#### Endpoint Analysis

To help you assess the vulnerability status of an endpoint, Cortex Cloud provides a full list of all installed applications and existing CVEs per endpoint and also assigns each endpoint a vulnerability severity score that reflects the highest NIST vulnerability score detected on the endpoint. This information helps you to determine the best course of action for remediating each endpoint. From Inventory → Endpoints+Host Inventory → Vulnerability Assessment, select Endpoints on the upper-right bar. This information is also available in the va\_endpoints dataset. In addition, the host\_inventory\_endpoints preset lists all endpoints, CVE data, and additional metadata regarding the endpoint information. You can use this dataset and preset to build queries in XQL Search.

For each vulnerability, Cortex XDR displays the following default and optional values.

Value	Description
CVEs	A list of all CVEs that exist on applications that are installed on the endpoint.
Endpoint ID	Unique ID assigned by Cortex Cloud that identifies the endpoint.



Value	Description
Endpoint name	<p>Hostname of the endpoint.</p> <p><b>TIP:</b></p> <p>You can click each individual endpoint to view in-depth details about it on a panel that appears on the right.</p>
Last Reported Timestamp	The date and time of the last time the Cortex XDR agent started the process of reporting its application inventory to Cortex Cloud.
MAC address	The MAC address associated with the endpoint.
IP address	The IP address associated with the endpoint.
Platform	The name of the platform running on the endpoint.
Severity	The severity level (Critical, High, Medium, or Low) of the CVE as ranked in the NIST database.
Severity score	The CVE severity score based on the NIST Common Vulnerability Scoring System (CVSS). Click the score to see the full CVSS description.

You can perform the following actions from Cortex Cloud as you investigate and remediate your endpoints:

- **View endpoint details:** Left-click the endpoint to view in-depth details about it on a panel that appears on the right. Use the in-panel links as needed.
- **View a complete list of all applications installed on an endpoint:** Right-click the endpoint and then select View installed applications. This list includes the application name, and version, of applications on the endpoint. If an installed application has known vulnerabilities, Cortex Cloud also displays the list of CVEs and the highest Severity.
- (Windows only) **Isolate an endpoint from your network:** Right-click the endpoint and then select Isolate the endpoint before or during your remediation to allow the Cortex Cloud agent to communicate only with Cortex Cloud .
- (Windows only) **View a complete list of all KBs installed on an endpoint:** Right-click the endpoint and then select View installed KBs. This list includes all the Microsoft Windows patches that were installed on the endpoint and a link to the Microsoft official Knowledge Base (KB) support article. This information is also available in the `host_inventory_kbs` preset, which you can use to build queries in XQL Search.
- **Retrieve an updated list of applications installed on an endpoint:** Right-click the endpoint and then select Rescan endpoint.

#### Application Analysis

You can assess the vulnerability status of applications in your network using the Host inventory. Cortex Cloud compiles an application inventory of all the applications installed in your network by collecting from each Cortex XDR agent the list of installed applications. For each application on the list, you can see the existing CVEs and the vulnerability severity score that reflects the highest NIST vulnerability score detected for the application. Any new application installed on the endpoint will appear in Cortex Cloud within 24 hours. Alternatively, you can re-scan the endpoint to retrieve the most updated list.

**NOTE:**

Starting with macOS 10.15, Mac built-in system applications are not reported by the Cortex XDR agent and are not part of the Cortex Cloud Application Inventory.

From Inventory â†“ Endpoints â†“ Host Inventory, select Applications.

- To view the details of all the endpoints in your network on which an application is installed, right-click the application and select View endpoints.
- To view in-depth details about the application, left-click the application name.

## 4 | Review and prioritize posture issues



## 4.1 | Cases and issues

### 4.1.1 | Overview of cases

Understand how cases work in Cortex Cloud.

#### 4.1.1.1 | What are cases?

Abstract

A case provides the full contextual story of a problem that impacts your organization's security, giving you an end-to-end view of the problem and streamlining your understanding of what needs to be solved and how.

A case is a defined problem created by connecting related issues into a single story. It shows the impacted assets and key data in one place, helping you focus on the threats that matter most, reduce noise, and resolve the problem efficiently using automation. Each case is unique and requires its own investigation.

Cases comprise the following objects:

- **Issues:** Problems detected in your environment that exceed defined thresholds or surpass your organization's accepted level of risk and threat tolerance.
- **Assets:** Specific entities impacted in a case and how they fit into the case story.
- **Artifacts:** Objects to which behavior or influence can be attributed, such as filenames, processes, domains, and IP addresses.

To see a list of all cases, go to Cases & Issues → Cases.

#### Case creation

A case can be created automatically from an issue or manually by a user. When new issues are detected, Cortex Cloud checks them against existing cases. If there is no matching case, a new case is created. When an issue is linked to a case, all associated assets and artifacts are also linked. After case creation, new issues can match the case until the grouping threshold is met.

A case is automatically generated for any issue with Medium severity or higher that falls into one of these categories:

- It is assigned to the Security domain.
- It is assigned to the Posture domain and has a High severity.
- It was generated from the public API or created from correlations.

While most low-severity issues do not create cases, specific analytic rules can trigger case creation for low-severity issues when action is deemed necessary. Low-severity issues created from correlation rules are not grouped into cases.

For more information about how cases are built, see Case grouping.

#### 4.1.1.2 | Resolving cases with AI

Abstract

AI tools can help you through the case analysis and resolution process.

To simplify and accelerate case resolution, Cortex Cloud integrates advanced generative intelligence directly into the case management lifecycle. By leveraging built-in machine learning and intelligent grouping logic, Cortex Cloud shifts the focus from resolving isolated issues to a holistic approach that resolves the case as a whole:

- **Intelligent case grouping:** Cortex Cloud automatically consolidates related issues, assets and artifacts into a single unified case that reveals the full scope of an attack.
- **SmartScore prioritization:** Each case is assigned a SmartScore based on its severity and calculated risk. This enables teams to focus on the most critical cases first, ensuring that high-impact security threats, posture gaps, or health issues are handled with appropriate urgency.
- **AI summarization:** Agentic AI is integrated in the case resolution process to automatically summarize context, help you investigate entities, and suggest remediation actions.
- **Guided resolution:** The Resolution Center guides you to resolution with actionable tasks that are designed to remediate the entire case as a single entity, significantly accelerating the path to resolution.

#### Agentic AI

Cortex Cloud leverages Agentic AI to collaborate on investigations and actively accelerate the entire resolution lifecycle.



Feature	Description
AI-generated case summaries	Instantly analyzes the case's full scope and impact and accelerates triage.
Agentic Assistant	<p>The autonomous "brain" of Cortex Cloud. It utilizes AI agents that plan, reason, and investigate complex threats, such as cloud identity theft or container breaches. These agents have access to case context and can create plans and perform actions such as running commands, playbooks, and scripts.</p> <p>The Agentic Assistant chat provides an interactive and intelligent way to simplify and streamline complex security operations. Enter a prompt using natural language, and your agent plans and executes the most relevant actions to fulfill your request.</p>
Resolution Center	<p>Provides actionable remediation tasks, recommendations, and progress tracking to guide you step-by-step to a complete resolution.</p> <p>With playbook task tracking across all issues and in-context links to the Workplan, you can manage tasks awaiting action, monitor work in progress, and review completed items.</p>

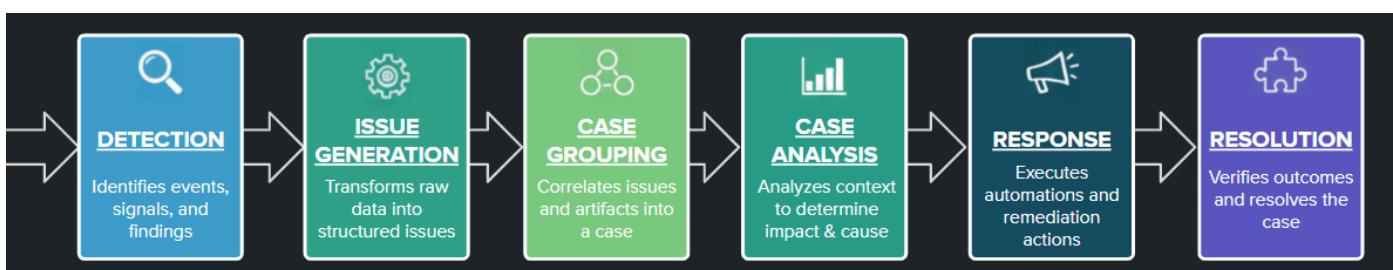
#### 4.1.1.3 | Case lifecycle

##### Abstract

Understand the lifecycle of a case.

Cortex Cloud handles cases through a structured process that moves from identification to resolution.

Stage	Description
Detection	Signals or findings surface across the environment.
Issue generation	Raw data is converted into structured, defined as Issues.
Case grouping	Issues are evaluated for case qualification. If the issue qualifies it is grouped into a case with related issues, or if no match is found, a new case is generated.
Case analysis	Examination of context, relationships, and evidence.
Response	Application of remediation actions to mitigate the threat.
Resolution	Final confirmation that the issues in the case are fully addressed.



#### 4.1.1.4 | Case thresholds

##### Abstract



Case grouping thresholds are implemented to keep cases manageable.

To keep cases manageable, Cortex Cloud implements case grouping thresholds. When the case reaches a threshold, it stops accepting issues and groups subsequent related issues in a new case.

- 30 days have passed since case creation.
- 14 days have passed since the last issue was detected.
- A case reaches the 1,000 issue limit.

You can track the threshold status in the **Issues Grouping Status** field in the cases table.

#### Auto-resolved cases

If a case is resolved with the status **Resolved – Auto Resolved**, Cortex Cloud reopens the case within a six-hour window if a matching issue occurs. The six-hour period is defined by the timestamp of the last issue that was grouped into the case. After the six-hour period, any new issues are linked to a new case for a new investigation.

#### 4.1.1.5 | Case scope and impact

##### Abstract

A case's scope and impact is determined by the assigned severity, score, and domain.

The prioritization and governance of cases are determined by the case **Severity**, **Score**, and **Domain**. Together, these factors define the operational urgency and the investigative boundaries of a case.

- **Severity:** This attribute reflects the immediate risk level. Cortex Cloud employs a logic where the overall case severity is dictated by the most critical issue linked to it. This ensures that high-impact threats are instantly visible to responders without being diluted by lower-level activity.
- **Score:** The case score provides a quantitative measure of risk. While severity indicates the severity of a case, the score offers a granular numerical value used for precise ranking.
- **Domain:** This categorizes the case context for example Security or Health. The domain determines the case's scope, directing it to the appropriate specialized team.

By aligning these three factors, Cortex Cloud automates the transition from detection to response, ensuring the most critical risks are addressed by the right experts.

#### 4.1.1.6 | Case and issue domains

##### Abstract

Cortex Cloud assigns each case and issue to a domain. Domains help you to organize and manage your work efforts, and differentiate between use cases.

Depending on the objects identified in a case or issue, each case and issue is assigned to a domain that reflects the root cause and the system areas of operation.

Domains are a contextual boundary that allow you to manage and prioritize each use case and help you to differentiate between your security use cases and non-security use cases. Domains help you to organize and manage your work efforts, streamline the assignment of cases, and enable you to create tailored experiences for each domain.

When an issue is created, Cortex Cloud automatically assigns it to a domain, and the same domain is assigned to the associated case.

Each case and issue is assigned to a single domain. You cannot change the assigned domain, however cases can be linked to issues from different domains.

#### Built-in domains

Cortex Cloud provides the following built-in domains:

Domain	Description
Security	For cases and issues that are associated with case response activities for detecting, preventing, and blocking threats as they occur in runtime.  For example, the identification of malware in a file, a compromised endpoint, or a phishing attempt. These cases can be assigned to a SOC analyst who specializes in blocking and remediating attacks.



Domain	Description
Posture	<p>For cases and issues that are associated with risk management activities to detect and mitigate risks to assets in the environment before they occur in runtime, and improve resilience.</p> <p>For example, misconfigurations in cloud instances, over-permissive users, or the detection of secrets or shadow data. These cases can be assigned to an analyst who specializes in strengthening the security posture.</p> <p>The Posture domain has subcategories that define the posture issue (Configurations, Vulnerability, Identity, etc).</p>
Health	<p>For cases and issues that are associated with health monitoring activities, to ensure optimal platform performance and gain insights into health drifts. For example, disruptions in data ingestion, collector connectivity errors, correlation rule errors, and event forwarding errors.</p>

#### 4.1.2 | Case concepts

##### 4.1.2.1 | Issues, findings, and events

###### Abstract

Understand how issues, findings, and events are related to cases.

Understand how issues, findings, and events are related to cases.

###### 4.1.2.1.1 | Issues

Issues identify the problems that you need to solve in your environment. Cortex Cloud creates issues when problems occur in your environment that cross defined thresholds, or surpass your organization's accepted level of risk and threat tolerance.

Each issue comprises a defined framework of:

- **What happened:** A description of the problem
- **How is your environment impacted:** Affected assets or the impact of this issue in your environment
- **Contributing evidence:** Data that supports our analysis and observations
- **Recommended actions:** Automations and manual suggestions

Issues are created from findings or from events that occur in your environment. When an issue is created, Cortex Cloud assesses the content of the issue and assigns it to a new or existing case. In addition, according to the content of the issue, it is assigned to a domain that reflects the operational use case of the issue, such as Security or Health. Using case grouping logic, Cortex Cloud then determines whether to link the issue to a case.

When you open a case, you can see all issues that are linked to the case. Review the **Grouping graph** to see why the issues were grouped together in the case. For more information about how issues are grouped in cases, see Case grouping.

In addition, Cortex Cloud offers the flexibility to:

- Manually link and unlink issues from cases. Issues can also be linked to multiple cases. For more information, see Link or unlink issues from a case.
- Mirror Cortex issues with external applications (for example, Atlassian Jira). For more information, see Issue syncing.
- Create issues from custom rules that you define. For example, correlation rules, malware rules, and vulnerability rules. For more information about setting up rules, see What are detection rules?.

###### 4.1.2.1.2 | Findings and events

###### Abstract

Findings and events form the core of our knowledge data lake. **Findings** provide context about the current state of the assets in your environment and **Events** are logged activities that occur in your environment.

Findings and events form the core of our knowledge data lake.



## Findings

**Findings** are non-actionable, informational objects that provide context about the *current state* of the assets in your environment.

To gather findings, Cortex Cloud periodically scans the assets in your environment and collects raw data about vulnerabilities, compliance, exposures, malware, secrets, and other posture-related information about the asset. This raw data is processed, saved to datasets, and recorded as findings.

Each time the assets are scanned, the findings are updated to reflect the current state of the assets. Therefore, the finding for an asset will change over time.

Each finding is categorized according to its context, for example Configuration, Vulnerability, Compliance, or Identity, and is related directly to the scanned asset. When you investigate an asset through the Asset Inventory, you can see any findings that were collected for the asset.

Findings themselves are not issues, however findings that match a specific logic can generate issues. You can also set up your own rules to trigger issues when certain types of findings are recorded. For example, you can set up Compliance rules that will create issues if specific compliance fails are identified in compliance findings.

To view findings:

- View all findings. From the Issues page click Findings.
- See findings for a specific asset. From the Asset Inventory, select a specific asset to open the asset card. If findings are available for the asset you can click to open the finding card.
- Search the **Findings** data set to see the findings collected over time for an asset.

## Events

**Events** are logged activities that occur in your environment.

Cortex Cloud collects event logs that audit the activities that occur in your environment. The logs are ingested from various sources, such as Palo Alto Networks Next-Generation Firewall (NGFW), Prisma Access, third-party sources, and EDRs. These logs provide a complete picture of the events that occur in the environment and the activities surrounding the events.

When certain malicious objects (such as malware) are discovered in the event logs, an issue is created. During case investigation, you can query your event logs to see information about the actors and processes that triggered the issue.

### 4.1.2.2 | Case grouping

#### Abstract

Cortex Cloud uses a specific case grouping logic to build cases.

Case grouping is a Precision AI-powered capability that eliminates alert fatigue by automatically consolidating related issues and artifacts into a single unified case. Case grouping links issues that originate from the same attack flow or involve the same entity to reveal the full scope of a case. This approach replaces manual correlation with automated context, allowing you to focus on resolving complete problems rather than triaging isolated events.

#### Grouping methodologies

The key grouping methodologies of case grouping are:

- **Artifact association:** Groups issues that share core artifacts (for example, SHA256, HostName, UserName).
- **Exact match detection:** Groups similar detections for the same entities.
- **Related entities:** Groups detections involving related assets within a close timeframe to highlight possible connections.

#### Case qualification for issues

Not all issues create cases. When a new issue is created, it is evaluated to determine if it meets the criteria for case promotion. If the issue qualifies, the system attempts to correlate it with an existing case; if no match is found, a new case is generated. Issues that do not meet these requirements are categorized as Insights.

The qualification logic varies by domain. For the Security domain, the system promotes issues with Medium severity and above, as well as select Low-severity analytics. Other domains employ more selective promotion based on specific criteria. This logic is dynamic and may be updated to reflect ongoing research and threat relevance.

Cortex Cloud applies the following logic when building cases:

- **Automatic promotion criteria:** Issues with the following conditions automatically generate a new case, or join existing cases:
  - Assigned to the **Security** domain with **Medium** severity or higher
  - Assigned to the **Posture** domain and with **High** severity.
  - Generated from the **public API** or created from **correlations**.



- **Low severity handling:** Most low severity issues do not initiate case creation, unless specific analytic rules deem action necessary. Low severity issues generated from correlation rules are not grouped into cases.
- **Case grouping thresholds:** To keep cases manageable, Cortex Cloud enforces specific grouping thresholds. For more information see Case thresholds.

#### Grouping artifacts

The grouping algorithm evaluates extracted artifacts to determine whether an issue should join an existing case or initiate a new one. Each artifact type is governed by specific logic that accounts for its unique lifecycle and reliability. For example, grouping by Username may be subject to temporal constraints, while IP address logic varies based on whether the address is public, private, or dynamically allocated (DHCP).

These proprietary grouping logics are continuously tuned and updated. As a result, artifact behavior and correlation may change over time.

#### Integration with SmartScore

Case grouping and SmartScore work together to improve triage efficiency. While case grouping provides the full context of an attack, **SmartScore** assigns a numerical value to that context, indicating the urgency and impact of the case. This allows you to prioritize the most critical cases first.

#### Limitations

Case grouping is natively supported within built-in domains only, for example Security.

### 4.1.2.3 | Case scoring

#### Abstract

Learn about the different case scoring methods.

A case score is a numeric value that indicates the urgency of a case. Scoring can help you to streamline the process of prioritizing and investigating your cases, and help you to identify the cases that require immediate attention.

#### Types of scoring

Cortex Cloud uses the following scoring methods:

- Rule-based scoring: The score is determined by user-defined scoring rules that match the issues linked to the case.

You create scoring rules that define scores for issues with specific attributes or assets. You can base scoring rules on:

- Hostnames
- Asset objects, such as asset names, classes, categories, groups, providers, and business application names.
- IP addresses
- Users
- Active Directory, or Azure groups and organization units

(Requires the Cloud Identity Engine to be configured).

