>

Cloud Identity and Access Management (Cloud IAM) roles prescribe how you can use the Security Command Center API. Below is a list of each Cloud IAM role available for Security Command Center and the methods available to them. Apply these roles at the **organization** level.

Role	Title	Description	Permissions	Lowest resource
`roles/securitycenter.admin`	Security Center Admin	Admin(superuser) access to security center	resourcemanager.organizations.get securitycenter.*	Organiza
`roles/securitycenter.adminEditor`	Security Center Admin Editor	Admin Read-write access to security center	resourcemanager.organizations.get securitycenter.assets.* securitycenter.assetsecuritymarks.* securitycenter.findings.* securitycenter.findingsecuritymarks.* securitycenter.sources.get securitycenter.sources.list securitycenter.sources.update	Organiza
`roles/securitycenter.adminViewer`	Security Center Admin Viewer	Admin Read access to security center	resourcemanager.organizations.get securitycenter.assets.group securitycenter.assets.list securitycenter.assets.listAssetPropertyNames securitycenter.findings.group securitycenter.findings.list securitycenter.findings.listFindingPropertyNames securitycenter.sources.get securitycenter.sources.list	Organiza
`roles/securitycenter.assetSecurityMarksWriter`	Security Center Asset Security Marks Writer	Write access to asset security marks	securitycenter.assetsecuritymarks.*	Organiza
`roles/securitycenter.assetsDiscoveryRunner`	Security Center Assets Discovery Runner	Run asset discovery access to assets	securitycenter.assets.runDiscovery	Organiza

Role	Title	Description	Permissions	Lowest resource
`roles/securitycenter.assetsViewer`	Security Center Assets Viewer	Read access to assets	resourcemanager.organizations.get securitycenter.assets.group securitycenter.assets.list securitycenter.assets.listAssetPropertyNames	Organiza
`roles/securitycenter.findingSecurityMarksWriter`	Security Center Finding Security Marks Writer	Write access to finding security marks	securitycenter.findingsecuritymarks.*	Organiza
`roles/securitycenter.findingsEditor`	Security Center Findings Editor	Read-write access to findings	resourcemanager.organizations.get securitycenter.findings.* securitycenter.sources.get securitycenter.sources.list	Organiza
`roles/securitycenter.findingsStateSetter`	Security Center Findings State Setter	Set state access to findings	securitycenter.findings.setState	Organiza
`roles/securitycenter.findingsViewer`	Security Center Findings Viewer	Read access to findings	resourcemanager.organizations.get securitycenter.findings.group securitycenter.findings.list securitycenter.findings.listFindingPropertyNames securitycenter.sources.get securitycenter.sources.list	Organiza
`roles/securitycenter.sourcesAdmin`	Security Center Sources Admin	Admin access to sources	resourcemanager.organizations.get securitycenter.sources.*	Organiza
`roles/securitycenter.sourcesEditor`	Security Center Sources Editor	Read-write access to sources	resourcemanager.organizations.get securitycenter.sources.get securitycenter.sources.list securitycenter.sources.update	Organiza
`roles/securitycenter.sourcesViewer`	Security Center Sources Viewer	Read access to sources	resourcemanager.organizations.get securitycenter.sources.get securitycenter.sources.list	Organiza

When you enable Security Command Center, a service account is created for you in the format of `service-org-`***`organization-id`***`@security-center-api.iam.gserviceaccount.com`. That service account is automatically granted the `securitycenter.serviceAgent` role. This role enables Security Command Center to create and update its own copy of your organization's asset inventory metadata on an ongoing basis. This is an internal role that includes the following permissions:

Role	Title	Description	Methods Allowed
`securitycenter.serviceAgent`	Access to scan Google Cloud resources and import security scans	Security Center Service Agent	All of the permissions of the following roles: • `appengine.appViewer` • `cloudasset.viewer` • `compute.viewer` • `container.viewer` • `dlpscanner.policyReader` • `dlpscanner.scanReader` • `dlp.jobsReader` Plus the following additional permissions: • `resourcemanager.folders.list` • `resourcemanager.folders.get` • `resourcemanager.organizations.list` • `resourcemanager.organizations.get` • `resourcemanager.projects.list` • `resourcemanager.projects.get` • `resourcemanager.projects.getIamPolicy` • `storage.buckets.get` • `storage.buckets.list` • `storage.buckets.getIamPolicy`

To add `roles/securitycenter.serviceAgent`, you must have `roles/resourcemanager.organizationAdmin`. You can add the role to a service account by running:

For more information about Cloud IAM roles, see understanding roles (/iam/docs/understanding-roles).