Manage User Accounts and Roles

User account and role management includes user accounts, administrative users, user roles, role permissions, and Global API permission categories.

User accounts

Users are accounts that administrators create for people who use Crosswork Network Controller.

As a best practice, administrators should create separate accounts for all users. Prepare a list of the people who will use Crosswork Network Controller. Decide on their user names and preliminary passwords, and create user profiles for them. During the creation of a user account, you assign a user role to determine the functionality that the user can access. If you use user roles other than "admin", create the user roles before you add your users (refer to Create user roles, on page 5).

You can optionally view the Network Configuration Access Control Model (NACM) rules that let admin members grant access to devices in selected groups and deny access to other devices.

Administrative users created during installation

During installation, Crosswork Network Controller creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **`cw-admin`**, and the default password **`admin`**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Crosswork Network Controller server.
2. The **Cisco Crosswork administrator**, with the username **`admin`** and the default password **`admin`**. Product administrators use this ID to log in to and configure the user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used.

Add a user

This topic explains how to add a user in Crosswork Network Controller.

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To add a new user:

a) Click  and enter the required user details.

When you are configuring Device Access Groups for your users, select the **Device Access Group** listed in the right pane to assign it to the new user you are creating.

Note

1. By default users associated with ALL-ACCESS Device Access Group are provided access to ALL devices.
2. You must associate at least one Device Access Group to a user.

b) Click **Save**.

Edit a user

This topic explains how to edit settings for an existing user.

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To edit a user:

a) Click the checkbox next to the User and click  .

b) After making changes, click **Save**.

Delete a user

This topic explains how to delete an user account.

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To delete a user:

a) Click the checkbox next to the User and click .
b) In the **Confirm Deletion** window, click **Delete**.

View user audit logs

This topic explains the steps to view the audit logs for a selected user.

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To view the audit log for a user:

a) Click the icon under the **Actions** column, and select **Audit Log**.

The **Audit Log** window is displayed for the selected user name.

Generate NACM rules for users

This topic explains the steps to generate NACM rules for a selected user.

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To view NACM rules for a user:

a) Click the icon under the **Actions** column, and select **Generate NACM Rules**.

The **NACM Rules** window is displayed for the selected user name.

If you have an NSO service configured on your Crosswork Network Controller, you can generate NACM rules by

clicking the icon under the **Actions** column for a user and selecting **Generate NACM Rules**. This integrates device-level NACM control with the NSO workflow. Note that for each unique combination of Device Access Group associated with a user, there is:

- A NACM group associated with the user.
- A corresponding NACM rule list associated with the user.

The rule allows access to devices in selected Device Access Groups and denies access to other devices. You can copy the XML rules file and add it in your NSO NACM Rule configuration setup. The options available under the NSO

Actions tab, located in Device **Management > Network Devices**, are also restricted based on the Device Access Groups permissions of the user.

You can also view the Crosswork Network Controller Audit log and the NSO commit logs to track and verify the activities of users using the NACM rules, ensuring traceability.

User roles, functional categories, and permissions

Every Crosswork Network Controller user must have a user role assigned. The user role controls what the user who is assigned that role can do when using the platform and its applications, which are controlled by internal APIs. The default user role, “admin”, gives users with that role access to all of the underlying APIs, which means an admin user can perform any and all functions the platform offers to users via the user interface.

The **Roles** window lets users with the appropriate privileges define custom user roles. As with the default *admin* role, a custom user role consists of:

- A unique name, such as “Operator” or “admin”.
- One or more selected, named functional categories, which control whether or not a user with that role has access to the APIs needed to perform specific Crosswork Network Controllerfunctions controlled by that API.
- One or more selected permissions, which control the scope of what a user with that role can do in the functional category.

For a user role to have access to a functional category, that category and its underlying API must show as selected on the **Roles** page for that role. If the user role shows a functional category as unselected, then users with this role assigned will have no access to that functional area at all.

Some functional categories group multiple APIs under one category name. For example: The “AAA” category controls access to the Password Change, Remote Authentication Servers Integration, and Users and Role Management APIs. With this type of category, you can deny access to some of the APIs by leaving them unselected, while providing access to other APIs under the category by selecting them . For example: If you want to create an “Operator” role who is able to change his own password, but not refer to or change the settings for your installation’s integration with remote AAA servers, or create new users and roles, you would select the “AAA” category name, but uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” checkboxes.

For each role with a selected category, the **Roles** page also lets you define permissions to each underlying functional API:

- **Read** permission lets the user refer to and interact with the objects controlled by that API, but not change or delete them.
- **Write** permission lets the user refer to and change the objects controlled by that API, but not delete them.
- **Delete** permission gives the user role delete privileges over the objects controlled by that API. It is useful to remember that delete permission does not override basic limitations set by the Crosswork Network Controller platform and it applications.