When an issue is created, Cortex Cloud searches for scoring rules that match the issue. An issue can match multiple rules or sub-rules. If a match is found, Cortex Cloud assigns the scores of the matching rules to the issue. If multiple rules match the issue, the issue score is an aggregation of the rule scores. By default, a score is applied only to the first issue in the case that matches the defined rule and sub-rule.

You can create a rule hierarchy by setting up sub-rules. If an issue matches one or more sub-rules, the sub-rule scores are also aggregated in the issue score. However, a sub-rule score is only applied to an issue if the top-level rule was a match.

To determine the case score, Cortex Cloud calculates the combined issue score total for all issues in the case. You can see a breakdown of the score by clicking on the score in the details pane.

- Manual scoring: The score is defined by the user.

#### How Cortex Cloud assigns the score

For Cortex Cloud to provide effective rule-based scores, you must define accurate scoring rules that are suitable for your environment and workflows.

When a case is created, Cortex Cloud searches for a match between your scoring rules and the issues linked to a case. If a match is found, a rule-based score is assigned.

You can view the assigned score on the Cases page.



#### 4.1.2.4 | Case starring

##### Abstract

Starring cases can help you to prioritize and filter your cases.

To help you focus on the most important cases, you can star a case. Starring enables you to narrow down the scope of cases on the Cases page. Cortex Cloud identifies starred cases with a purple star.

You can star cases manually, or create a starring configuration. A starring configuration automatically categorizes and stars cases that contain issues with specific attributes. For example, you can define a starring configuration that stars all issues containing specific assets, hosts, or business application names. If an issue matches the attributes in the starring configuration, the issue and case linked to the issue are starred.

You can manage all starring configurations under Case & Issues → Case Configuration → Starred Issues. For more information see Create a starring configuration.

#### 4.1.2.5 | What is Causality?

##### Abstract

Learn more about Causality in Cortex Cloud.

Causality is the idea of telling a story in a simple and coherent manner and in a proper context. With the purpose of leading security teams to actionable outcomes.

Palo Alto Networks products, such as Next-Generation Firewall (NGFW) or the Cortex XDR Agent, can be configured to send rich and detailed data about all activities to the Strata Logging Service, not only items related to attacks. This means that millions of data points are collected about every entity every single day. Analyzing so much data as log lines is practically impossible, so Cortex Cloud takes these data points and continuously stitches them automatically → Causality Chains. This automates the dot-connection process that an investigator would otherwise have to do manually during an investigation. This process happens constantly for all collected data points, such as processes, files, network connections, and more, regardless of prevention, detection, or alerts of any kind. With causality, when analysts decide to investigate alerts or go on a hunt, they don't need to manually connect the dots getting distracted with millions of irrelevant data points, and instead they can focus only on data related to the investigation.

Even the most complicated investigations take just a few moments for a novice analyst, during which causality reveals answers to critical questions, such as:

- What was the root cause?
- What might be the damage?
- What's the scope? Are there any related issues?
- Who's involved?
- Which steps are required to contain, mitigate and recover?
- Are similar threats prevalent in the environment?
- What can be done to reduce the risk of the same thing happening again?

To achieve this, Palo Alto Networks invested and patented the causality engine and the ways it works.

##### How it works

Causality chains are built using a deep understanding of each operating system (OS) and the way it works, which processes fulfil the various functions and more. Causality chains in Windows, macOS, and Linux work with the same guidelines, with different processes and methods used to decide how to build chains.

There are some processes in the OS that have very specific roles to fill. For example, `services.exe` and `explorer.exe` are used mainly to spawn other processes. This means that causality chains don't show these processes by default and start from their child processes as these are only OS processes doing their job; yet, you can manually add them by right clicking on the Causality Group Owner (CGO) and adding the parent process.

Cortex Cloud tracks Remote Procedure Call (RPC) requests between processes and it doesn't break the causality chain into sub chains, so the analyst still sees the full chain of execution, including actions done via RPC. Same goes for code injection, as Cortex Cloud tracks the new threads that are started as a result of such actions and can tie anything that happens as a result to the original injecting processes and its causality chain.

##### Spawners

Processes that are used to spawn other sub processes are called spawners. Those processes are known to start other processes as part of the normal flow of the operating system (OS). Examples of such processes are `explorer.exe`, `services.exe`, `wininit.exe`, `userinit.exe`, and more. When spawner processes are started by a non-spawner process, they are not considered spawners. In Cortex Cloud, we don't distinguish between a Causality Group Owner (CGO) and spawner, calling both CGO.

Example 14.



- `userinit.exe` starts `explorer.exe`: `explorer.exe` is considered a spawner, as this is what we expect to see in the OS.
- `cmd.exe` starts `explorer.exe`: `explorer.exe` is NOT considered as a spawner as it's not the role of `cmd.exe` to start `explorer.exe`.

The child processes of a spawner are considered as CGOs and they start off the causality chain.  
Causality Chain

When a malicious file, behavior, or technique is detected, Cortex Cloud correlates available data across your detection sensors to display the sequence of activity that led to the alert. This sequence of events is called the causality chain. The causality chain is built from processes, events, insights, and alerts associated with the activity. During the alert investigation, you should review the entire causality chain to fully understand why the alert occurred.

#### Causality Analysis Engine

The Causality Analysis Engine correlates activity from all detection sensors to establish causality chains that identify the root cause of every alert. The Causality Analysis Engine also identifies a complete forensic timeline of events that helps you to determine the scope and damage of an attack and provide an immediate response. The Causality Analysis Engine determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident.

#### Causality Group Owner (CGO)

The Causality Group Owner (CGO) is the process in the causality chain that the Causality Analysis Engine identified as being responsible for or causing the activities that led to the alert. A CGO is always the child of a spawner, so it's the first process in the operating system (OS) chain of execution that is not loaded by default as part of what's expected in a normal OS flow. All sub-processes started by the CGO are linked to it, and help analysts quickly identify the root cause of why something happened.

#### **NOTE:**

There are no CGOs in the Cloud Causality View, when investigating cloud Cortex Cloud alerts and Cloud Audit Logs, or SaaS Causality View, when investigating SaaS-related alerts for 501 audit events, such as Office 365 audit logs and normalized logs.

#### CID

Each causality chain gets a unique ID called a CID. All actions on this chain, such as process execution, registry changes, and network connections, receive the same ID. This means that whenever the user queries about a given action, for example who connected to a malicious IP, the response not only includes the process who performed it or the user, it includes all actions related to the same CID. This shows the entire chain of execution alongside all other actions performed with the connection to the malicious IP.

This concept is important because any alert that is triggered about any action is also mapped to the same CID, meaning that one chain of execution displays all processes and alerts associated with the relevant CID. Alerts on the same CID is also one of the methods Cortex Cloud uses to group alerts into an incident.

### 4.1.3 | Analyze and resolve cases

#### Abstract

Learn how to analyze and resolve cases.

The following sections explain how to review, analyze, and resolve cases. You can start reviewing the cases in your environment on the Cases page.

#### 4.1.3.1 | Review all cases

#### Abstract

Start reviewing your open cases on the **Cases** page.

The main **Cases** page is the starting point for monitoring and managing all cases in your environment. It provides visibility into all cases and their current status, helping you track progress, investigate individual cases, and take remediation actions. Severity indicators, scores, and starred icons help you quickly identify your high-priority cases.

You can access the **Cases** page from **Cases & Issues** → **Cases**. By default, all open cases are displayed.

#### Viewing modes

The cases page supports the following viewing modes:

- **Split view (default)**

Displays cases in a split-pane layout that highlights key details and enables you to quickly compare cases, prioritize urgent items, and assess severity and impact at a glance.

- **Table view**

Displays cases in a table layout with widgets that summarize the table data. Widgets are customizable, allowing you to tailor the table for structured analysis and review.



Click the **Display** menu to switch between modes. Any changes that you make to the case fields persist between modes.

#### NOTE:

The legacy view is also available for users who prefer this format. From the Actions menu select Switch to legacy view.

##### Saved table views

Saved table views are saved filter configurations of table data that help you to focus on the data that most matters to you. You can filter your table data by domain, context, work queue, or other criteria, and save configurations that support your workflow.

The default view on the Cases page is **All Cases**. Click on the arrow next to All Cases to see all available saved views. If you change the table filters, you will see a Modified label next to the view name. You can create a new saved views. Once you have change the table filters, click the three dots next to the view name to save the new configuration, update an existing saved view, or revert to the original configuration.

#### 4.1.3.2 | Start case analysis

##### Abstract

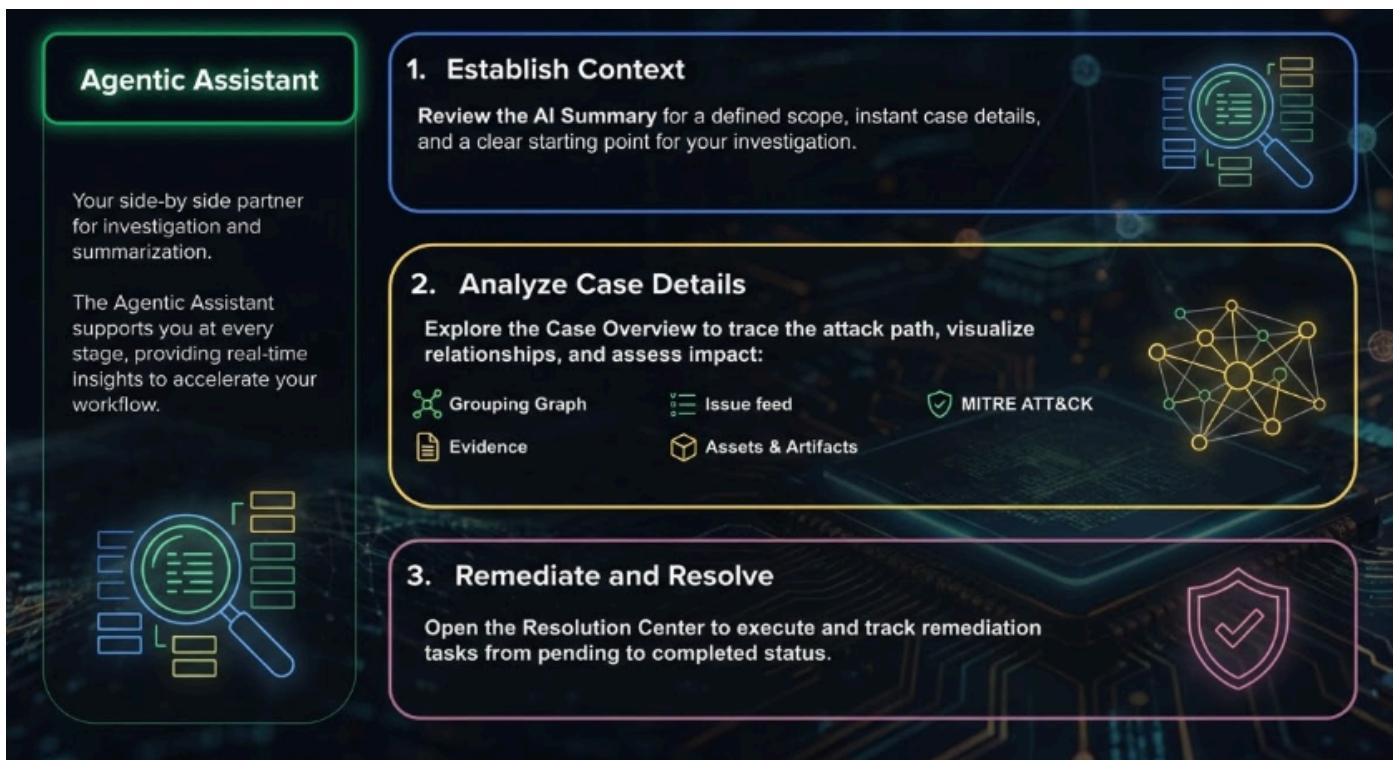
Understand the case analysis and resolution process.

To start analyzing a case, open the case from the main **Cases** page. In the Split view, click a case to open it in the side panel. To open a case in a full page layout, right-click a case in the list and select View case in new tab.

The case card opens a dedicated workspace where you can fully understand, investigate, and resolve the case from start to finish.

The case card brings together case context, correlated issues, affected assets, and remediation actions in one place. It helps you quickly understand the case context, see how events are connected, and take action with confidence. Click through the view to dive into investigation data, resolution tasks, and AI assistance without switching pages or losing context, keeping your focus on resolution.

##### Case analysis and resolution process



The following table describes the core components of case analysis and resolution:



Component	Description	Link To Detailed Information
Agentic Assistant	Provides side-by-side support by recognizing case context, delivering advanced summarization, and helping you pivot to additional investigative views.	Agentic Assistant- Case Investigation agent
AI-generated case title and description	Helps you quickly understand the scope and nature of the case by summarizing key case details.	AI-generated case summaries
Case overview	<p>Breaks down case components to help you understand how the case was built:</p> <ul style="list-style-type: none"> <li>• <b>Grouping graph:</b> Illustrates issue relationships</li> <li>• <b>Evidence:</b> Details casualties and events</li> <li>• <b>Issue feed:</b> Narrates the case story</li> <li>• <b>Associated assets, artifacts, and MITRE ATT&amp;CK tactics:</b> Provides additional context and links to detailed views and actions</li> </ul>	Analyze case details
Detailed view	Provides detailed information about the investigation in a tabular format, for example Timeline and War Room.	Detailed View
Resolution Center	Guides you towards resolution by presenting actionable remediation steps and enables you to track all related playbook tasks without opening individual playbooks.	Resolution Center

#### 4.1.3.2.1 | Agentic Assistant- Case Investigation agent

##### Abstract

The Agentic assistant provides side-by-side support throughout the case analysis and resolution process.

The **Agentic Assistant** is a context-aware, generative intelligence tool embedded directly within the case card. It is designed to act as a side-by-side partner for security analysts, eliminating the need to pivot away from the investigation to consolidate complex data.

When you open the Agentic Assistant you can select the agent that is best suited for each task. The dedicated Case Investigation agent can help you with your case investigation. It specializes in advanced summarization, and recognizes the context of the case, ensuring every insight provided is highly relevant and grounded in the specific issues, assets, and telemetry of the current investigation.

For more information about using other agents in the Agentic Assistant, see Get started with Agentic Assistant chat.

##### Core functionalities of the Case Investigation agent

To streamline case analysis, the assistant provides the following areas of support:

- Dynamic summarization of log data and issues into clear, actionable narratives, including:
  - **Executive overviews:** High-level summaries that focus on impact and risk.
  - **Extended technical overviews:** Deep-dive summaries that outline the technical progression of the threat.
- Focused contextual inquiries to extract specific details without manual filtering. You can ask targeted questions regarding:
  - **Issue deep-dives:** Understanding the specific triggers and severity of an issue.
  - **Asset relationships:** Identifying which users or devices are at the center of the activity.
  - **Asset and artifact investigation:** Understanding the impact and risk of the assets and artifacts in the investigation.
- Intelligent pivoting and clarification to help you navigate through complex investigations:
  - **Entity-specific prompts:** By clicking Ask AI next to a specific entity (such as an IP address or file hash), the assistant launches with a pre-configured prompt tailored to that specific object.
  - **Investigation guidance:** It suggests potential next steps and actions, and links to detailed views



#### 4.1.3.3 | Establish case context

Before you start to analyze the case, review the case title and description to establish case context. You can also review the case score, assignee, and decide whether to star the case.

##### 4.1.3.3.1 AI-generated case summaries

###### Abstract

AI generated case summaries helps you quickly understand the scope and nature of the case by summarizing key case details.

To gain immediate situational awareness, Cortex Cloud automatically builds a narrative of the case using **AI-generated titles and descriptions**. This summarized context allows you to quickly grasp the scope of a case and provides a clear starting point for your investigation.

Leveraging LLM-based summarization, the system analyzes complex data to produce a human-readable overview of:

- The nature of the threat or activity
- The key issues and artifacts involved
- The affected assets or identities

###### View the AI-generated case summary

When you open a case, the case title and summary is automatically generated. As an investigation evolves, the case context is updated. Each time new data or issues are added, the system regenerates the title and description to ensure your situational awareness reflects the most current information available.

###### NOTE:

The AI-generated title and description is a calculated value that is regenerated each time you open a case.

This value is not a saved static description, therefore it is not reflected in the saved case names in the list of cases in the **Split view**, or in the **Case Name** and **Case Description** columns in the **Table view**.

###### System-generated case titles and descriptions

In addition to the AI-generated case titles and summaries, Cortex Cloud automatically generates static case titles and descriptions that are stored in the cases dataset. These are generated at the time of case creation based on correlated issues, behaviors, and contextual data.

These static descriptions are used when AI-generated case summaries are unavailable or disabled. In addition, they are reflected in the case title in the List of cases in the **Split view**, and the **Case Name** and **Case Description** columns in the **Table view**.

You can manually update these values. From the **Actions**  menu select **Edit case details**.

###### Single issue cases

For cases that contain a single issue, the case title and description directly reflect the issue's title and description. In addition, AI-generated case summaries are not available. If more issues are linked to the case, Cortex Cloud generates a case title and description to reflect the issues in the case, and a AI case title and summary is available.

###### Limitations

- **Supported regions:** AI-generated case titles and summaries are available only in supported regions. For more information, see Cortex Agentic Assistant.
- **Supported domains:** AI-generated case titles and summaries are only supported for cases assigned to the **Security** and **Posture** domains.
- **Single-issue cases:** For cases that contain a single issue, AI-generated case summaries are not available. Instead, the case title and description directly reflect the issue's title and description. If more issues are linked to the case, an AI case title and summary is generated.

###### Enable AI summarization

To enable AI case summarization on your tenant, go to Configurations → General → Server Settings → AI Configuration and enable the following settings:

- Agents & LLM Experience
- AI Case Summarization

You can also turn AI summarization on or off for a specific case. Take the following steps:

1. Open the case, click the **Actions** menu.
2. Select **Edit case details**.
3. Switch the **Summarize with AI** toggle.



#### 4.1.3.3.2 | Assess case severity and score

##### Abstract

Review the case severity and score, and see a breakdown of how the score was calculated.

You can review the severity and score assigned to the case, and update them if necessary.

##### Review case severity

The severity value indicates the urgency of a case. Possible values are **Critical**, **High**, **Medium**, and **Low**. Click on the assigned severity to change the value.

##### Review the case score

The assigned case score is displayed in the cases header. This score indicates the urgency and impact of the case.

Click on the case score to see the assigned scoring method. For more information about scoring types and how Cortex Cloud assigns a score, see Case scoring.

##### See a breakdown of the score

You can see details about the scoring method and the assigned score.

1. On the **Cases** page, click on the menu icon to switch to the detailed view.
2. Click on an assigned score.

If you are not satisfied with the score, you can change the scoring method or overwrite the score by setting the score manually. If you see a discrepancy with the assigned score, consider the following:

- For rule-based scores, revise your scoring rules.
- For SmartScores, help to improve the accuracy of SmartScore. **Give feedback** by hovering over the displayed score.

