Cisco Identity Troubleshooting & Support

Troubleshooting & Support

Opening a Customer Support Issue with Cisco Identity

If you are a Duo customer, you can contact Duo support following those instructions: https://help.duo.com/s/article/1441?language=en_US

If you are not a Duo customer, open a TAC case with the product that entitled you to Cisco Identity: https://www.cisco.com/c/en/us/support/index.html

API Permissions for Integrations

Overview

This page contains API details for the following Integrations:

- Azure AD
- Duo
- Okta
- Auth0
- Google (G-Suite)
- Salesforce

Integrations

This section contains a summary of the API permissions for Cisco Identity integrations and the purpose for which the connection is used

Azure AD

This section covers the API permissions for the following Microsoft Azure APIs:

MS Graph API - Application Permissions

Name	Description	Purpose
`AuditLog.Read.All`	Read all audit log data	Read user activity from the Audit Log
`Directory.Read.All`	Read directory data	

`Group.Read.All`	Read all groups	
`GroupMember.Read.All`	Read all group memberships	Get a list of user's group memberships
`Reports.Read.All`	Read all usage reports	Find a manager's end user direct reports
`User.Read.All`	Read all users' full profiles	
`Policy.Read.All`	Read your organization's policies	Get a list of policies and named locations
`IdentityRiskyUser.Read.All`	Read your organization's risky users	Get a list of users marked as `Risky` by Azure
`IdentityRiskEvent.Read.All`	Read your organization's risky user events	Read details on events associated with `Risky` user activities
`UserAuthenticationMethod.Read.All`	Read user auth methods	Read user authentication methods that are available

MS Graph API - InTune Devices

Name	Description
`DeviceManagementApps.Read.All`	Read Microsoft InTune apps
`DeviceManagementConfiguration.Read.All`	Read Microsoft InTune device configuration and policies
`DeviceManagementManagedDevices.Read.All`	Read Microsoft InTune devices

MS Graph API - Permissions for Remediation Actions

Note: These API permissions allow updates to be made directly from Cisco Identity to Azure AD

Name	Remediation Type

`User.ReadWrite.All`, `User.ManageIdentities.All`, `Directory.ReadWrite.All`	Update User Type
`User.ReadWrite.All`, `Directory.ReadWrite.All`	User Log out
`UserAuthenticationMethod.ReadWrite.All`	Factors Reset (TBD)

Duo

Duo Admin API with the following permissions are required for Duo integration instances:

Name	Description	Purpose
Grant read log	Permit Admin API application to read logs	Read the Duo event log
Grant read resource	Permit Admin API application to read resources such as users, phones, and hardware token	Get a list of users and devices

The following permissions are required for Remediation Actions:

Note: These API permissions allow updates to be made directly from Cisco Identity to Duo

Name	Remediation Type
Grant write resource	Reset Factors

Okta SSWS API Token Scopes

API	HTTP Operation
`/api/v1/*`	READ

As we require the minimal set of privileges, the custom admin role must be created in order to support remediations in Cisco Identity (ref to `Oort Help Desk Admin` role in https://oortpreview-admin.oktapreview.com):

Edit role

A role contains permissions that you want to grant to an admin. After creating a role, you can further constrain it to a resource set. See best practices for creating a role assignment.

Role name

Oort Help Desk Admin

Role description

Oort Help Desk Admin

Add permissions

View by type

- [x] User
- [x] Group
- [x] Application
- [ ] Profile source
- [ ] Workflow
- [ ] Authorization server
- [ ] Customizations