Although you can mix permissions as you wish:

- If you select an API for user access, you must provide at least “Read” permission to that API.

- When you select an API for user access, Crosswork Network Controller assumes that you want the user to have all permissions on that API, and will select all three permissions for you, automatically.
- If you uncheck all of the permissions, including "Read", Crosswork Network Controller will assume that you want to deny access to the API, and unselect it for you.

Best practices for user roles

Custom role permission recommendations

Cisco recommends that you follow these best practices when creating custom user roles:

- Restrict **Delete** permissions in roles for *admin* users with explicit administrative responsibility for maintenance and management of the Crosswork Network Controller deployment as a whole.
- Roles for developers working with all the Crosswork Network Controller APIs will need the same permissions as *admin* users.
- Apply at least **Read** and **Write** permissions in roles for users who are actively engaged in managing the network using Crosswork Network Controller.
- Give read-only access to roles for users who only need to refer to the data to help their work as system architects or planners.

Note Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions. Using Zero Touch Provisioning features requires access to all ZTP APIs.

Sample custom user roles

The following table describes some sample custom user roles you should consider creating:

Table 1: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager, triggers Playbooks in response to KPI alerts	All	Read, Write
Monitor	Monitors alerts only	Health Insights, Inventory, Topology	Read only
API Integrator	All	All	All

Create user roles

Local users with administrator privileges can create new users as needed (refer to Add a user, on page 1).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

Follow the steps below to create a new user role.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles** tab.

The **Roles** window has a **Roles** table on the left side and a corresponding **Global API Permissions** tab on the right side which shows the grouping of user permissions for the selected role.

Step 2 On the **Roles** table, click  to display a new role entry in the table.

Step 3 Enter a unique name for the new role.

Step 4 To define the user role's privilege settings, select the **Global API Permissions** tab and perform the following:

a) Check the check box for every API that users with this role can access. The APIs are grouped logically based on their corresponding application.

b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 5 Click **Save** to create the new role.

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (refer to Edit user roles, on page 7).

Clone user roles

Cloning an existing user role is the same as creating a new user role, except that you need not set privileges for it. If you like, you can let the cloned user role inherit all the privileges of the original user role.

Cloning user roles is a handy way to create and assign many new user roles quickly. Following the steps below, you can clone an existing role multiple times. Defining the cloned user role's privileges is an optional step; you are only required to give the cloned role a new name. If you like, you can assign it a name that indicates the role you want a group of users to perform. You can then edit the user IDs of that group of users to assign them their new role (refer to Add a user, on page 1). Later, you can edit the roles themselves to give users the privileges you want (refer to Edit user roles, on page 7).

Note Some API permissions are predefined in the system admin role and remain unchanged in the cloned role. For example, the system admin role includes the default **Read** and **Write** permissions for the **Alarms & Events** API. These permissions are not configurable for both, original, and cloned admin roles.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click an existing role.

Step 3 Click  to create a new duplicate entry in the **Roles** table with all the permissions of the original role.

Step 4 Enter a unique name for the cloned role.

Step 5 (Optional) Define the role's settings:

a) Check the check box for every API that the cloned role can access.

b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Edit user roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click and select on an existing role from the left side table. The **Global API Permissions** tab on the right side displays the permission settings for the selected role.

Step 3 Define the role's settings:

a) Check the check box for every API that the role can access.

b) For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 4 When you are finished, click **Save**.

Delete user roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles** > **Roles** tab.

Step 2 Click the role you want to delete.

Step 3 Click  .

Step 4 Click **Delete** to confirm that you want to delete the user role.

Global API permissions

This topic lists the global API permission categories and role permission categories available for Crosswork Network Controller.

The **Roles** window lets users with the appropriate privileges define custom user roles.

The following table is an overview of the various **Global API Permissions** in Cisco Crosswork Network Controller:

Table 2: Global API permission categories

Category	Global API Permissions	Description
AAA	Remote Authentication Servers Integration	Provides permission to manage remote authentication server configurations in Crosswork Network Controller. You must have READ permission to view/read configuration, and WRITE permission to add or update the configuration of any external authentication server (e.g. LDAP, TACACS) into Crosswork Network Controller. The Delete permissions are not applicable for these APIs.
	Users and Roles Management	Provides permission to manage users, roles, sessions, and password policies. Supported operations include "Create new user/role", "Update user/role", "Delete a user/role", "Update task details for a user/role", "Session management (Idle-timeout, max session..)", "update password policy", "get password tooltip help text", "get active sessions", etc. The READ permission allows you to view the content. The WRITE permission allows you to create and update. The DELETE permission allows you to delete a user or role.
	User Preferences	Allows you to manage the dashlets in the homepage. The READ permission allows you to view dashboards, WRITE permission allows you to edit dashboards, DELETE permission allows you to delete dashboards.