##### Change the scoring method or set the score manually

You can change the default scoring method. In addition, if Cortex Cloud was unable to assign a score, you can set the score manually.

1. Click on the assigned score.  
If no score was assigned, in the case investigation pane, click the more options icon and select **Manage Score**.
2. Select a different scoring method, or click **Set score manually** and define a new score.

#### 4.1.3.3.3 | Update case attributes

##### Abstract

You can update the case title and description, and choose whether to star a case.

When you start reviewing a case, you can update the case title and description, assign the case, and star a case.

##### Assign a case

You can assign or reassign a case by clicking on the assigned field.

If the case contains unassigned issues, or the issues are not assigned to the case assignee, a dialog opens with options for assigning the issues.

##### Update the case title and description

A case title and description is automatically generated for each case. In addition, AI-generated case summaries are automatically generated when you open a case to provide case context.

You can manually update the saved case description, as required.

1. Select a case and open the Actions  menu.
2. Select **Edit case details**.
3. Update the values in the Case title and Case description fields.

##### NOTE:

The defined values are shown in the Case Name and Case Description columns in the Table view, and saved to the cases dataset. The case title is also shown the list of cases in the Split view.

These values do not replace the AI-generated case title and summary. If the **Summarize with AI** toggle is enabled, AI-generated case summaries are automatically generated when you open a case. For more information about how Cortex Cloud generates case titles and descriptions, see AI-generated



## case summaries.

4. Save your changes.

Star or un-star a case

You can manually star or un-star a case:

1. Go to Cases & Issues → Cases and select the case that you want to star.
2. Depending on the selected view, take the following action:
  - In the **Split** view, open the Actions menu and select Edit case details. Switch the toggle to star or un-star the case.
  - In the **Table** view, select one or more cases and right-click. Select whether to star or un-star the cases.

### 4.1.3.4 | Analyze case details

Abstract

You can analyze detailed information about the case in the **Overview** section of the Case card.

Once you have established the initial context, you can use the case **Overview** to deconstruct the case and understand how its underlying components are connected. Use the following sections within the **Overview** to review the full scope of activity:

- **Grouping Graph:** View a visual mapping of how issues and artifacts are linked together, including details on shared artifacts, to better understand the underlying grouping logic.
- **Evidence:** Trace issue causality chains and recorded events to follow the attack sequence from the initial root cause to the final recorded activity.
- **Issue feed** Review the case's story in a chronological visualization that maps the case lifecycle and highlights key case information, with the option to group by attribute.
- **Associated assets and artifacts:** Drill down into the specific identities, endpoints, and digital artifacts associated with the case to assess the threat's footprint.
- **MITRE ATT&CK tactics and techniques:** Review the specific tactics and techniques identified in issues linked to the case to align your investigation with industry-standard adversary behaviors.

The following topics describe each section of the Case **Overview**.

#### NOTE:

If you prefer a tabular or legacy layout, switch the case card to the **Detailed view**.

This view preserves the legacy tab based format and custom layouts, ensuring full backward compatibility. You can switch between the new case experience and the legacy view based on personal workflow preferences. For more information, see [Detailed View](#).

#### 4.1.3.4.1 | Grouping graph

Abstract

Gain insight into why issues were grouped in a case.

The **Grouping Graph** is a visual representation of the logic used to group issues in a case. It provides transparency into why specific issues are linked, illustrating the relationships between data points and the underlying decision-making process of the analysis engine.

By revealing these connections, the graph offers key insights into the case narrative, visualizes the overall scope, and identifies common artifacts for investigation.

Understanding case grouping

Cortex Cloud automatically matches issues and artifacts into a unified case based on a specific grouping logic. This allows you to resolve the entire scope of a case rather than treating detections in isolation. The logic is driven by the following factors:

- **Artifact association:** Issues sharing core artifacts, for example the same file hash or IP.
- **Similarity clustering:** Issues with similar detection patterns on the same entities.
- **Related entities:** Detections on related assets occurring within a close timeframe or context.
- **Linked and merged issues:** Issues that were manually linked to the case and merged issues.

Related issues are added to the case until a specific **grouping threshold** is met. In the **Grouping Graph** you can see whether case grouping is active or inactive. For more information about case grouping and case thresholds, see [Case grouping](#).

Core components of the Grouping Graph



The graph uses a structured hierarchy of edges and nodes to represent the primary elements of a case:

Component	Description
Edges	<p>Represent the relationship between graph entities to show why they were linked. Edges display as lines that link nodes and entities together. Each full line represents a direct relationship.</p> <p>The system defines three edge types:</p> <ul style="list-style-type: none"> <li>• <b>Case &gt; Issue:</b> Links the case to the issue that initiated its creation.</li> <li>• <b>Issue &gt; Artifact:</b> Links an issue to an associated artifact. This indicates that the issue is the source of the artifact in the case.</li> <li>• <b>Artifact &gt; Issue:</b> Links an artifact to an issue or issue cluster. This indicates that the artifact is the source of the issues in the case.</li> </ul> <p>Edges display as:</p> <ul style="list-style-type: none"> <li>• <b>Solid line:</b> Connects the case node to its originating issue, as well as to related artifacts and additional issues later grouped into the case.</li> <li>• <b>Broken line:</b> Connects similar, manually linked, or merged issues to the case. The connection type is indicated by a label: <ul style="list-style-type: none"> <li>◦ <b>linked:</b> Issues manually linked to the case</li> <li>◦ <b>similar:</b> Issues grouped by similarity clustering</li> <li>◦ <b>merged:</b> Issues merged into the case</li> </ul> </li> </ul>
Case node	The central anchor node to which all other elements are connected.
Issue nodes	Visualized with parent/child relationships to show how primary threats spawned secondary activities.
Clusters	<p>Groups of issues that are automatically clustered to keep the visual workspace organized, with details of the total issue count in the cluster and severity breakdown. Issues are clustered if they:</p> <ul style="list-style-type: none"> <li>• Share a common artifact.</li> <li>• Are manually linked to the case.</li> <li>• Have been merged.</li> <li>• Are identified as similar through similarity clustering.</li> </ul> <p><b>NOTE:</b></p> <p>Similar issues are displayed as individual entities rather than in a parent/child hierarchy.</p>
Artifacts	Represent artifacts that are linked to the issues in the case. Artifacts include user names, IPs, and causality chains. Causality chains link issues in the same causality chain to the case.

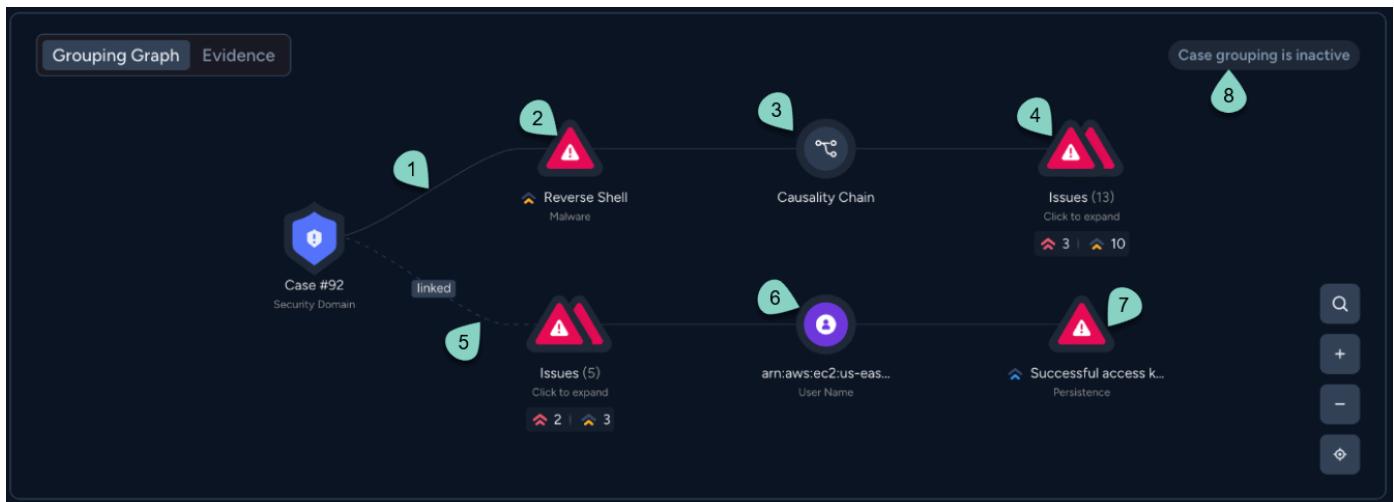
## Explore the graph

You can interact with the graph to uncover deeper layers of data without leaving the case view:

- **Expand and break down:** Click elements within the graph to expand clusters and view additional node details, such as severity, domains, and current status.
- **Review issues and artifacts:** Hover over any entity in the graph to open a quick-view panel containing high-level details such as severity, domain, and current status. Hover over a cluster to see a breakdown of the severities contained within it.
- **Deep dive into issues:** Click an issue node and select **Open Issue** to view a detailed issue card with granular details about the issue.

Example 15.





The following table breaks down the components in this example:

Label	Explanation
1	Solid edge linking the case node to the issue that initiated case creation.
2	The issue that initiated case creation.
3	Causality chain related to the initial issue.
4	Cluster of issues. These issues are part of the same causality chain as the initial issue. You can see that there are 13 issues in the cluster, and their severity breakdown.
5	Broken edge linking to a cluster of issues that were manually linked to the case. This is indicated by the linked label.
6	User name related to one or more issues in the linked issues cluster.
7	Issue related to the user name.
8	Case grouping is inactive label. This indicates that the case is no longer accepting new matching issues, which happens when a case grouping threshold is met. For more information, see Case thresholds.

#### 4.1.3.4.2 | Evidence

##### Abstract

Review the Evidence section of the Case card to see details of causalities and events.

The **Evidence** tab allows you to trace issue causality chains to follow the sequence of events from the initial root cause to the final recorded activity. If causalities are not available, the Events table lists related events for the process node which matches the issue criteria that were not triggered in the issues table, but are informational.

By mapping these dependencies, you can pinpoint exactly how a threat entered your environment and identify the specific actions taken at each stage of the attack. This insight helps you move beyond seeing what happened to understanding the attacker's path, enabling you to implement more effective containment and remediation strategies.

How to investigate a causality chain



The causality chains are listed according to the Causality Group Owner (CGO), expand the CGO card you want to investigate. Each CGO card displays the CGO name, the following CGO event details, and the causality chain:

- CGO name
- Issue sources associated with the entire causality chain
- Execution time of the causality chain
- Number of issues that include the CGO according to severity.

Expand the causality chain to further investigate in the full Causality view. For more information, see Causality view.

#### 4.1.3.4.3 | Issue feed

##### Abstract

See a chronological visualization of the case lifecycle in the issue feed.

The issue feed provides a chronological visualization of the case lifecycle, highlighting key case information from initial detection to the most recent activity. Key features include:

- **Issue count:** See the total number of issues linked to the case.
- **High level details:** Review issue details in the timeline, or click an issue to open the full issue card. When an issue is resolved, the issue status and title is dimmed.
- **Contextual insights:** View integrated insights directly within the timeline (when available), providing extra layers of intelligence on why specific events were flagged.
- **Unified progression:** Gain immediate clarity on the speed of an attack, helping you distinguish between rapid automated threats and slow-moving lateral movement.
- **Group issues by attribute:** Sort the issues in the timeline with the **Group By** option that allows you cluster issues and insights by selected criteria, such as category, severity, or detection method.

#### 4.1.3.4.4 | Associated assets and artifacts

##### Abstract

Review the associated assets and artifacts identified in the case

This section displays the technical entities involved in the case, such as endpoints, hosts, IP addresses, and files. Assets and artifacts are organized by class, such as User, Hash, or IP. Malicious artifacts as identified by WildFire are highlighted red.

Hover over an asset or artifact to see key details about the entity. Click on an asset to see full details in the asset card.

To investigate further, click Ask AI next to an asset or artifact to open the **Agentic Assistant** with an automatically generated prompt tailored to the selected entity. You can also use the **Actions**  menu next to an asset or artifact to drill down to dedicated views or take direct actions on the asset or artifact.

##### NOTE:

If you do not have permissions to access an asset of a case (which is shown as grayed out and locked), check your scoping permissions in **Manage Users** or **Manage User Groups**.

For more information about dedicated asset and artifact views, see [Investigate artifacts and assets](#).

#### 4.1.3.4.5 | MITRE ATT&CK tactics and techniques

The MITRE ATT&CK card maps observed behaviors to relevant tactics and techniques associated with the issues linked to the case. For increased visibility, click **Insights** to include tactics and techniques from low severity insights.

To see a full breakdown by MITRE ATT&CK tactic and technique, including the number of issues in which a tactic was identified, open the full view.

##### NOTE:

This component is available for cases associated with the Security domain or custom domains.

#### 4.1.3.4.6 | Detailed View

##### Abstract



Switch to the Detailed View to see a breakdown of case information in a table-based format.

The **Detailed View** in the case card provides a table-based format and custom layouts, ensuring full backward compatibility. You can switch between the **Overview** and the **Detailed View** based on your workflow preferences.

The **Detailed View** supports deep inspection and manual analysis while maintaining access to the same underlying case data. It includes the following tabs:

Tab	Description
Issues & Insights	Displays a list of issues and insights linked to the case. Click on an issue or insight to open the issue card.
Key Assets & Artifacts	Displays asset and artifact information of the key artifacts, hosts, and users associated with the case. Hover over an icon for more information, or click the more options icon to see the available views and actions. For more information about investigating key assets and artifacts, see <a href="#">Investigate artifacts and assets</a> .
Timeline	Displays a chronological representation of issues and actions relating to the case. Each timeline entry represents a type of action that was triggered in the issue.  Issues that include the same artifacts are grouped into one timeline entry and display the common artifact in an interactive link. Click on an entry to view additional details in the Details pane. You can also filter the timeline by action type. Depending on the type of action, you can select the entry to further investigate and take action on it.
Case War Room	The Case War Room is a collection of the Active Response investigation actions, artifacts, and collaboration pieces for an issue or case. It is a chronological journal of the case investigation. You can run commands and playbooks from the War Room and filter the entries for easier viewing.  The War Room facilitates real-time investigation. Powered by ChatOps, the War Room helps you perform different tasks related to their case investigation using CLI commands. For example, running real-time security actions through the CLI, without switching consoles, and running security playbooks, scripts, and commands. For more information, see <a href="#">Use the War Room in an investigation</a>
Executions	Displays the causality chains associated with the case. On this tab, you can investigate a causality chain and take actions on a host. For more information, see <a href="#">Causality view</a> .

#### Investigate issues and insights

The Issues & Insights tab displays a table of the issues and insights associated with the case.

1. Use the toggle to switch between issues and insights, and add filters to the table to refine the displayed entries.
2. Click an issue to open the issue investigation panel. This panel provides detailed information about an issue, enables you to take actions on an issue, open the causality, and start remediation.
3. If required, you can unlink the issue from the case or link it to other related cases. Click the more options icon and select [Manage issue+Link to case](#) or [Unlink from case](#).

#### NOTE:

When an issue is resolved, it remains linked to a case. Once all of the issues in a case are resolved, the case is automatically closed.

#### Run an automation on an issue

You can run or rerun an automation on one or more issues. If there is currently an automation running on one or more of the selected issues, the Run Automation option does not appear. If an automation is running on the issue, but has been paused (for example, waiting for a user action), you can select to rerun the automation or select a new automation.

1. In the Issues & Insights tab, right-click one or more issues and click [Run Automation](#).
2. If the issues have an automation already assigned, choose [Rerun current Automation](#) or [Choose another Automation](#). If the playbooks do not have an automation assigned, select a action to run and define the action parameters.
3. Run the automation.

#### Investigate key assets and artifacts



The Key Assets & Artifacts tab displays all the case assets and artifact information of hosts, users, and key artifacts associated with the case.

1. Investigate artifacts.

In the Artifacts section, review the artifacts associated with the case. Each artifact displays, if available, the artifact information and available actions according to the type of artifact: File, IP Address, and Domain.

2. Investigate hosts.

In the Hosts section, review the hosts associated with the case. Each host displays, if available, host information and available actions.

To further investigate the host, select the host name to display the Details panel. The panel is only available for hosts with the agent installed and displays the host name, whether it's connected, along with the Endpoint Details, Agent Details, Network, and Policy information details. If the Details panel is not available, click the more options icon next to a host name to see the available options.

3. Investigate users.

In the Users section, review the users associated with the case. Each user displays, if available, the user information and available actions

#### [Investigate the case timeline](#)

The Timeline tab is a chronological representation of issues and actions relating to the case.

1. Navigate to the Timeline tab and filter the actions according to the action type.

2. Investigate a timeline entry.

Each timeline entry is a representation of a type of action that was triggered in the issue. Issues that include the same artifacts are grouped into one timeline entry and display the common artifact in an interactive link. Depending on the type of action, you can select the entry, host names, and artifacts to further investigate the action:

- Locate the action you want to investigate:
  - For Quick Actions and Case Management Actions, you can add and view comments relating to the action.
  - For Issues, click the action to open the Details panel. In the panel, go to the Issues tab to view the issues table filtered by issues ID, the Key Assets to view a list of Hosts and Users associated to the issue, and an option to add Comments.
- Select the Host name to display the endpoint data, if available.
- Select the Artifact to display the following type of information:
  - Hash artifact: Displays the Verdict, File name, and Signature status of the hash value. Select the hash value to view the Wildfire Analysis Report, Add to Block list, Add to Allow list and Search file.
  - Domain artifact: Displays the IP address and VT score of the domain. Select the domain name to Add to EDL.
  - IP address: Display whether the IP address is Internal or External, the Whois findings, and the VT score. Expand Whois to view the findings and Add to EDL.
- In action entries that involved more artifacts, expand Additional artifacts found to further investigate.

#### 4.1.3.4.7 | [Issue card](#)

##### Abstract

On the Issue card, you can see details of the selected issue and take actions on an issue.

The Issue card provides a full breakdown of an issue, helping you understand the root cause and take action through relevant evidence, remediation guidance, and response options.

The issue card supports full case investigation by retaining case context. Once you have finished reviewing an issue, close the card to return to the initial case investigation.

Each issue card adapts to the type of issue you're investigating, surfacing the most relevant information and tools at every stage of the workflow. While layouts may vary, most issues share a common set of tabs designed to support triage, investigation, and resolution.