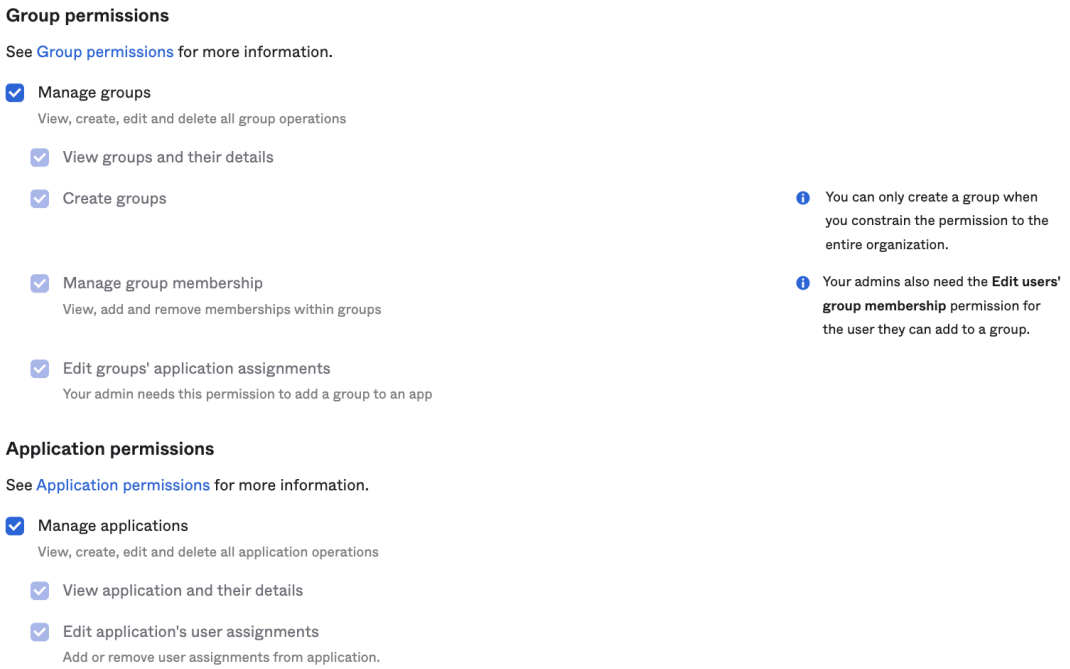
Filter by permission

11 hidden permissions

User permissions

See User permissions for more information.

- [ ] Manage users
  View, create, edit and delete all user operations
  - [ ] Create users
  - [x] Edit users' profile attributes
  - [x] Edit users' lifecycle states
    - [x] Activate users
    - [x] Deactivate users
    - [x] Suspend users
    - [x] Unsuspend users
    - [x] Delete users
    - [x] Unlock users
    - [x] Clear users' sessions
  - [x] Edit users' authenticator operations
    - [x] Reset users' authenticators
    - [x] Reset users' passwords
    - [x] Set users' temporary password
      Allows admin to expire a user's password and set a temporary password



Auth0 API Permissions

In Auth0 Management API:

Add a "Machine to Machine" application (`Applications --> Applications`) should be configured in Auth0 (via a configured API (`Applications --> APIs`) with the following scope permissions:

Scope	Description	Purpose
`read:users`	Read Users	Get a list of Users
`read:logs`	Read Logs	Read Auth0 Event logs
`read:user_logs`	Read logs relating to users	Read Auth0 User logs
`read:guardian_factors`	Read Guardian factors configuration	Get a list of Users and Authenticator configurations

G-Suite Connected App Permissions

Scope	Description
`https://www.googleapis.com/auth/admin.directory.group.member.readonly`	groups membership
`https://www.googleapis.com/auth/admin.directory.group.readonly`	groups

`https://www.googleapis.com/auth/admin.directory.user.readonly`	users
`https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly`	rolemanagement
`https://www.googleapis.com/auth/admin.directory.orgunit.readonly`	devices
`https://www.googleapis.com/auth/admin.directory.audit.readonly`	audit logs

The following permissions are required for Remediation Actions:

Note: These API permissions allow updates to be made directly from Cisco Identity to G-Suite

Scope	Description
`https://www.googleapis.com/auth/admin.directory.user.security`	audit logs

Salesforce Connected App Permissions

Scope	Description	Purpose
Manage user data via APIs (api)	Allows access to the current account using APIs, such as REST API and Bulk API 2.0	Collect user data

Responsible Disclosure Policy

At Cisco Identity, our mission is to make network security easy for distributed companies. We value the insights of our clients, partners, and the independent security research community, and we welcome the opportunity to work together with this community when vulnerabilities are discovered. We believe that the disclosure of vulnerabilities is essential for improving the quality and security of our product, and the safety of our customers who rely upon it.

If you are a security researcher and have identified a suspected security vulnerability in our product, we appreciate your help in disclosing it to us in a coordinated and responsible manner. If you report a valid security vulnerability in compliance with this Responsible Disclosure Policy (“Policy”), Cisco Identity will collaborate with you to understand, validate and resolve the issue.

Responsible disclosure helps us to ensure that our product and infrastructure is tested and reliable. Moreover, our commitment to mitigate vulnerabilities is reassuring for our customers

and the security industry as a whole.

Cisco Identity's responsible disclosure program is intended to encourage coordinated responsible disclosure. We endeavor to apply industry best practices for coordinated disclosure of vulnerabilities to ensure that customers get the highest quality information and to drive public discussion of methods for improvement of products, protocols, and standards. Unless required by law or law enforcement authorities, Cisco Identity does not intend to initiate a lawsuit or law enforcement investigation against a security researcher who discovers and reports a security vulnerability in compliance with this Policy. Cisco Identity reserves all rights in the event of noncompliance. If your security research involves the networks, systems, information, applications, products, or services of another party, including a third-party application that is integrated with Cisco Identity, that third party may determine whether to pursue legal action. We cannot and do not authorize security research involving any other entities.

Your participation in this program is voluntary and subject to the terms and conditions set forth in this Policy. By submitting reports or otherwise participating in this program, you agree that you have read and will follow this Policy. Cisco Identity reserves the right to change or modify the terms of this program or terminate this program at any time.

Please submit your findings to security@oort.io.

Cisco Identity’s Responsible Disclosure Policy

For more information on Cisco Identity’s responsible disclosure policy, see the Cisco Trust Portal.