Tab	Description
Overview	<p>Displays a description of the issue and provides key information, including:</p> <ul style="list-style-type: none"> <li>• Assignee</li> <li>• Status</li> <li>• Time at which the issue was created and updated</li> <li>• Suggested automations to run on the issue. Click the automation to open to the Work Plan tab with details of the automation.</li> <li>• Affected Assets with links to the affected asset cards</li> <li>• Cases linked to the issue</li> <li>• (For issues related to Container images) Related Affected Assets displays the assets that are related to the assets listed under Affected Assets. For example, if one of the associated assets is a container image running on a VM, the VM will be listed under this section.</li> </ul> <p>The Evidence section contains information to help you investigate the issue, such as the causality chain.</p> <p><b>NOTE:</b></p> <p>This section is context-specific and shows data according to the issue context.</p>
Issue Information	<p>Displays a summary of the issue, such as issue details , indicators, and outstanding tasks. Some fields are informational and some can be edited. Includes the following sections (depending on the layout):</p> <ul style="list-style-type: none"> <li>• ISSUE DETAILS: A summary of the issue, such as type, severity, and when the issue occurred. You can update these fields as required.</li> <li>• COMMAND AND TASK RESULTS: Lists any manual commands and playbook task results.</li> <li>• WORK PLAN: View or take action on the following: <ul style="list-style-type: none"> <li>◦ Playbook tasks: When a playbook runs, any outstanding tasks appear. You can take various actions here or in the Work Plan tab.</li> <li>◦ To-Do Tasks: An ad-hoc item that is not attached to the Work Plan. Create tasks for users to complete as part of an investigation. These are like a To-Do list that you keep in an investigation on an ad-hoc basis, rather than the Work Plan, which follows a pre-defined process. You can view or create To-Do tasks.</li> </ul> </li> <li>• NOTES: Helps you understand specific actions taken, and allows you to view conversations between analysts to see how they arrived at a certain decision. You can see the thought process behind identifying key evidence and identifying similar cases.</li> <li>• MALICIOUS OR SUSPICIOUS INDICATORS: A list of any malicious or suspicious indicators. If you have the Threat Intel add-on, you can pivot to the Indicators page, where you can take further action on the indicator.</li> <li>• INDICATORS HANDLING: Take actions on indicators from the displayed options.</li> </ul>
Technical Information	<p>Displays an overview of the information collected about the investigation, such as indicators, email information, URL screenshots, etc. When you run a playbook, the sections are automatically completed.</p>
Investigation Tools	<p>Enables you to take action on the issue, such as converting a JSON file to CSV and checking if the IP address is in CIDR.</p>
War Room	<p>A comprehensive collection of all investigation actions, artifacts, and collaboration. It is a chronological journal of the issue investigation. Each issue has a unique War Room. For information, see Use the War Room in an investigation.</p>
Work Plan	<p>A visual representation of the running playbook that is assigned to the issue. For more information, see Use the Work Plan in an investigation.</p>
Actions	<p>Recommended actions to resolve the issue.</p>



#### 4.1.3.5 | Resolve the case

##### Abstract

You can start remediating a case by reviewing the actions in the Resolution Center.

After analyzing a case, you can start remediation in the Resolution Center. This process involves executing specific tasks to address the problems identified in the case. Once the remediation tasks are completed and verified, you can officially close the case to reflect its updated status and maintain an accurate audit trail.

##### 4.1.3.5.1 | Resolution Center

##### Abstract

Review the remediation action in the Resolution Center to start resolving a case.

The **Resolution Center** is the primary workspace for managing and resolving cases. With a focused, action-oriented flow, you can focus on resolving the entire case rather than investigating isolated issues. By removing fragmented navigation, this workspace allows you to work without context switching, enabling you to open and run playbooks within the case context and quickly review the status of all tasks for all issues in the case.

The **Resolution Center** guides you toward resolution by answering the question, **What should I do next?** You can track your progress using four specialized tabs:

##### Pending

This tab acts as your to-do list for case actions. It displays any tasks waiting for execution or playbook tasks that require your input.

- **Task details:** You can view the task summary and assignee, listed in order they were created.
- **Play book execution:** Each task shows its source (Issue ID and Automation Name). You can click the Issue ID to open the issue card or click the playbook to open the workplan.

If the playbook is already in progress but requires user input, the label shows the status of the playbook. Click the label to open the Workplan and directly execute the playbook task.

##### NOTE:

Tasks that are already In Progress but still require your input will appear in both the Pending and In Progress tabs.

##### Recommended

Lists suggested playbooks and response actions to help remediate issues linked to the case.

- **Task details:** You can see details of the recommended tasks, including the name of the source that triggered the recommendation.
- **Consolidated tasks:** If the same action is recommended for multiple issues, it is only listed once. Review the labels on a task to see the issues for which the task is relevant.
- **Playbook execution:** Click a playbook to preview and execute it in the **Work Plan**. If the playbook applies to multiple issues, you can choose which issues to run it against.
- **Recommended response actions:** Click a recommended action to open a dialog with detailed steps for executing the action.

##### In Progress

Track currently running automations and remediation workflows in real time.

- **Real-time tracking:** This tab shows all active playbooks, including those in the run queue.
- **Status details:** Each record includes the playbook name, related issue, and current status (Error, Waiting, or Running).
- **Navigation:** You can click any playbook to open the Work Plan or click an Issue ID to view the associated issue card.

##### Done

This tab provides a clear audit trail of your resolution steps.

You can review a list of completed playbooks and actions. Each record includes the playbook name, the related issue, the completion time, and the final status.

##### 4.1.3.5.2 | Collaborative notes and comments

Located within the **Resolution Center**, the **Notepad** and **Comments** panels enable team-wide communication and documentation. This workspace ensures all analysts stay aligned by maintaining a continuous record of the investigation.

Capabilities include:



- **Notepad:** Record critical evidence, observations, and investigative steps to maintain a shared history for the case.
- **Comments:** Share progress updates and discuss the case with team members in real-time.

#### 4.1.3.5.3 | Resolve a case

You can resolve a case in the following ways:

- Manually on the Cases page:
  - Click the case status and select Resolved.
  - In the Resolve case dialog, select the resolution reason and leave a comment.
  - Select whether to resolve all of the issues in the case, and whether to create an exclusion.
  - Click Resolve.
- In the API, run the `Update Case` command .

#### **NOTE:**

If a case is resolved with the status `Resolved - Auto Resolved`, Cortex Cloud can reopen the case for up-to six hours if a new issue is triggered that matches the case. The six-hour period is defined by the timestamp of the last issue that was grouped into the case. After the six-hour period, any new issues are linked to a new case for a new investigation.

#### 4.1.3.5.4 | Resolution reasons for cases and issues

Abstract

Describes the resolution reasons for cases and issues.

When you resolve a case or issue, you must also specify a resolution reason. The following table describes the resolution reasons for selection.

Resolution Reason	Description
Resolved - True Positive	<p>The case or issue was correctly identified by Cortex Cloud as a real threat, and the case was successfully handled and resolved.</p> <p><b>NOTE:</b></p> <p>Cases and issues resolved as True Positive and False Positive help Cortex Cloud to identify real threats in your environment by comparing future cases and associated issues to the resolved cases. Therefore, the handling and scoring of future cases is affected by these resolutions.</p>
Resolved - False Positive	<p>The case or issue is not a real threat.</p> <p><b>NOTE:</b></p> <p>Cases and issues resolved as True Positive and False Positive help Cortex Cloud to identify real threats in your environment by comparing future cases and associated issues to the resolved cases. Therefore, the handling and scoring of future cases is affected by these resolutions.</p>
Resolved - Security Testing	<p>The case or issue is related to security testing or simulation activity, such as a BAS, pentest, or red team activity.</p>
Resolved - Known Issue	<p>The case or issue is related to an existing issue or an issue that is already being handled.</p>
Resolved - Duplicate Case	<p>The case or issue is a duplicate of another case.</p>
Resolved - Risk Accepted	<p>The case or issue is related to a known mitigation or impact.</p>



#### 4.1.3.6 | Additional case actions

##### 4.1.3.6.1 | Create a case

###### Abstract

You can manually create a new case, assign it to a specific domain, and define custom fields for the case.

###### **NOTE:**

To create a case manually, you must have View/Edit permission for Cases and Issues selected under Settings â Management â Roles â Components â Cases & Issues. Configurations â Access

You can create a case directly from the Cases page.

1. On the Cases page click New Case.
2. Under Case Details, specify the name, severity, and (Optional) description.  
The severity of a manually generated case cannot be low.
3. Under Issue Details, select the issues to link to the case, or create a new issue.

###### **TIP:**

The issues that you link to a case can be linked to multiple cases, and the issue domains do not need to match the case domain.

4. Under Issue Fields, define the following:

###### **NOTE:**

This option is only relevant for certain domains.

- MITRE ATT&CK tactics and techniques to assign to the case.
- Custom issue fields.

5. (Optional) Under Playbook, specify playbook run settings. By default, a playbook is run Automatically by trigger.

###### **NOTE:**

This option is only relevant for certain domains.

6. Click Create new case.

Each case creation generates one issue. The name, the severity, and the description of the generated issue mirrors the name, the severity, and the description of the case.

###### **NOTE:**

You can't attach files to manually created cases.

##### 4.1.3.6.2 | Merge a case

###### Abstract

You can merge cases from the Table view of the Cases page.

You can merge cases you think belong together.

1. On the Cases page, click the Display menu and switch to the Table view.
2. Select the cases you want to merge, right-click and select Merge cases.

Information about merging scores and case assignees

Case assignees are managed as follows:

- If both cases have been assigned, the merged case takes the target case assignee.
- If both cases are unassigned, the merged case remains unassigned.
- If the target case is assigned and the source case is unassigned, the merged case takes the target assignee.
- If the target case is unassigned and the source case is assigned, the merged case takes the existing assignee.
- In the merged case, all source context data is lost even if the target case does or doesn't contain context data. If the target case contains context data, that context data is preserved in the merged case.



## 4.2 | Investigation and response

### 4.2.1 | Investigate issues

#### Abstract

Cortex Cloud generates issues to bring your attention to security risks in your framework.

Issues help you to monitor and control the security of your system framework by notifying you about risks to security in your framework. Cortex Cloud generates issues from the following:

- Rules that you set up, such as vulnerability rules.
- Findings

Findings themselves are not issues, but findings that match a specific logic can generate issues.

- Integrations

Integrations enable you to ingest events, such as phishing emails, SIEM events, from third-party security and management vendors. You might need to configure the integrations to determine how events are classified as events. For example, for email integrations, you might want to classify items based on the subject field, but for SIEM events, you want to classify by event type.

#### 4.2.1.1 | Overview of the Issues page

#### Abstract

The Issues page consolidates all non-informational issues from your detection sources.

The Issues page consolidates all non-informational issues from your detection sources. By default, the Issues page displays the security issues received over the last seven days. To access the Issues page, go to Cases & Issues → Issues.

Each issue is linked to one or more cases. A case provides the full story of a problem by linking related issues, assets, and artifacts in one place. To make sure that you understand the full picture of how an issue fits into the bigger picture, we recommend that you start your investigation from the Cases page. You can see the issues linked to a case in the Issues & Insights tab of the selected case. Click on an issue to open the Issue card. For more information, see Issue card.

For issues associated with the Health domain, these issues are not linked to cases and should be investigated individually. You can also see Health domain issues on the Health Issues page. For more information, see About health issues.

#### NOTE:

Every 12 hours, the system enforces a cleanup policy to remove the oldest issues once the maximum limit is exceeded. The default issue retention period in Cortex Cloud is 186 days.

#### Standardized format of user names in issues

Cortex Cloud processes and displays the names of users in the following standardized format, also termed “normalized user”.

`<company domain>\<username>`

As a result, any issue triggered based on network, authentication, or login events displays the User Name in the standardized format in the Issues and Cases pages. This impacts every issue for Analytics and Cortex Cloud Analytics BIOC, including Correlation, BIOC, and IOC issues triggered on one of these event types.

#### Deduplicated FW issues

To reduce noise in your environment, if firewall issues with the same name and host are raised within 24 hours, the issues are deduplicated. A label indicates the number of deduplicated issues up to 1,000 issue counts, larger quantities display as 1000+.

#### Issue fields

To see a full list of issue fields and descriptions, run the following query in the Query Builder:

```
datamodel dataset = issues
```

#### 4.2.1.2 | Link or unlink issues from a case

You can link and unlink issues from cases. An issue can be assigned to more than one case, and the case domain can be different from the issue domain.

#### Link issues to a case

From the Issues page, select one or more issues that you want to link, right-click and select Manage Issue+Link to case. You can select one or more case to link the issues.



## Unlink an issue from a case

From the Issues page, select the issue that you want to unlink, right-click and select Manage Issue+Unlink from case. You can select one or more cases to unlink the issue. You cannot bulk select issues to unlink.

### 4.2.1.3 | Run an automation on an issue

#### Abstract

Save time and expense by using playbooks and Quick Actions to automatically investigate and take remedial action on issues.

You can automate issue investigation and remediation by running a playbook or Quick Action on one or more issues. Automations can help to improve efficiency by automating and standardizing your workflows, promoting consistent and effective case response and management. For example, automations can automatically remediate a case by interacting with a third-party integration or open tickets in a ticketing system such as Jira.

You can view the playbook that is running on an issue or the playbooks that have already run in the Work Plan for an issue. You can view Quick Actions in the War Room for an issue.

#### **NOTE:**

In addition to automation, some playbooks contain manual tasks that prompt the analyst for input. This enables you to enhance an automation workflow with analyst input.

You can run automations in the following ways:

Manually run a playbook or Quick Action on one or more issues

1. Right-click one or more issues in the Issues table and select Run Automation.

If there is currently an automation running on one or more of the selected issues, the Run Automation option does not appear. If an automation is running on the issue, but has been paused (for example, waiting for a user action), you can select to rerun the automation or select a new automation.

2. If the issues have an automation already assigned, choose Rerun current Automation or Select another Automation. If the issues do not have an automation assigned, Select Automation.

3. If you are not rerunning the current assigned automation, select an automation to run for the selected issue(s).

4. Click Run.

#### **NOTE:**

You can also manually select a playbook to run from the Issue Work Plan tab.

#### Apply automation rules

You can create automation rules that automatically run a playbook or Quick Action when an issue is created that meets specific criteria. For more information, see Create an automation rule.

For more information, see Automation in Cortex Cloud.

### 4.2.1.4 | Use the War Room in an investigation

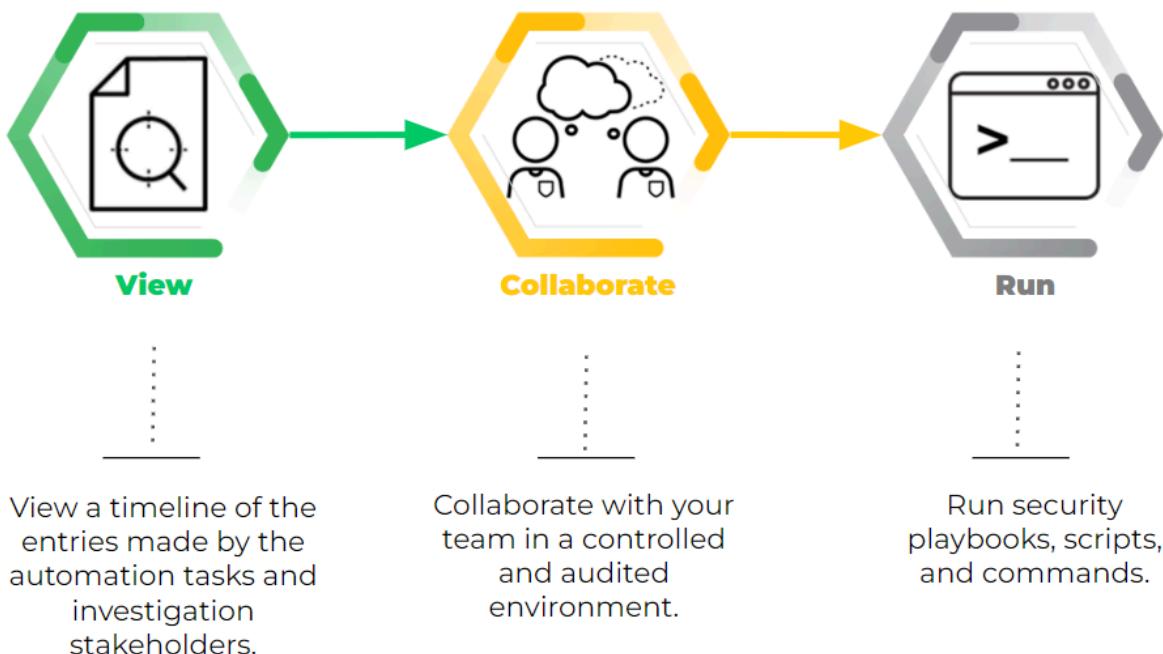
#### Abstract

Use the War Room for real-time investigation into a case, to filter war room entries, and to disable indicator notifications.

The War Room contains an audit trail of all automatic or manual actions that take place in a case or issue. A War Room is where you can review and interact with your case or issue. Cortex Cloud provides machine learning insights to suggest the most effective analysts and command-sets. Each case and issue has a unique War Room.



# The War Room: A Chronological Journal



Within Cortex Cloud, real-time investigation is facilitated through the War Room, which is powered by ChatOps. In the War Room you can take the following actions:

- Run real-time security actions through the CLI, without switching consoles
- Run security playbooks, scripts, and commands
- Collaborate and execute remote actions across integrated products
- Capture case context from different sources.
- Document all actions in one source.
- Communicate with others for joint investigations.

## NOTE:

The case War Room is usually used for communication capabilities, but unlike the issue War Room, it does not include playbook specific entries. The case War Room enables you to investigate an entire case, not just an issue.

Every case has a War Room, but every user has access, subject to permissions, to a private War Room called the Playground.

## The Playground

The Playground is a non-production environment where you can safely develop and test data, such as scripts, APIs, and commands. It is an investigation area that is not connected to a live (active) investigation.

To access the Playground, do one of the following:

- Go to Investigation & Response → Automation → Playground
- In any browser, type <https://<tenant>.<region>.paloaltonetworks.com/playground>

## TIP:

In the Playground, you can clear the context data, if needed, which deletes everything in the Playground context data, but does not affect the actual issue or case. To clear the context, run `!DeleteContext all=yes` from the CLI or click Clear Context Data while viewing the context data.

## The War Room

When you open the War Room, you can see all the actions taken on a case, such as commands and notes in several formats such as Markdown, and HTML. When Markdown, HTML, or geographical information is received, the content is displayed in the relevant format.

To view specific data entries, you can filter entries by selecting the relevant checkbox, such as:



- Chats: Shows communication between team members.
- Notes: Any entries marked as notes.
- Files: Anything uploaded to the War Room in a playbook, script, or by the analyst.
- Issue History: Any issue field that was modified.
- Commands and playbook tasks: Any actions taken by playbook tasks or run manually by the analyst.
- Tags: Any tags added to the investigation.

**NOTE:**

Cortex Cloud does not index notes and chats.

In each War Room entry, you can take the following actions:

Action	Description
Mark as note	<p>Marks the entry as a note, which can help you understand why certain action was taken and assist future decisions.</p> <p>You can also add a note by doing the following:</p> <ul style="list-style-type: none"> <li>• Upload a file to the War Room by selecting Mark as Note.</li> <li>• If the Issue Overview tab includes a NOTES section, add it to the section.</li> <li>• In a playbook task (Advanced tab)</li> </ul> <p>Tasks can be automatically added from script outputs as notes.</p> <ul style="list-style-type: none"> <li>• In the CLI by running the <code>!markAsNote entryIDs=&lt;ID of the war room entry&gt;</code> command.</li> </ul> <p>In the relevant War Room entry, click Copy to CLI to retrieve the <code>ID of the War Room entry</code>.</p> <p>When marked as a note, it is highlighted, so you can easily find them in the War Room or the Issue Overview tab.</p>
View artifact in new tab	Opens a new tab for the artifact.
Detach from task	Removes a task from the artifact.
Attach to a task	Adds a task to the artifact.
Add tags	Add any relevant tags to use that help you find relevant information.
Copy to CLI	<ul style="list-style-type: none"> <li>• ID: Entry IDs are used to uniquely identify War Room entries and take the format <code>&lt;ENTRY_IDENTIFIER&gt;@&lt;CASE_ID&gt;</code>, for example, <code>54925dc3-a972-4489-8bef-793331fa6c77@1</code>. Many out-of-the-box commands and scripts use entry IDs arguments to pass in files as inputs.</li> <li>• URL: Copy the URL which is a direct link to the War Room entry</li> </ul> <p>To find the entry ID or URL of an entry in the War Room, click on the vertical ellipsis icon at the upper right of the entry, then copy the value.</p>

Run Commands in the War Room CLI

Cortex Cloud enables you to run system commands, integration commands, and scripts from an integrated command line interface (CLI), which enables you to make comments in your case (in plain text or Markdown) and to execute automation scripts, system commands, and integration commands. This gives SOC teams the power to execute automations ad-hoc to support their investigations or make notes as they investigate cases.

In the CLI, you can run various commands by typing the following:



Action	Description
!	Runs integration commands, scripts, and built-in commands, such as adding evidence and assigning an analyst.

You can find relevant commands, scripts, and arguments with the CLI's auto-complete feature. This also includes fuzzy searching to help you find relevant commands based on keywords. If you type the exclamation mark (!) and start typing, autocomplete populates with options that might suit your needs. For example, if you want to work with tasks, type !task, and all commands and scripts that include the task in their name will display.

#### TIP:

You can use the up/down arrow buttons in the CLI to do a reverse history search for previous commands with the same prefix.

Special characters

Characters	Description
&&,   , !, {, }, [, ], (, ), ~, *, ?	To use these characters, place them within single or double quotes. An escape character \ is not required.
\, \n, \t, \r, ", ^, :, comma, and space	To use these characters, place them within single or double quotes and use an escape character \.

Common arguments

The following common arguments are available for every script run from the CLI.

Argument Name	Description
auto-extract	Whether/when to extract indicators. Possible values: <ul style="list-style-type: none"> <li><b>inline</b>: Extracts indicators within the indicator extraction run context (synchronously).</li> <li><b>outofBand</b>: Extracts indicators in parallel (asynchronously) to other actions.</li> <li><b>none</b>: Does not extract indicators (recommended for scripts with large outputs when indicator extraction is not required).</li> </ul>
execution-password	Supplies a password to run a password-protected script.
execution-timeout	Defines how long a command waits in seconds before it times out.
extend-context	Select which information from the raw JSON you want to add to the context data. For a single value: <code>contextKey=RawJsonOutputPath</code> For multiple values: <code>contextKey1=RawJsonOutputPath1::contextKey2=RawJsonOutputPath2</code>
ignore-outputs	Possible values: <code>true</code> or <code>false</code> . If set to <code>true</code> , it does not store outputs in the context (besides extend context).
raw-response	Possible values: <code>true</code> or <code>false</code> . If set to <code>true</code> , it returns the raw JSON result from the script.
retry-count	Determines how many times the script attempts to run before generating an error.
retry-interval	Determines the wait time (in seconds) between each script execution.



Argument Name	Description
using	Selects which integration instance runs the command.
using-brand	Selects which integration runs the command. If the selected integration has multiple instances, the script may run multiple times. Use the <code>using</code> argument to select a single integration instance.
using-category	Selects which category of integrations runs the command. If the selected category includes multiple integration instances, the script may run multiple times. Use the <code>using</code> argument to select a single integration instance.

#### Access attributes in the Unified Asset Inventory

Commands you run in the War Room can automatically populate parameters such as region, account id, and tags, based on asset data. Commands can reference UIA attributes for the relevant asset(s) in the issue context and use those attributes as input. The issue must contain the relevant `Asset ID`.

The syntax to reference attributes in the UAI is  `${asset.xdm.asset.attributename}`. To find the property path in the XDM data set, see the asset data card for the asset in the Inventory page. For example, to print the region for the asset, enter `!print value=${asset.xdm.asset.cloud.region}`. You can also run commands and scripts directly on the asset using  `${asset.xdm.asset}`.

#### Run commands in the Automations browser

You can view and run commands and scripts (not system commands, operations, and notifications) in the Automations Browser, by clicking  next to the CLI.

The Automations Browser enables you to run commands and all associated arguments. The scripts and commands are separated into sections such as scripts and built-in commands. In each argument, you can do the following:

- Hardcode the value
- Use a dynamic value

You can dynamically pass information into the argument by clicking the curly bracket. For example, the `EmailAskUser` command asks a user a question via email. In the `email` argument, rather than typing the user's email address, you can send it to whoever created the case.

1. In the email field, click the curly brackets.

2. In the search box, enter `created`.

3. Under CASE DETAILS click Created by.

The email argument appears as  `${alert.dbotCreatedBy}`.

4. Run the command.

An email is sent to the user who created the case.

You can use transformers and filters to filter and transform data from the command.

#### Common arguments when using the Automations browser

Argument	Description
Using	Selects which integration instance runs the command.
Extend context	Determines the wait time (in seconds) between each script execution.  For a single value: <code>contextKey=RawJsonOutputPath</code>  For multiple values: <code>contextKey1=RawJsonOutputPath1::contextKey2=RawJsonOutputPath2</code>
Ignore outputs	Does not store outputs in the context (besides extend context).
Execution timeout (seconds)	Defines how long a command waits in seconds before it times out.



Argument	Description
Number of retries	Determines how many times the script attempts to run before generating an error.
Retry interval (seconds)	Determines the wait time (in seconds) between each script execution.

#### Examples using the CLI

To run the print script with a value of "hello" and the key a from the context:

```
!Print value="hello ${a}"
```

To run the Python command returning Hello World using escape characters:

```
!py script="demisto.results(\"hello world\")"
```

To run the Python command returning Hello World using backticks:

```
!py script=`demisto.results("hello world")`
```

#### 4.2.1.5 | Use the Work Plan in an investigation

##### Abstract

A Work Plan is a visual representation of the running playbook that is assigned to a case. Use it to monitor and manage a playbook workflow.

The Work Plan is a visual representation of the running playbook assigned to the issue. Playbooks enable you to automate many security processes, such as managing your investigations and handling tickets. Work Plans enable you to monitor and manage a playbook workflow, and add new tasks to tailor the playbook to a specific investigation.

In an investigation, when you open the Work Plan tab you can see the playbook, the playbook name, and navigation tools.

By default, the Follow checkbox is checked, which allows you to see the playbook executing in real-time. The playbook moves when a task is completed.

In the Work Plan you can do the following:

Action	Description
Change the default playbook	On the left-hand side of the window, select the playbook you want to run. When changing the playbook, all completed tasks are removed and the new playbook will run. If you select playbooks several times you can view the history of which playbooks ran.
Rerun the playbook	When changing the playbook, select the current playbook to run again.
View inputs and outputs	View the inputs and outputs of each task that has run. You can't view inputs and outputs of any task that hasn't run.



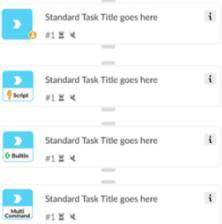
Action	Description
Manage tasks	<p>View, create, and edit a playbook task. For each task, you can do the following:</p> <ul style="list-style-type: none"> <li>Designate tasks as complete either manually or by running a script.</li> <li>Assign an owner.</li> <li>Set a due date.</li> <li>Add comments and completed notes, as required.</li> <li>View any automation exclusion policies that affected the task execution. Automation exclusion policies prevent automated remediation on critical assets specified by admins. The Policies tab only appears if the task includes a command or script affected by an automation exclusion policy.</li> </ul> <p>You can manage these tasks in the CLI by using the <code>/task</code> command.</p>
Export to a PNG	Export the Work plan to a PNG format for easy analysis.

The color coding and symbols in the Work Plan help you to easily troubleshoot errors or respond to manual steps. The following table displays the playbook tasks and icons in the Work Plan.

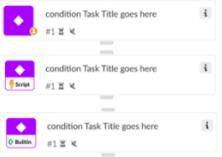
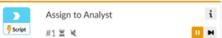
**IMPORTANT:**

A playbook will not continue its execution path if a prior task has failed; you must resolve the failed task before subsequent tasks can run.

Playbook tasks and icons in the Work Plan

Task	Description
	<p><b>Standard manual task</b></p> <p>An arrow with a light blue square background indicates a standard manual task. The following are kinds of standard tasks.</p> <ul style="list-style-type: none"> <li>Manual Standard task (no lightning bolt logo):</li> <p>These tasks are used where usually it's not possible to automate them. You can add comments, assign them to an owner, and set a due date. The analyst who is responsible for the investigation needs to complete the task before the Work Plan can continue. A user icon (User icon) indicates the task requires manual inputs.</p> <li>Automated Standard task (with lightning bolt script logo):</li> <p>A single command or script that is set to automatically run when the Work Plan execution reaches this step. Some scripts need arguments in order to run - make sure to set them up properly. If left empty, the analyst who is responsible for the investigation will need to complete them so the script will run and the Work Plan can continue.</p> <li>Automated Standard task (with Builtin logo):</li> <p>A single system command or script that is set to automatically run when the Work Plan reaches this step. Some scripts need arguments in order to run - make sure to set them up properly. If left empty, the analyst who is responsible for the investigation will need to complete them so the script will run and the Work Plan can continue.</p> <li>Automated Standard task (with Multi Command logo):</li> <p>A generic single command or script that can be used with multiple integrations is set to automatically run when the Work Plan reaches this step. Some scripts need arguments in order to run - make sure to set them up properly. If left empty, the analyst who is responsible for the investigation will need to complete them so the script will run and the Work Plan can continue.</p> </ul>



Task	Description
	<p> <b>Conditional task</b></p> <p>A diamond icon in a purple square background indicates a conditional task used as decision trees in your Work Plan. The following are kinds of conditional tasks.</p> <ul style="list-style-type: none"> <li>• Manual conditional task. A user icon (  ) indicates the task requires manual inputs.a</li> <li>• Automated conditional task (with the lightning bolt script logo).</li> <li>• Automated conditional task that uses a system script (with the Builtin logo).</li> </ul>
	<p> <b>Data collection task / Communication task</b></p> <p>The speech bubble in a turquoise background indicates a data collection task. This task prompts the receivers to respond to a multi-question form and submit replies, even if they are not Cortex users. A user icon (  ) indicates the task requires manual inputs.</p>
	<p> <b>Sub-playbook task</b></p> <p>The workflow icon in a blue background indicates that the task is a playbook nested within the parent playbook. You can view the playbook by opening the task and selecting Open sub-playbook.</p>
	<p><b>Task containing an error</b></p> <p>Scripts or sub-playbooks that have errors are designated by a red triangle. You need to open the script or sub-playbook to review the errors.</p>
	<p><b>Task containing a deprecated script or needs to be updated</b></p> <p>Scripts or sub-playbooks that have updates or are deprecated are designated by a yellow triangle. You need to update the scripts, integration commands, or sub-playbook tasks to their most current version.</p>
	<p> <b>Set to skip</b></p> <p>When a task is set to skip, the skip icon will be orange.</p>
	<p> <b>Breakpoint</b></p> <p>When the Work Plan reaches a breakpoint, the task has an orange line at the top to indicate the breakpoint.</p>
	<p> <b>Input / Output Overridden inputs or outputs</b></p> <p>When a task is set to have overridden inputs or outputs, the word Input or Output appears in orange.</p>
	<p> <b>Pending/in queue task</b></p> <p>When the Work Plan starts to run, all tasks that are about to be performed are gray.</p>
	<p> <b>Running/ in progress task</b></p> <p>A spinning circle inside the gray square indicates a running/in progress task.</p>



Task	Description
 Condition Task Title goes here #1 	 Completed task  The green square indicates a completed task.
 Standard Task Title goes here #1    Data collection Task Title goes here #1 	 Waiting task  The orange square indicates that the task is pending action.  If you hover over the icon on the top left corner, details about the reason the task is in waiting mode appear.  The user icon (  ) indicates the task requires you to open it and manually mark it as complete.  A speech bubble icon (  ) indicates the task is waiting for a questionnaire to be completed.
 Standard Task Title goes here #1    Standard Task Title goes here #1 	 Failed task  The red warning icon indicates that the task failed to complete as expected and requires manual inspection and troubleshooting. Contact your Cortex Cloud administrator.  If you hover on the icon on the top left corner, details about the specific problem appear.  If a red warning icon is paired with the clock icon (  , the task's SLA is overdue.
 Standard Task Title goes here #1 	 Skipped task  The task will look faded to indicate it was not executed. This can happen if this task was set to be skipped when an error occurs, or if it is in a branch that was not executed if a condition wasn't met.

#### Add ad-hoc tasks to the Work Plan

As part of your issue investigation, within the Work Plan you can create tasks for a specific iteration of a playbook. The task type can be an automation or another playbook. For example, within a manual task, you might need to enrich some data and run an investigation playbook.

When you create a task, add a name, automation, and description. The name and description should be meaningful so that the task corresponds to the data that you are collecting.

1. In the Cases page, select the case to update.
2. In the Issues & Insights tab, click the issue to add the task to and then click the Work Plan tab.
3. In the Work Plan, go to the task where you want to add a new task and click the + sign at the bottom right-hand corner of the task.

The ad-hoc task is added after the task you clicked.

4. Select the task type.

- Standard: Runs a single automation.
- Playbook: Runs a playbook to enhance the investigation.

The playbook functions as any playbook would and requires you to define the inputs and outputs, as well as any other details.

- Click Save.

5. To run the Work Plan again click the Run Again icon.

#### 4.2.1.6 | Issue syncing

##### Abstract

Set up integrations that mirror Cortex issues with external applications, such as Jira or ServiceNow.



You can set up integrations in Cortex Cloud that mirror Cortex issues with external applications, such as Atlassian Jira or ServiceNow. When mirroring issues (also referred to as issue syncing), you can make changes in an external application that will be reflected in Cortex Cloud, and vice versa. If an issue is mirrored with an external application, you have the following options:

- **Link the ticket to the issue:** If an issue is linked to a ticket, the ticket number is displayed in the Overview section of the issue card. You see details about the status of the ticket by clicking on the ticket number.
- **Sync changes between the issue and the ticket:** If an issue is synced to a ticket, changes are synchronized in an outbound, inbound, or bi-directional flow.

#### **NOTE:**

Multiple tickets can be linked to an issue with outbound syncing. Issues with inbound syncing can be linked to a single ticket only.

[Set up an external integration to sync with issues](#)

Before you can sync issues with external applications, you must set up and configure your integration instance. Complete the following steps:

1. Install the content pack.

1. To install from the Data Sources & Integrations page: Navigate to Settings → Data Sources & Integrations, click + Add New., and search for the relevant content pack.
- To install from Marketplace: Navigate to Settings → Configurations → Marketplace, and browse for the relevant content pack.

2. Install the relevant content pack, for example Atlassian Jira or ServiceNow.

2. Connect an integration instance.

1. Navigate to Settings → Data Sources & Integrations.
2. Search for the relevant data source (for example Atlassian Jira) select it, and click Add Instance.
3. Enter instance details in the required fields and click Connect.

[Manually create a synced ticket](#)

#### **PREREQUISITE:**

You must set up an integration before you can sync issues. For more information, see [Set up an integration for mirroring issues](#).

You can manually sync existing issues with external applications.

1. From the **Issues** page, right-click an issue and select Run Automation → Select Automation.

2. Under Quick Actions, select the action you want to configure, such as Create Jira Ticket or Create ServiceNow Ticket.

3. Define the required ticket parameters.

#### **NOTE:**

Using issue fields as variables is not currently supported.

4. Under Using, select the name of the instance to execute the command.

#### **WARNING:**

If you leave this field blank, all configured instances will be used.

5. Under Sync Configuration, the following options are displayed, depending on your selection:



- Link to issue: select this option if you want the issue to be linked to the created ticket. You must check this option if you want to sync the issue with the ticket.
- Sync Direction: select the syncing configuration:
  - Inbound: Sync changes from the external ticket with the Cortex Cloud issue.
  - Outbound: Sync changes from the Cortex Cloud issue with the external ticket.
  - Bi-directional: Sync changes in both directions.
  - None: Do not sync changes between the Cortex Cloud issue with the external ticket. If you select this option, the tickets are still linked, but changes are not synced. You can update this option at any time to start syncing.
- Define the inbound and/or outbound sync profiles.

Depending on the selected option, select sync profiles that define field mapping between the issue and the external ticket. You can use the default sync profiles or you can create custom profiles. For more information about sync profiles, see Create a sync profile.

**NOTE:**

You can only define a single inbound profile. If you change the inbound sync profile the current profile is overwritten.

You can define multiple outbound profiles; one issue can update multiple tickets.

6. Click OK.

After ticket creation, the ticket number is shown in the Issue card. Click on the ticket number to see details about the created ticket and syncing configuration. In addition, the execution is recorded in the War Room tab. If there is an error in the requested action, you can see details in the audit.

7. View or edit the syncing configuration. For more information, see View, update, or resolve a ticket.

Example 16.

The following example shows an automation run on an issue to create a ServiceNow ticket that is synced in an outbound flow with the ticket.

Select an Automation to run on selected issue 430, "Amazon EC2 instance exposed to the public internet" ⓘ

SET ACTION PARAMETERS

Create ServiceNow Ticket

Description\* ⓘ

EC2 instance 'i-065g8973df9e7vh68' in AWS is exposed to the internet ⓘ

Severity\* ⓘ

1 - High ⓘ

Short Description\* ⓘ

Instance ID: 'i-065g8973df9e7vh68' exposed to the internet ⓘ

Ticket Type\* ⓘ

incident ⓘ

Using

ServiceNow ⓘ

+ Set optional parameters ⓘ

Sync Configuration

Link to issue ⓘ

Sync Direction ⓘ

Outbound ⓘ

Outbound Profile ⓘ

Default ServiceNow V2 Outbound ⓘ

Cancel Ok



You can run the following command in the War Room to create an external ticket and define the syncing configuration:

```
!jira-create-issue-quick-action summary=<summary> project_key=<key> issue_type_name=<type>
description=<description> using=<instance> mirroring_link_to_object="true"
mirroring_sync_direction=<syncDirection> mirroring_outbound_profile_id=<profileID>"
```

#### TIP:

You can find a sync profile ID under Settings à Configurations à Object Setup à Issues à Sync Profiles. By default the ID field is not displayed in the table. Click the three dot menu and add it to the table layout.

Example 17.

The following example creates a Jira Bug ticket for the Project Key SCRUM, with an Outbound sync configuration:

```
!jira-create-issue-quick-action summary="Restrict ingress on AWS Network ACLs for admin ports 22 and 3349"
project_key="SCRUM" issue_type_name="Bug" description="We identified that multiple AWS Network ACLs are
allowing inbound (ingress) traffic on admin ports" using="JiraV3" mirroring_link_to_object="true"
mirroring_sync_direction="OUTBOUND" mirroring_outbound_profile_id="h8e14996-8695-5396-9g87-f08suu907486"
```

Create an automation rule for syncing issues with external tickets

#### PREREQUISITE:

You must set up an integration before you can sync issues. For more information, see Set up an integration for mirroring issues.

You can set up automation rules that create external tickets when certain issues occur and define the syncing configuration for transferring data between the issues and tickets.

1. Go to Investigation & Response à Automation à Automation Rules.
2. Click Add Automation Rule.
3. Enter a name and description for the rule.
4. Select whether to enable the rule after creation.
5. Under Rule Conditions, define the WHEN, and IF conditions. For more information about rule conditions, see Create an automation rule.
6. Under THEN select the desired automation, such as Create Jira Ticket and complete the following fields:

1. Define the required ticket parameters.

#### NOTE:

Using issue fields as variables is not currently supported.

2. Under Using, select the name of the instance to execute the command.

#### WARNING:

If you leave this field blank, all configured instances will be used.

3. Under Sync Configuration, the following options are displayed, depending on your selection:

- Link to issue: select this option if you want the issue to be linked to the created ticket. You must check this option if you want to sync the issue with the ticket.
- Sync Direction: select the syncing configuration:
  - Inbound: Sync changes from the external ticket with the Cortex Cloud issue.
  - Outbound: Sync changes from the Cortex Cloud issue with the external ticket.
  - Bi-directional: Sync changes in both directions.
- None: Do not sync changes between the Cortex Cloud issue with the external ticket. If you select this option, the tickets are still linked, but changes are not synced. You can update this option at any time to start syncing.

- Define the inbound and/or outbound sync profiles.

Depending on the selected option, select sync profiles that define field mapping between the issue and the external ticket. You can use the default sync profiles or you can create custom profiles. For more information about sync profiles, see Create a sync profile.

#### NOTE:

You can only define a single inbound profile. If you change the inbound sync profile the current profile is overwritten.

You can define multiple outbound profiles; one issue can update multiple tickets.

4. Click OK.



If a ticket is created, the ticket number is shown in the Issue card. You can click on the ticket number to see details about the created ticket and syncing configuration. In addition, the execution is recorded in the War Room tab. If there is an error in the requested action, you can see details in the audit.

#### 7. Click Create.

The rule is added to the Automation Rules page. If required, drag to reorder the rules.

#### Example 18.

The following example shows an automation rule that creates a Jira ticket with bi-directional syncing when a Critical Posture issue is triggered.

The screenshot shows the 'Create New Automation Rule' interface. The rule is named 'Create Jira ticket for Critical Posture issues'. It has a description: 'Create a Jira ticket with bi-directional syncing for Critical Posture issues'. The status is enabled. The rule conditions are: WHEN the following trigger occurs - 'Issue is created'; IF the following conditions match - '(issue domain = Posture AND severity = Critical)'; THEN perform the following action - 'Create Jira Ticket'. There is a 'Change' button next to the action.

[View, update, or resolve a ticket](#)

Once you have set up ticket syncing, you can view, update and resolve the issue and external ticket as required. The changes are reflected according to the defined syncing configuration.

#### 1. To open the ticket details, in the Overview section of the issue card, click on the external ticket number.

A panel opens with details of the external ticket. You can see the external ticket number, the sync configuration, and details of the ticket.

#### 2. Open the linked ticket by clicking on the external ticket number in the panel.

#### 3. Update the fields as required.

The updates are logged in the ticket history.

#### **NOTE:**

- The inbound syncing flow runs every two minutes, and the outbound syncing flow runs every five minutes.
- In a bi-directional set-up, if the same field is updated in both tickets, the most recently updated value is used.
- In the external ticket, the logged history shows updates to the ticket. The user name that is logged with the history reflects the user token of the user who configured the data source.

#### 4. Resolve the ticket.

#### **NOTE:**

After an issue is resolved, ticket syncing remains active for up-to seven days. Therefore, you still update, change, or reopen the issue or external ticket and the tickets will continue to sync.

[Edit or disable ticket syncing](#)

You can change the syncing configuration between a ticket and an issue from the issue card.

#### 1. In the Overview section of the issue card, click on the external ticket number.

A panel opens with details of the ticket.



2. Click on the settings icon.

3. Under Sync Configuration, change the syncing configuration as required.

**NOTE:**

If you change the selected inbound sync profile, the original sync profile is immediately overwritten.

4. To disable ticket syncing, take one of the following actions:

- To pause ticket syncing, set the Sync Direction value to None.

This temporarily stops the tickets from syncing, but the tickets are still linked. You can update the syncing configuration at any time to resume ticket syncing.

- To unlink the tickets, uncheck Link to issue.

This action is not reversible.

5. Click Save.

Add playbook tasks to create external tickets

**PREREQUISITE:**

You must set up an integration before you can sync issues. For more information, see [Set up an integration for mirroring issues](#).

You can add a playbook task that creates external tickets and defines the syncing configuration.

1. Open a new or existing playbook and add a new task.

2. Select the Task Type and add a task name.

3. Select one of the following scripts:

- `jira-create-issue-quick-action (Jira V3)`
- `servicenow-create-issue-quick-action (Jira V3)`

4. Under Inputs, add fields for the ticket parameters.

Example 19.

This example defines fields for a Jira ticket.

- Summary: AWS Network ACLs allow ingress traffic on Admin ports
- Project Key: SCRUM
- Issue Type: Bug
- Description: We identified that multiple AWS Network ACLS are allowing inbound (ingress) traffic on admin ports

5. Under Sync Configuration, the following options are displayed, depending on your selection:

- Link to issue: select this option if you want the issue to be linked to the created ticket.

- Sync Direction: select the syncing configuration:

- Inbound: Sync changes from the external ticket with the Cortex Cloud issue.
- Outbound: Sync changes from the Cortex Cloud issue with the external ticket.
- Bi-directional: Sync changes in both directions.
- None: Do not sync changes between the Cortex Cloud issue with the external ticket.

- Define the inbound and outbound sync profiles.

Depending on the selected option, select sync profiles that define field mapping between the issue and the external ticket. You can use the default sync profiles or you can create custom profiles. For more information about sync profiles, see [Create a sync profile](#).

**NOTE:**

You can only define a single inbound profile. If you change the inbound sync profile the current profile is overwritten.

You can define multiple outbound profiles; one issue can update multiple tickets.

6. Save the playbook.



## Limitations of issue mirroring

Consider the following limitations of issue mirroring:

- Issue syncing requires the latest version of Atlassian Jira (V3) and ServiceNow (V2).
- Issue syncing is currently supported in Atlassian Jira (V3) and ServiceNow (V2) only.
- You can sync up to 50K objects.
- You can create a maximum of 200 sync profiles.
- Cortex Cloud supports up-to 100 Inbound syncs across all synced tickets over a two-minute time period. Any additional changes beyond this limit will not be synced.
- If a connector instance is deleted or disabled, tickets are no longer synced and external ticket information is not available.
- Custom statuses are not supported.
- Currently, a specific set of fields is supported.

### 4.2.1.7 | Issue investigation actions

#### 4.2.1.7.1 | Copy issues

Abstract

You can copy an issue into memory.

You can copy issue text into memory and paste it into an email. This is helpful if you need to share or discuss a specific issue with someone. If you copy a field value, you can also paste it into a search or begin a query.

How to copy an issue value

1. From the Issues page, right-click the issue you want to send.

2. Select one of the following options:

- Copy text to clipboard
- Copy entire row
- Copy issue URL

Cortex Cloud saves the copied text to memory.

3. Paste the URL into an email or use it as needed to share the information.

#### 4.2.1.7.2 | Update issue fields

Abstract

Use a playbook, script, or command to update issue fields.

You can update issue fields by running the `setIssue` and `setIssueStatus` commands in the CLI, in a script, or a playbook task.



- **setIssue**: Sets values for specific issue fields. The supported fields are presented in the list of arguments.

Example 20. Examples of the setIssue command in the CLI

The following examples show how to run the **setIssue** command in the CLI. You can run CLI commands in the War Room. When you start typing the CLI provides the available options and if you select an enum field, the CLI provides the available values.

- To change the issue severity to **high**, run

```
!setIssue severity=high
```

- To change the issue severity to **high** and star the issue, run

```
!setIssue severity=high starred=true
```

- **setIssueStatus**: Sets the status or resolution value for an issue. This command supports the **status** argument, which presents a list of status and resolution type values. The selected status is set in the **custom\_status** field.

If you specify a resolution status, the issue is closed and the **resolution\_status** and **closeReason** fields are updated to the same value as the **custom\_status** field. If you specify a New, Reopened, or Under Investigation status, the issue remains open and the **resolution\_status** and **closeReason** fields are empty.

#### TIP:

You can create custom issue statuses and resolution reasons, and use the **setIssueStatus** command to set these custom statuses for issues.

For example, when a user starts investigating an issue, the issue status is automatically changed from New to Under Investigation. In some cases, it is useful to create an interim status, such as Triage. After you create the custom status, the new status will be available for selection. To create a custom status, follow the instructions in [Create custom case statuses and resolution reasons](#).

Example 21. Examples of using the setIssueStatus command in the CLI

The following examples show how to run the **setIssueStatus** command in the CLI. You can run CLI commands in the War Room. When you start typing, the CLI provides the available options and if you select an enum field, the CLI provides the available values.

- To change the issue status to **Resolved - Known Issue**, run

```
!setIssueStatus status="Resolved - Known Issue"
```

- To change the issue status to custom status **Triage**, run

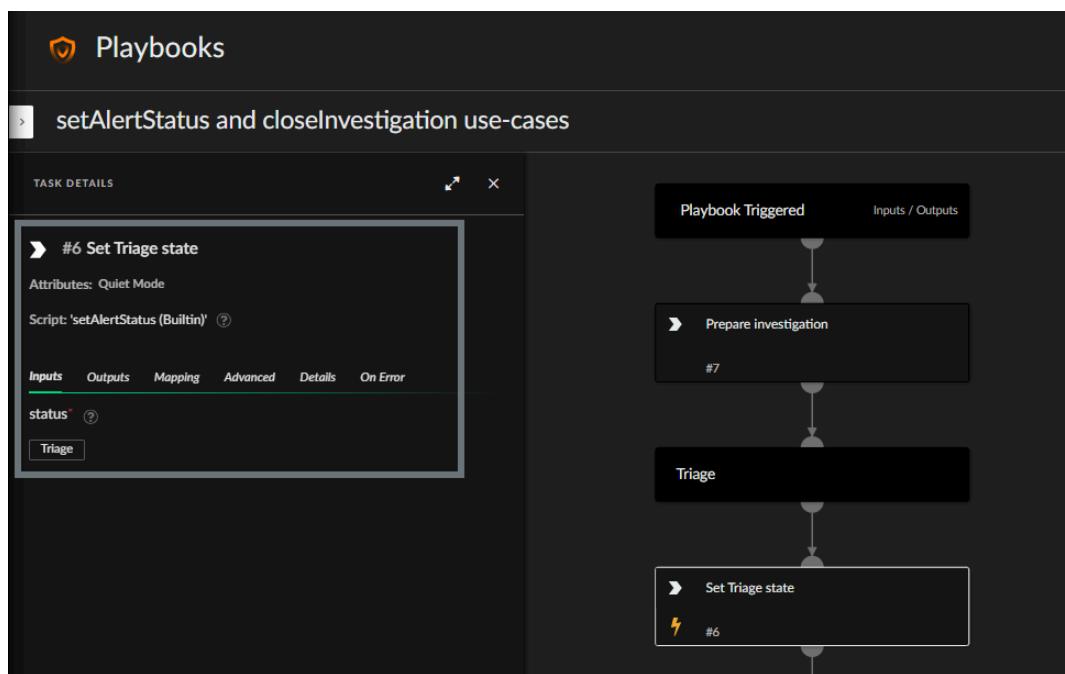
```
!setIssueStatus status=Triage
```

#### NOTE:

You must create a custom status before you can select it.

Example 22. Example of using the setIssueStatus command in a playbook

The following example shows how the **setIssueStatus** command can be used in a playbook task. In this example, the task sets a custom issue status (Triage). The custom issue status was created before setting up the playbook.



#### 4.2.1.7.3 | Export issue details to a file

##### Abstract

You can review issue details offline by exporting issues to a TSV file.

To archive, continue investigation offline, or parse issue details, you can export issues to a tab-separated values (TSV) file:

1. From the Issues page, adjust the filters to identify the issues you want to export.
2. When you are satisfied with the results, click the download icon ().

The icon is grayed out when there are no results.

Cortex Cloud exports the filtered result set to the TSV file.

#### 4.2.1.7.4 | Exclude an issue

##### Abstract

You can exclude issues that are not deemed to be a threat.

During the process of triaging and investigating issues, you might determine that an issue does not indicate threat. You can choose to exclude the issue, which hides the issue, excludes it from cases, and excludes it from search query results.

You can also set up issue exclusion rules that automatically exclude issues that match certain criteria. For more information, see Issue exclusions.

##### How to exclude an issue

1. From the Issues page, locate the issue you want to exclude.
2. Right-click the row, and select Manage Issue → Exclude Issue.

A notification displays indicating the exclusion is in progress.

#### 4.2.1.7.5 | Query case and issue data

##### Abstract

You can run queries on case and issue data with the **cases** and **issues** datasets.

Cortex Cloud uses Cortex Query Language (XQL) as the primary language for searching, analyzing, and transforming security data. XQL allows for highly efficient querying across vast amounts of security telemetry, such as:

- Threat hunting: Proactively search your entire environment for malicious activity, anomalies, and indicators of compromise (IOCs). Formulate queries to look for specific patterns of behavior that might indicate an ongoing attack, even if no alert has been triggered.
- Investigation: When a case or issue is generated, XQL allows security analysts to drill down into the underlying data, understand the full scope of an attack, identify affected assets, and trace the attacker's actions.
- Forensics: Extract detailed information about past events for post-incident analysis and compliance audits.
- Reports and dashboards: Create custom reports and dashboards to visualize security posture, track key metrics, and communicate insights to stakeholders.

To view and use sample investigative queries, such as the Top Unresolved High Severity Cases query, go to Investigation & Response → Search → Query Builder → XQL → Query Library. For more information about using XQL, see Cortex Cloud XQL.

You can query case and issue data in the **cases** and **issues** datasets. When using the **issues** dataset, keep in mind the following:

- Informational issues are not included in this dataset.

The **issues** dataset is categorized by domain. To query only security issues, use the following XQL:

```
dataset = issues | filter issue_domain = "SECURITY"
```

To query only posture issues, use the following XQL:

```
dataset = issues | filter issue_domain = "POSTURE"
```



## 4.2.2 | Review findings

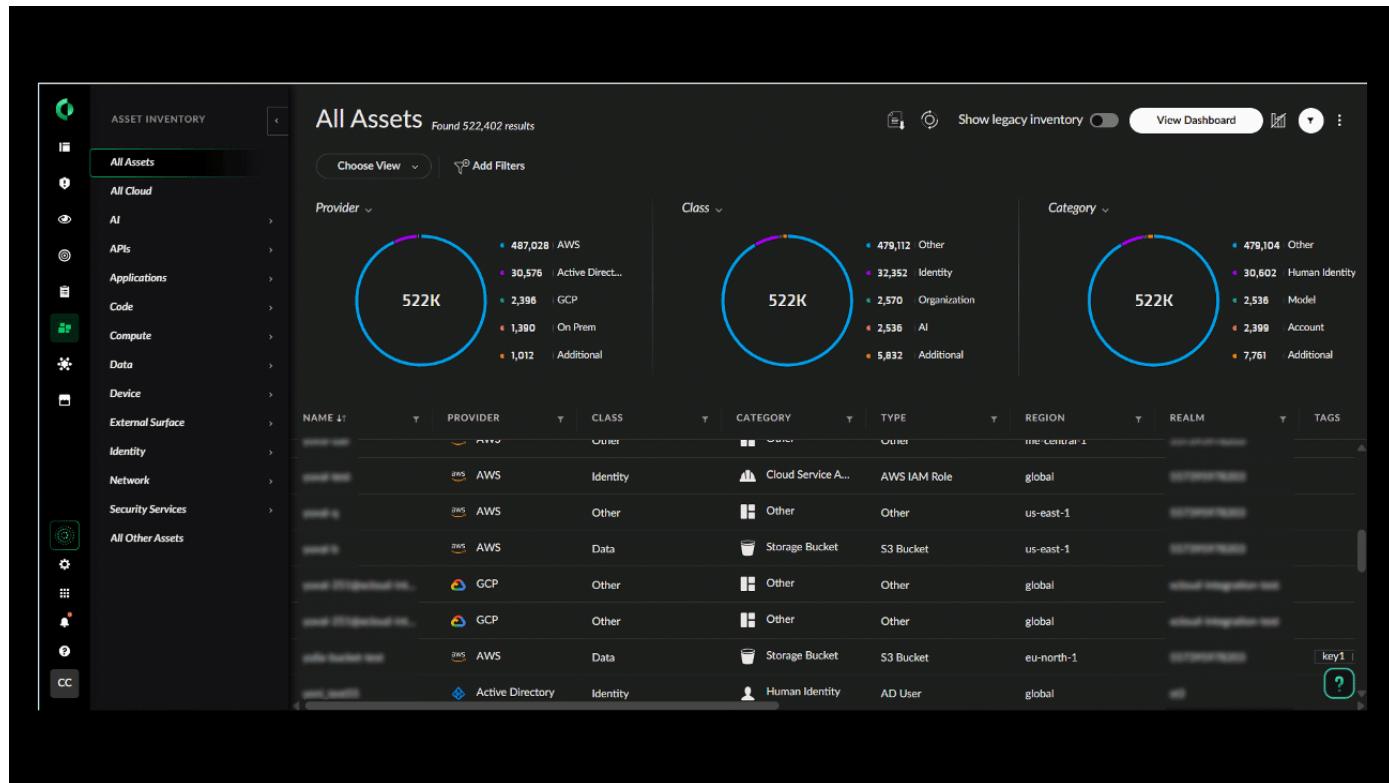
### Abstract

Review findings for an asset to gain insights into an asset's posture status.

Findings provide knowledge about an asset by leveraging the data we collect from various sources. This process helps build a more accurate and comprehensive understanding of the asset's current state, including its configuration, behavior, and context within the environment. Additionally, findings provide visibility into potential exposures and vulnerabilities, contributing to a clearer assessment of the asset's risk level. By continuously analyzing and updating findings, we can maintain an up-to-date view of the asset's security posture and support more informed decision-making for detection, prioritization, and remediation efforts. For more information, see Findings and events.

Click on a finding from any location in the UI to open the findings card. For more information, see Findings card. To view all findings, go to Issues+Findings table. You can also see findings for a specific asset by opening the asset card.

 Show me more



### Types of findings

The following table describes the different types of findings:

#### NOTE:

Type	Description
Code	Discovery of security issues within application source code, such as bugs, logic flaws, and insecure coding practices.
Compliance	Discovery of compliance violations that do not adhere to the security standards for your organization.
Configuration	Discovery of incorrect settings or configurations in systems, applications, or devices that reduce the environment's resilience and increase the potential for compromise.
Data	Discovery of sensitive data misuse, secrets, and shadow data.
Identity	Discovery of suspicious user identities, highlighting authentication and access control to prevent unauthorized access and minimize the risk of over-permissive access rights that could lead to security breaches.



Type	Description
Malware	Discovery of malicious files within cloud workloads.
Posture	Discovery of posture risks that might expose critical assets to potential cyberattacks and operational disruption.
Vulnerability	Discovery of weaknesses or flaws in software or hardware that attackers can exploit to gain unauthorized access, disrupt operations, or steal data.

#### Set up rules to trigger issues from findings

Findings themselves are not issues, but findings that match a specific logic can generate issues. You can also set up your own policies and rules to trigger issues when the following types of findings are recorded:

- Compliance, Malware, or Secrets findings, for more information, see Cloud workload policies and rules.
- Vulnerability findings, for more information, see Vulnerability policies.

#### Query findings data

You can query finding data in the `findings` data set.

#### Example 23.

The following query searches for all findings for AssetA:

```
dataset = findings | filter xdm.finding.asset_name = "AssetA"
```

#### 4.2.2.1 | Findings card

##### Abstract

The Findings card provides information about a selected finding, including the Finding ID, category, and associated asset.

The Findings card displays information about the selected finding. On this card you can see the following information.

##### **NOTE:**

The information in this card is context specific, therefore some sections are not available for all findings.

Section	Description
Header	Finding ID, name, category (such as, Vulnerability or Compliance), time created, and time updated.
Description	Reason that the finding was created.
Impact	Information about the possible impact of the finding on your system.
Asset	Name and type of the affected asset. To investigate the asset, click on the asset name to open a new tab displaying the asset card.
Evidence	Visualization of the finding in your environment.
Data	Normalized finding data.



#### 4.2.3 | Investigate artifacts and assets

##### Abstract

You can investigate specific artifacts and assets on dedicated views related to IP address, Network Assets, and File and Process Hash information.

From the Cases view, open the Key Assets & Artifact tab to see the assets and artifacts that are associated with the case, including hosts, IP addresses, and users. Icons represent properties of the artifacts and assets. Hover over an icon for more information. Click the more options icon to drill down in dedicated views, or take actions on the asset or artifact. The Key Assets & Artifact tab shows the following information:

- Artifacts

To aid you with threat investigation, Cortex Cloud displays the WildFire-issued verdict for each key artifact in a case. To provide additional verification sources, you can integrate external threat intelligence services with Cortex Cloud.

- Assets

Displays Hosts and Users details. For hosts with a Cortex XDR agent installed, click on the host name to see more information in the Details panel.

##### 4.2.3.1 | Investigate an IP address

##### Abstract

Investigate cases, connections, and threat intelligence reports related to a specific IP address on the IP View.

Drill down on an IP address on the IP View. On this view, you can investigate and take actions on IP addresses, and see detailed information about an IP address over a defined 24-hour or 7-day time frame. In addition, to help you determine whether an IP address is malicious, the IP View displays an interactive visual representation of the collected activity for a specific IP address.

##### How to investigate an IP address

1. Open the IP View.

Right-click the IP address that you want to investigate and select Open IP View.

2. In the left panel, review the overview of the IP address.

The overview displays network operations, cases, actions, and threat intelligence information relating to the selected IP address, and provides a summary of the network operations and processes related to the IP address.

The displayed information and available actions are context-specific.

- a. Add an Alias or Comment to the IP address.

- b. Review the location of the IP address. By default, Cortex Cloud displays information on whether the IP address is an internal or external IP address.

- Externalâ€ Connection Type: Incoming displaying IP address is located outside of your organization. Displays the country flag if the location information is available.
- Internalâ€ Connection Type: Outgoing displaying IP address is from within your organization. The XDR Agent icon is displayed if the endpoint identified by the IP address had an agent installed at that point in time.

- c. Identify the IOC severity.

The color of the IP address value is color-coded to indicate the IOC severity.

- d. Review threat intelligence for the IP address.

Depending on the threat intelligence sources that are integrated with Cortex Cloud, the following threat intelligence might be available:

- Virus Total score and report

##### NOTE:

Requires a license key. Select Settings â€“ Configurations â€“ Integrations â€“ Threat Intelligence.

- Whois identification data for the specific IP address.

- e. Review the related cases.

Recent Open Cases lists the most recent cases that contain the IP address as part of the caseâ€ s key artifacts, according to the Last Updated timestamp. If the IP address belongs to an endpoint with a Cortex XDR agent installed, the cases are displayed according to the hostname rather than the IP address. To dive deeper into a specific case, select the case ID.

3. In the right-hand view, use the filter criteria to refine the scope of the IP address information that you want to visualize in the map.

In the Type field, select Host Insights to pivot to the Asset View of the host associated with the IP address, or select Network Connections to display the IP View of the network connections made with the IP address.



#### 4. Review the selected data.

- Select each node for additional information.
- Select Recent Outgoing Connections to view the most recent connections made by the IP address. Search all Outgoing Connections to run a Network Connections query on all the connections made by the IP address.

##### 4.2.3.2 | Investigate an asset

###### Abstract

Investigate host assets and view host insights on the Asset View.

Drilldown on an asset on the Asset View. On this view you can investigate host assets, view host insights, and see a list of cases related to a host.

###### **NOTE:**

The Asset view is available for hosts with a Cortex XDR agent installed.

###### How to investigate an asset

###### 1. Open the Asset View.

Identify a host with a Cortex XDR agent installed and select Open Asset View.

###### 2. In the left panel, review the overview of the host asset.

The overview displays the host name and any related cases.

- a. Add an Alias or Comment to the host name.

- b. Review the related cases.

Recent Open Cases lists the most recent cases that contain the host as part of the case's key artifacts, according to the Last Updated timestamp. To dive deeper into a specific case, select the Case ID.

###### 3. In the right hand view, use the filter criteria to refine the scope of the host information that you want to display.

In the Type field, select one of the following:

- Host Insights: View a list of the host artifacts.
- Network Connections: Pivot to the IP view displaying the IP addresses associated with the host.
- Host Risk View: View insights and profiling information. Available with the Identity Threat Module.

###### 4. Review the data.

Select Run insights collection to initiate a new collection. The next time the Cortex XDR agent connects, the insights are collected and displayed.

###### 5. Perform actions on the host.

##### 4.2.3.3 | Investigate a file and process hash

###### Abstract

Investigate cases, actions, and threat intelligence reports related to a specific file or process hash on the Hash View.

Drilldown on a file or process hash on the Hash View. On this view you can investigate and take actions on SHA256 hash processes and files, and see information about a specific SHA256 hash over a defined 24-hour or 7-day time frame. In addition, you can drill down on each of the process executions, file operations, cases, actions, and threat intelligence reports relating to the hash.

###### How to investigate a file or process hash

###### 1. Open the Hash View.

Identify the file or process hash that you want to investigate and select Open Hash View.

###### 2. In the left panel, review the overview of the hash.

- a. Review the signature of the hash, if available.

- b. Identify the WildFire verdict.

The color of the hash value is color-coded to indicate the WildFire report verdict:



WildFire color key

- Blue → Benign
- Yellow → Grayware
- Red → Malware
- Light gray → Unknown verdict
- Dark gray → The verdict is inconclusive

c. Add an Alias or Comment to the hash value.

d. Review threat intelligence for the hash.

Depending on the threat intelligence sources that are integrated with Cortex Cloud, the following threat intelligence might be available:

- Virus Total score and report.

**NOTE:**

Requires a license key. Go to [Settings](#) → [Configurations](#) → [Integrations](#) → [Threat Intelligence](#).

- IOC Rule, if applicable, including the IOC Severity, Number of hits, and Source according to the color-coded values:
- WildFire analysis report.

e. Review if the hash has been added to:

- Allow List or Block List.
- Quarantined, select the number of endpoints to open the Quarantine Details view.

f. Review the recent open cases that contain the hash as part of the case's Key Artifacts according to the Last Updated timestamp. To dive deeper into specific cases, select the Case ID.

3. In the right hand view, use the filter criteria to refine the scope of the IP address information that you want to visualize.

Filter criteria

Filter	Description
Event Type	Main set of values that you want to display. The values depend on the selected type of process or file.
Primary	Set of values that you want to apply as the primary set of aggregations. Values depend on the selected Event Type.
Secondary	Set of values that you want to apply as the secondary set of aggregations.
Showing	Number of Primary and Secondary aggregated values to display.
Timeframe	Time period over which to display your defined set of values.

4. Review the selected data.

To view the most recent processes executed by the hash, select Recent Process Executions. To run a query on the hash, select Search all Process Executions.

5. (Optional) Perform actions on the hash.

4.2.3.4 | [Investigate a user](#)

Abstract



Investigate user assets associated with your cases.

Drill down on a user in the User Risk View or the User View. In this view Cortex Cloud aggregates all of the data collected for a user, displays the information in graphs and tables, and provides further drilldown options for easy investigation. Cortex Cloud uses Identity Analytics to aggregate information on a user and displays insights about the user.

You can take the following actions to investigate a user:

- Assess the user's behavior and score.
- Star the user to be included in the watchlist.

How to investigate a user

1. Right-click a user name and select Open User Card.

**TIP:**

You can also see a list of all users under Inventory â† Assets â† Asset Scores.

2. Select the timeframe to view the user's details.

**NOTE:**

Cortex Cloud normalizes and displays case and issue times in your time zone. If you're in a half-hour time zone, the activity in the Issues & Insights Heatmap is displayed in the whole-hour time slot preceding it. For example, if you're in a UTC +4.5 time zone, the time displayed for the activity will be UTC +4.5, however, the visualization in the Issues & Insights Heatmap will be in the UTC +4 slot.

3. Investigate the user.

User View

Review the sections of the User View. Depending on your permissions, some information might be limited by your scope.

1. In the left panel, review the overview of the user. The displayed information is aggregated by Cortex Cloud from cases, Workday, and Active Directory data.

The User Score displays the score that is currently assigned to the user and is updated continuously as new issues are associated with cases.

2. Review the Score Trend graph.

The graph is based on new cases created within the selected time frame, and updates on past cases that are still active. The straight line represents the user score, which is based on the scores of the cases associated with the user.

Select a score to display in the Cases table, the cases that contributed to the total user score on a specific day.

3. Click a score to drill down on the score for a specific day. Alternatively, review the user information for the selected timeframe (Last 7D, 30D, or custom timeframe).

The widgets in the right panel reflect the selected timeframe.

4. Review the Related Cases for the selected timeframe or score selected in the Score Trend graph. If you are drilling down on a score, you can see the cases that contributed to the total score on the selected day. Review the following data:

- The Status column provides visibility into the reason for the score change. For example, if a case is resolved, its score will decrease, bringing down the host score.
- The Points column displays the risk score that the case contributed to the host score. The points are calculated according to SmartScore or Case Scoring Rules.

5. Review the following additional widgets:

- User Associated Insights
- Top 5 Hosts Logged Into
- Top 5 Authentication Target Hosts
- Top 5 Authentication Source Hosts
- Recent Login
- Recent Authentications

#### 4.2.4 | Cortex Assistant

Abstract



Cortex Assistant is designed to streamline processes by simplifying case triaging, investigation, and remediation. It enables you to seamlessly uncover new insights on hashes, hosts, and more. You can get tailored suggestions, and run actions in natural language from anywhere without losing context.

Cortex Assistant is an innovative tool specifically developed to streamline various processes, including case triaging, investigation, and remediation. By utilizing Cortex Assistant, you can uncover valuable insights on a wide range of entities such as hashes, hosts, and more. Its primary objective is to simplify these tasks, allowing for a more efficient workflow and enhanced productivity.

#### **NOTE:**

If you are in an eligible region and have enabled the Cortex Agentic Assistant, the Cortex Agentic Assistant replaces the Cortex Assistant. The Cortex Assistant is available if you do not have access to the Cortex Agentic Assistant based on the tenant region or you have not enabled it. For more information, see [Cortex Agentic Assistant](#).

One of the key features of Cortex Assistant is its ability to provide personalized suggestions based on your specific needs and context. This helps you find the most relevant information and solutions quickly and effortlessly.

Cortex Assistant allows users to execute commands using natural language from anywhere within the interface. This means that users can interact with the tool seamlessly, without losing their train of thought or context.

#### Access Cortex Assistant

Cortex Assistant is conveniently accessible from the main menu in the left pane, ensuring easy navigation and usage. Alternatively, you can right-click on specific entities, such as an asset name or IP address, and select Open in Cortex Assistant to immediately open the Cortex Assistant with a focus on that entity.

To increase usability, you can create a personalized keyboard shortcut: Settings → Configurations → Server Settings → Keyboard Shortcuts and choose the shortcut you want to use. You can use this shortcut anytime, from anywhere within Cortex Cloud, to instantly open Cortex Assistant. If you highlight an entity and open Cortex Assistant with the keyboard shortcut, it will open with a focus on that entity.

#### What can Cortex Assistant do for you?

- Perform investigations of entities such as cases, hashes, hosts, domains, IP addresses, and users, using advanced XQL queries and activate tailored responses.
- Use Cortex Assistant as a navigation tool to search for information, perform common investigation tasks, or initiate response actions.

#### Responsible AI

Cortex Assistant is developed in accordance with responsible AI principles. Customer data is not used to train the AI models, and your data is private and secure. For added security, user prompts are processed within the tenant's region. Safety and security measures include user confirmation for write actions and adherence to RBAC permissions. At the same time, explainability is maintained by providing the logic behind answers and offering a feedback option for user opinions.

#### 4.2.4.1 | Cortex Assistant layout

##### Abstract

Understand the main components in Cortex Assistant: search bar, insights and suggestions, action log, and feedback.

Cortex Assistant consists of the following primary components:

##### Search bar

The search bar is located at the top of the Cortex Assistant screen. This is where you interact with Cortex Assistant, providing a centralized location to access assistance, obtain insights, and navigate the platform efficiently.

##### Insights and suggestions

You can find Cortex Assistant's responses to your queries in the insights and suggestions area. The insights section includes all the important information Cortex Assistant can provide in response to your query.

Below that, Cortex Assistant offers suggestions, which are divided into three columns, each with specific functionalities:

- Investigate: Choose from the recommended relevant questions you can ask to further your investigation. Responses leverage advanced XQL queries.
- Respond: Take action by running recommended playbooks or scripts, enabling you to initiate response actions based on Cortex Assistant's suggestions.

#### 4.2.4.2 | Cortex Assistant capabilities

##### Abstract

Understand Cortex Assistant's capabilities and how to use them.



## Entity investigation

The Cortex Assistant conducts investigations on entities entered in the search bar. It can investigate a range of entities, including hosts, users, hashes, domains, IP addresses, and cases. To initiate an investigation, enter the entity name in the search bar or ask specific questions about the entity, such as "What are the events related to <entity>?". You can then select from the relevant options displayed in the Investigate column, which includes a comprehensive set of Cortex XQL library queries for conducting investigations. A summary of the entity's details is displayed. For more details, click Show me more.

## Respond

After entering an entity in the Cortex Assistant search bar, you have the option to take action by selecting one of the suggestions listed in the Respond column. These suggestions encompass a variety of actions, such as running playbooks and scripts, performing scans, and collecting support files.

### **NOTE:**

When you choose an option from the Respond column, Cortex Assistant will always prompt you to approve the action before executing.

## RBAC

Cortex Assistant uses Cortex's role-based access control (RBAC) to control the type of access and actions a user can perform in Cortex Cloud. Suggestions and responses offered by Cortex Assistant will be customized according to that specific user's RBAC access. A user with Admin rights can manage user roles that are assigned to Cortex Cloud users or user groups in Cortex Cloud by selecting Settings → Configurations → Access Management.

For more information on user roles and groups, see [Manage user roles and access management](#).

## Navigation mode

Use Cortex Assistant to navigate in Cortex Cloud. You can search in navigation mode by entering a forward slash / in the search bar, followed by your search string. For example, typing /issues searches for all pages that include the term "issues" and allows you to navigate to them directly.

Additionally, you can enter multiple search terms, and Cortex Assistant will search for pages that include either of the terms (as if there were a logical OR between the words).

## 4.2.5 | Automation

Automation leverages playbooks and Quick Actions to execute predefined workflows, use context data to make informed decisions, and interact with lists to store and retrieve information as needed during the automation process.

### 4.2.5.1 | Automation in Cortex Cloud

#### Abstract

Automate response to issues, using playbooks and Quick Actions, triggered automatically by automation rules or manually from an issue.

Automation enables you to improve efficiency and response times by performing actions on one or more issues, either automatically in response to predetermined conditions or manually triggered during your investigation workflow. In Cortex Cloud, you can use playbooks, scripts, and commands, and Quick Actions to streamline operations, accelerate triage, and boost productivity.

The Automation Insights dashboard provides a high level overview of your automations.



- Playbooks

Playbooks enable you to organize and document security monitoring, orchestration, and response activities. Playbooks are self-contained, fully documented prescriptive procedures that query, analyze, and take action based on the gathered results.

Playbooks are built from regular tasks, quick actions, and sub-playbooks. Playbook tasks can run out-of-the-box or custom scripts and integrations to communicate with third-party systems. You can use out-of-the-box playbooks as is, or customize them according to your requirements. You can also reuse individual playbook tasks as building blocks for new playbooks, saving time and streamlining knowledge retention.

Playbooks can run automatically on issues based on automation rules or manually on one or more issues.

**NOTE:**

You can build end-to-end automation workflows from within the playbook editor, including creating automation rules, configuring integration instances, and creating and editing tasks. For more information, see [Playbooks](#).

- Scripts and commands

Cortex Cloud includes built-in commands, as well as commands and scripts from the core content packs. In addition, when you adopt playbooks, any necessary scripts and integrations for the playbook are automatically downloaded. You can also write your own scripts or edit existing scripts.

Scripts and commands can be used in playbook tasks or run manually from the War Room.

- Quick Actions

Quick actions are single commands that enable you to respond rapidly without requiring complex playbooks.

Quick Actions can be included within playbooks, run automatically on issues based on automation rules, or run manually on one or more issues.

Automation rules

Automation rules enable you to run playbooks or Quick Actions automatically on issues, based on preset criteria. Automation rules follow a WHEN / IF / THEN structure. For example, WHEN an issue is created, IF the severity is critical, THEN set the case assignee to a specific analyst. For more information, see [Create an automation rule](#).

Manually trigger automation

Playbooks and Quick Actions can also be run on demand. For more information, see [Run an automation on an issue](#).

#### 4.2.5.2 | Quick Actions

Quick Actions are preset single commands that enable you to automate basic tasks such as creating tickets in third-party systems, sending Slack messages, and changing issue severity.

You can create quick actions using the following:

- **Automation rules:** You can create predefined rules to run Quick Actions as issues are created. For more information, see [Create an automation rule](#)
- **Playbooks:** You can use Quick Actions as tasks within playbooks.

When investigating an issue, in the Issues table, you can right-click to Run an Automation on one or more issues. For more information, see [Run an automation on an issue](#).

By default, Quick Actions run using all available integration instances that contain the command. When selecting a Quick Action to run on an issue or to use for an automation rule, you can also choose one specific integration instance.

When you run an automation from the Issues table, in some cases the system provides recommended Quick Actions, based on the context. Quick Actions may also be provided in Recommended Automation Rules.

**NOTE:**

Quick Actions appear as War Room entries, but do not appear in the Work Plan.

Access attributes in the Unified Asset Inventory

Quick Actions can automatically populate parameters such as region, account id, and tags, based on asset data. When a Quick Action is triggered manually by a user or automatically through an automation rule, it can reference UIA attributes for the relevant asset(s) in the issue context and use those attributes as input. The issue must contain the relevant `Asset_ID`.

The syntax to reference attributes in the UAI is  `${asset.xdm.asset.attributename}`. To find the property path in the XDM data set, see the asset data card for the asset in the Inventory page. For example, to print the region for the asset, enter `!print value=${asset.xdm.asset.cloud.region}`. You can also run Quick Actions directly on the asset using  `${asset.xdm.asset}`.



#### 4.2.5.3 | Automation Exclusion Center

##### Abstract

Automation exclusion policies prevent commands and scripts from performing remediation on critical assets.

Automation exclusion policies enable you to protect critical assets from automated remediation, without having to detach and customize playbooks and scripts.

Automation exclusion policies prevent commands and scripts from performing automated remediation actions on critical assets, such as users, IP addresses, and domains. For example, a playbook task might block multiple domains, but mission-critical domains in the policy list would not be blocked.

Automation exclusion policies apply any time a relevant command or script runs, whether in a playbook task, a Quick Action, or the CLI. If you configure a policy to allow overrides, users can manually run the command in the War Room, using the **override-policy** parameter. Any command triggered with the **override-policy** parameter appears in the Management Audit Logs. If you attempt to use the **override-policy** parameter and the policy does not allow overrides, an error entry appears in the War Room.

When an automation exclusion policy prevents a command or script from a remediation action, the exclusion appears in the issue War Room.

When a playbook task contains a command or script that is included in an automation exclusion policy, a Policy tab appears in the task details pane, showing the relevant policy.

To enable an automation exclusion policy, add critical assets to a list. Each policy uses one or more lists to exclude assets from remediation. By default, all policies are enabled, but lists are empty until assets are added to the list.

##### NOTE:

By default, all users have read and edit permissions to lists. When creating a list of critical assets, we recommend limiting the read and edit permissions to specific roles.

User Hard Remediation and User Soft Remediation policies can also use asset groups, enabling automatic updates of critical assets without requiring you to edit a list. These remediation policies can contain lists, asset groups, or a combination of lists and asset groups.

Policies can be enabled or disabled, and lists can be edited, but you cannot add or remove policies.

Each policy can include one or more scripts or commands. Commands and scripts only appear if the content is installed. The policy affects only these scripts and commands. Scripts and commands cannot be added, edited, or removed from the policy.

By default, only admin users have access to the Automation Exclusion Center page. You can also provide other roles with View or View/Edit access to the Automation Exclusion Center. When creating or editing a role, the permission can be found under Investigation & Response → Automations.

Policies can be sorted, filtered, and searched using the category, status, policy, exclude, and description columns.

#### 4.2.5.3.1 | Manage automation exclusion policies

##### Abstract

Automation exclusion policies prevent commands and scripts from performing remediation on critical assets. Edit lists of critical assets and enable/disable policies.

Automation exclusion policies prevent commands and scripts from performing automated remediation actions on critical assets, such as users, IP addresses, and domains. For example, a playbook task might block multiple domains, but mission-critical domains in the policy list would not be blocked.

Admin users and all roles with read/write permissions to the Automation Exclusion Center can edit, disable, and enable policies.

1. Go to Settings → Configurations → Automation → Automation Exclusion Center.

2. Right-click on a policy and choose Edit.

3. From the Edit Policy page, you can do the following:



- Enable or disable the policy. Policies are enabled by default.
- Enable or disable policy overrides. If you enable policy overrides, users can manually run the commands and scripts on the excluded critical assets, using the **override-policy** parameter. Use of the **override-policy** parameter is included in the Management Audit Logs.
- Select one or more lists of excluded assets.

Clicking the list icon opens a new browser tab for the Lists page, where you can create and edit lists.

**NOTE:**

For the IAM User Hard Remediation and User Soft Remediation policies, we recommend including username, email, and ID for each user you want to exclude. Example: `username1, user@example.com, userID112`.

Each list can be filtered by conditions, such as `Equals`, `Ends with`, and `Doesn't include`. For example, you can exclude all email addresses with your company's domain using the `Ends with` filter.

- For IAM User Hard Remediation and User Soft Remediation policies, you can also select asset groups. These policies can include only lists, only asset groups, or a combination of asset groups and lists.
- Under THEN skip execution of the following commands and scripts, click to view the scripts and commands affected by the policy. Commands only appear if they are part of an active integration instance. You cannot edit the list of scripts and commands.

4. Save your changes.

**NOTE:**

You can also right click on a policy from the main Automation Exclusion Center page to disable or enable the policy.

If you click on a list name in the Exclude column, that list opens in the Lists page.

#### 4.2.5.4 | Playbooks

Playbooks automate and standardize workflows, ensuring consistent and efficient incident response and management.

**PREREQUISITE:**

To provide playbook access, ensure the Playbooks RBAC permission is set to View or View/Edit.

To completely restrict playbook access, first set the Cases & Issues RBAC permission to None and then set the Playbooks permission to None. Conversely, to provide access to cases and issues, first set the Playbooks permission to View or View/Edit (and then set the Cases & Issues permission).

##### 4.2.5.4.1 | Playbooks overview

Abstract

Cortex Cloud playbooks enable you to structure and automate many of your security processes. Parse case information, interact with users, and remediate.

Playbooks are a series of tasks that run in a predefined flow to save time and improve the efficiency and results of the investigation and response process. They enable you to automate many security processes, including handling investigations and managing tickets. For example, a playbook task can parse the information in an issue, whether it is an email or a PDF attachment.

One-stop playbook development

Before you start building your playbook, go to the Playbooks page and review the Org playbook list, which are playbooks that are currently used in your organization. On the Playbook Catalog page, you can find available out-of-the-box playbooks that are not in use in your organization which you can adopt and use. If an existing playbook does not meet your use case, you can develop a playbook from scratch. Whether editing an existing playbook or creating a new one, you can manage the entire automation development flow in the playbook editor, including creating and editing tasks, configuring automation rules to trigger your playbooks, and setting up all relevant integrations.

Task Library

The Task Library in the playbook editor contains the following objects you can add to your playbook. For example, you can create new tasks from scripts, repurpose existing tasks, and use existing playbooks as sub-playbooks.

Playbook tasks display unique logos to more easily identify task type and origin, for example third-party integration commands, built-in scripts and tasks, and tasks requiring manual inputs.

Task Library Object	Action	See More
Quick Actions	Add single commands requiring minimal configuration.	See topic.



Task Library Object	Action	See More
Commands & Scripts	Add commands and scripts from integrations that you install and configure instances for as needed.	See topic.
Playbooks	Add sub-playbooks to your playbook from your Org repository or from the Playbooks Catalog.	See topic.
AI Prompt	Add AI prompts with inputs and outputs that run automatically.	See topic.
Manual Tasks	Add tasks from playbooks in your Org repository.	See topic.
Header	Add section headers to organize your playbook.	See topic.
Blank Task	Create a new task from scratch.	See topic.

#### Post-development playbook testing

After developing the playbook (including setting automation rules to trigger the playbook), run the debugger to initially test the playbook.

After verifying the playbook is triggered and runs properly with issues, it is ready to use in production.

You can see which playbook ran for an issue by going to Cases & Issues, selecting Issues and scrolling to the Playbook column. You can view or update the playbook by selecting an issue and clicking the Work Plan tab. Select another playbook to run from the dropdown list.

You can see which playbook ran in a case, if any, by going to Cases & Issues, selecting Cases and looking at the Automation section in the Overview tab for the case. You can view or update the playbook by going to the Issues & Insights tab, selecting an issue, and then clicking the Work Plan tab. In the Work Plan, you can select another playbook to run from the dropdown list.

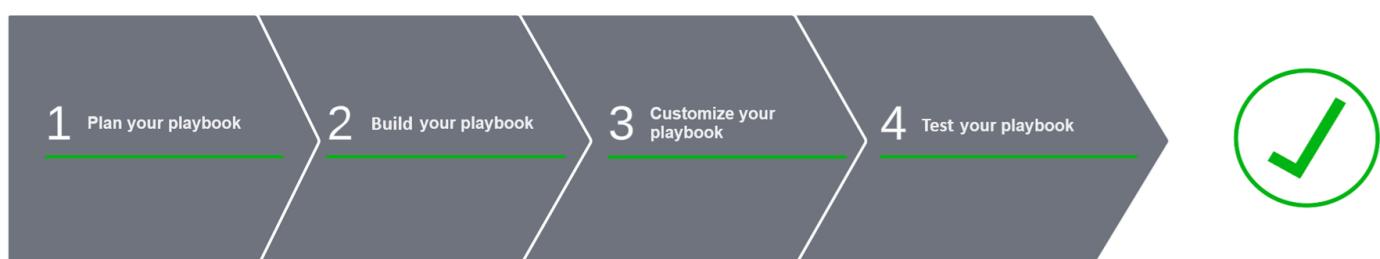
For more information, see [Investigate cases](#).

#### 4.2.5.4.2 | Playbook development checklist

##### Abstract

Follow the playbook development flow to create playbooks that structure and automate many of your security processes.

The playbook development checklist follows the logical flow for developing a playbook.



We recommend that you review the following steps to successfully implement your playbook.

Step	Details	See More
Step 1. Plan your playbook	<p>During the initial planning stage when designing your use case, start defining the playbook flow.</p> <p>Consider the process you want to automate and the steps and the decisions during the process. These steps and decisions become the playbook tasks.</p>	See topic



Step	Details	See More
Step 2. Build your playbook	Consider whether to use a playbook out-of-the-box, customize an existing playbook, or create a new playbook from scratch. Create playbook tasks, inputs, and outputs. Maintain playbook versioning to keep track of playbook development history.	See topic
Step 3. Customize your playbook	Fine tune your playbook for your needs, including extracting indicators, extending context, and adding issue fields to the system.	See topic
Step 4. Test your playbook	Debug errors in your playbook. Use playbook metadata to troubleshoot playbook performance.	See topic

#### 4.2.5.4.3 | Plan your playbook

##### Abstract

Considerations when planning your playbook.

When defining the workflow of your playbook, consider the following:

- What processes do you need to automate?
- Are there any decisions that require manual intervention?
- Are there any time-sensitive aspects to the playbook?
- When is the case considered remediated?

#### 4.2.5.4.4 | Manage playbooks

##### Abstract

Navigate the Playbooks page.

The Playbooks page is organized to help easily access and utilize playbooks specific to your use cases. It contains two main sections, key playbook details on the top and a table listing all the playbooks in your Org repository on the bottom.

##### Playbook status

Playbook statuses enable tracking the progress of automation tasks and identifying any issues or delays. If needed, you can then take corrective actions to ensure smooth workflow execution and operational efficiency. The status includes how many playbooks:

- Are in your Org repository
- Are enabled
- Are active
- Are using an automation rule
- Are used as sub-playbooks
- Ran in the past week

##### The Org repository table

The playbooks listed in the Org repository table have been either adopted by or built by your organization. The table shows high level details about the playbooks, including:



- Playbook name
- Description
- Status
- Source
- Enabled and disabled automation rules associated with the playbook
- How many playbooks it serves as a sub-playbook in
- Last updated
- Updated by
- The content pack the playbook is a part of
- Playbook tags

When you right-click a specific playbook, you can choose to open it in the editor, duplicate, disable, download, or remove it.

Playbooks in your Org Playbooks can be triggered to run by automation rules or can be manually run on one or more issues.

Playbooks that you adopted are part of content packs. When a playbook is adopted, the content pack for that playbook is downloaded and appears in Marketplace. If you remove a playbook from your Org Playbooks, the content pack remains installed, but the playbook is no longer available for automation rules or manual runs.

#### Playbook Catalog

The Playbook Catalog contains all the playbooks available in Marketplace, organized by cards. You can search for a playbook, and the system also recommends playbooks based on name, tag, or description.

Clicking a card provides a preview of the playbook. If it is relevant for your use case, click Adopt this playbook to bring it into your Org repository and make it available to run.

#### **NOTE:**

- The library by default shows only playbooks that are not adopted. Click the Show Adopted checkbox to show the adopted playbooks, indicated by an Adopted mark.
- The library shows the most updated playbook version. Adopting an older version than shown should be done through Marketplace.
- Adopting a playbook does not make it run. Some content packs include recommended automation rules. When you configure automation rules, you can view the recommendations. See Create an automation rule.

#### 4.2.5.4.5 | Build your playbook

##### Abstract

Use an out-of-the-box playbook, customize an existing playbook, or create a new playbook based on your organization's needs.

Depending on your use case, you can use or customize a system playbook or develop a new playbook from scratch.

Developing a new playbook from scratch enables a tailored solution for your use case, whereas customizing a system playbook can save time, reduce complexity, and be a more efficient way to meet your organization's specific security and issue response needs.

Follow these steps to build a playbook.

Task	Description	See More
Task 1. Choose from existing playbooks or create your own	Search for an out-of-the-box playbook to use, customize it, or create one based on your use case.	See topic.
Task 2. Configure playbook settings	Define playbook settings, such as playbook triggers, inputs and outputs, and general settings.	See topic.
Task 3. Add objects from the Task Library	The Task Library contains Quick Actions, scripts, sub-playbooks, and tasks that enable you to communicate with end users, set conditions, and store relevant data.	See topic.



Task	Description	See More
Task 4. Add custom playbook features	Customize your playbook, including adding scripts and sub-playbook loops, filtering and transforming data, extracting indicators, extending context, creating issue fields, and polling.	See topic.
Task 5. Test and debug the playbook	Set breakpoints, conditional breakpoints, skip tasks, and input and output overrides in the playbook debugger.	See topic.
Task 6. Manage playbook content	Save versions of your playbook in Cortex Cloud.	See topic.

4.2.5.4.5.1 | Task 1. Choose from existing playbooks or create your own

#### Abstract

Use an existing playbook from your Org repository or search for a playbook in the Playbook Catalog. Customize an existing playbook, or create a new playbook based on your use case.

Go to the Investigation & Response â–> Automation â–> Playbooks page to find an existing playbook, customize it, or create a playbook.

#### Find an existing playbook

Playbooks in your Org Repository have already been adopted by your organization and are available to run. The Playbook Catalog contains all available playbooks in Marketplace that you can adopt into your Org Repository. You can preview before adopting.

1. View the list of playbooks on the main Playbooks page in the Org Repository table. You can also search for a playbook that exists in the Org Repository by clicking Add Filter.

Use free text in the search box, entering part or all of the playbooks' names or description. You can also search for an exact match of the playbook name by putting quotation marks around the search text. For example, searching for "Block Account - Generic" returns the playbook with that name.

Search for more than one exact match by including the logical operator "or" in-between your search texts in quotation marks. For example, searching for "Block Account - Generic" or "NGFW Scan" returns the two playbooks with those names. Wildcards are not supported in free text search.

#### TIP:

If there are additional relevant playbooks in Marketplace that are not in your Org repository, you can click Explore them now to see them in the Playbook Catalog and choose to adopt.

2. Click Playbook Catalog to browse all available playbooks in Marketplace that you can adopt. Click Playbook Library to go back to the main Playbooks page.

1. Click a playbook card for a preview of the playbook.
  2. Click Adopt this playbook to add the playbook to your Org repository.
- A confirmation message displays when the playbook is successfully added.

3. Click View in Org Playbooks to select the adopted playbook from the Org repository table.

You can use the playbook as-is, or customize it as needed.

#### Edit a playbook

From the list of playbooks in your Org repository, right-click the playbook you want to edit and select Open in Editor. You can also duplicate, disable, download, or delete the playbook.

When you adopt a playbook, it is locked and you can only make limited changes to the playbook settings from the Playbook Starts task.

When you adopt a playbook, tasks and sub-playbooks that require configuration appear with a red triangle and an exclamation mark, enabling you to locate and configure all necessary components.

#### NOTE:

When a task inside of a sub-playbook is not configured, the alert is propagated to the main playbook. If multiple sub-playbooks are nested, and any of the sub-playbooks have non-configured components, the alert appears in the main playbook as well as in the sub-playbooks. Alerts also appear for the individual non-configured tasks within the sub-playbooks.

To reduce visual noise, you can dismiss certain alerts for unnecessary non-configured components such as sub-playbooks, scripts, and commands. You can dismiss an alert only if leaving the component in its non-configured state will not lead to a playbook error. For example, if the task must execute for the playbook to proceed, you cannot dismiss the alert.



When you click on the red triangle, you have the option to Dismiss Alert. After an alert is dismissed, the triangle is grey. Clicking on the grey triangle gives you the option to Mark as alert and revert to the red triangle. Alerts can be dismissed in both system and custom playbooks, and you do not need to duplicate a system playbook to dismiss an alert.

For full editing capabilities, right-click and select Open in Editor or Duplicate, which creates a copy of the playbook to edit, for example for a system playbook.

You can then configure the playbook settings or add quick actions, scripts, AI prompts, sub-playbooks, or tasks from the Task Library.

**TIP:**

- To open multiple playbooks at the same time, edit the first playbook and then click New next to the playbook name to create a new tab. You can either create a new playbook, or add an existing one.
- You can view recently modified or deleted playbooks by clicking version history for all playbooks 

Create a playbook

1. In the Playbooks page, click + Build New Playbook.
2. In the Create new pop up, enter a name, description, and tags for the playbook and click Save.

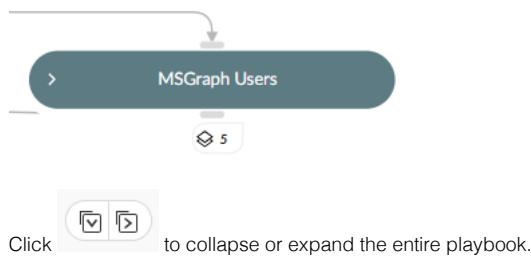
A blank playbook opens in the playbook editor. You can then configure the playbook settings or add quick actions, AI prompts, scripts, sub-playbooks, or tasks from the Task Library.

Collapse and expand playbook sections

You can easily navigate playbooks and focus on the parts you need to work on by collapsing and expanding playbook sections. Collapsing sections provides a condensed view of the playbook flow, reducing visual clutter and enabling quick access to specific sections. Expanding sections allows you to view or edit specific parts of a playbook while keeping the rest of the playbook compact and maintaining focus on the relevant playbook details. You can also hover over a section header to highlight all tasks under the section and easily identify the section scope.

To collapse and expand a section, in the Playbooks page, after selecting a playbook from the library or creating a new playbook and adding tasks, click  on a section header.

When you collapse a section, you can see the number of tasks included under the section. For example:



Click  to collapse or expand the entire playbook.

 Show me more



## Playbooks