Category	Global API Permissions	Description
Administrative Operations	Diagnostic Information	Allows you to access the diagnostic information.
	External Notification Subscription	Allows you to subscribe or unsubscribe the external kafka notification streaming. The READ permission allows you to view the list of subscriptions. The WRITE and DELETE permissions allows you to edit and delete the subscriptions respectively.
	Logging	Allows you to view and manage the logging information.
	Performance Monitoring Data Retension	Allows you to retain the Performance Monitoring data.
	Performance Monitoring Export APIs	Allows you to manage the Performance Monitoring export APIs.
	RESTCONF Notification Subscription	Allows you to subscribe or unsubscribe the RESTCONF notification streaming (WebSocket and connectionless). The READ permission allows you to view the list of subscriptions. The WRITE and DELETE permissions allows you to edit and delete the subscriptions respectively.

Category	Global API Permissions	Description
Device Monitoring	Device Inventory	Responsible for retrieving the device inventory.
	Device Inventory RESTCONF	Responsible for retrieving the inventory information. The READ permission allows you to get all the inventory data such as nodes, termination points, equipment, and modules. The WRITE and DELETE permissions are not applicable for this API as there is no support for configuration-related operations.
	Inventory Job	Responsible for retrieving the inventory job information.
	Network Inventory	Responsible for retrieving the network inventory.
	Performance Monitoring Dashboards	The READ permission allows displaying any metrics on the Crosswork Network Controller homepage, dashboard window, and deep inventory. The WRITE and DELETE permissions are not applicable for this API.
	Performance Monitoring Policies	Allows you to manage monitoring policies. The READ permission allows you to view the monitoring policies. The WRITE permission allows you to create and update monitoring policies. The DELETE permission allows you to delete monitoring policies.
	Performance Monitoring RESTCONF	Responsible for retrieving the device performance metrics. The READ permission allows you to get the metrics information such as CPU, temperature, CRC, and interface utilization. The WRITE and DELETE permissions are not applicable for this API as there is no support for configuration-related operations.

Category	Global API Permissions	Description
Alarms and Events	Alarm Notification Policies	The READ permission allows you to read system/network, and device alarm notification policies. The WRITE permission allows you to create system/network, and device alarm notification policies.
	Alarm Settings	The READ permission allows you to view alarm settings. The WRITE permission allows you to view and update alarm settings.
	Alarm Suppression Policies	The READ permission allows you to view a suppression alarm policy. The WRITE permission allows you to create, update and delete a suppression alarm policy.
	Alarm & Events	Allows you to manage alarms. The READ permission allows you to get events/alarms according to request criteria, get the list of Syslog destinations, and get the list of trap destinations. The WRITE permission allows you to set a response for when an alarm is raised, acknowledged, or unacknowledged, create/raise an event, update the event info manifest, and add notes to alarms. The DELETE permission allows you to delete REST destinations, Syslog destinations and trap destinations.
	Alarm and Events RESTCONF	Responsible for performing alarms related operations. The READ permission allows you to get all the alarm data (system,network & device). The WRITE permission allows you to acknowledge, unacknowledge, and clear alarms. The DELETE permission is not applicable for these APIs.

Category	Global API Permissions	Description
CNC	CAT FP Deployment Manager APIs	Allows you to manage function pack upload and deployment. The READ permission enables you to get the list of packages, files, and deployment information. The WRITE permission allows you to upload/deploy/un-deploy a package/function pack/file. The DELETE permission is not applicable for these APIs.
	CAT Inventory RESTCONF APIs	North Bound Interface (NBI) RESTCONF interface for the CAT services inventory data (from CAT to external consumers). The READ permission allows you to fetch the services information from CAT. The WRITE permission allows you to invoke operations APIs to retrieve the service information from CAT. The DELETE permission is not applicable for these APIs.
	CAT ISTP REST APIs	System use only. The READ/WRITE permissions are mandatory for CAT UI/ISTP to function. The DELETE permission is not applicable for these APIs.
	CAT Service Overlay	Primarily used to investigate issues in the overlay. Only READ permission is applicable.
	CAT UI	Mandatory APIs that enable CAT UI to fetch all NSO services and resources. The READ permission allows you to fetch and display all service information. The WRITE permission allows you to commit service assurance information. The DELETE permission is not applicable for these APIs.
	NSO Connector APIs	Allows you to perform services resync, full-resync, change log-level and return service HA status. The READ permission allows you to check the service status. The WRITE permission is required for all other operations. The DELETE permission is not applicable for these APIs.
	OAM Service APIs	Not Applicable

Category	Global API Permissions	Description
Change Automation	Administration	Provides administrative control to manage job scheduling, manage override credentials, and configuration of user roles for playbook executions. The READ permission allows you to check the status and fetch the information. , while the WRITE permission allows you to make changes. The DELETE permission is not applicable for these APIs.
	Application	Allows you to manage the Change Automation tasks (for example, schedule playbook executions, execute playbooks, update playbook jobs, check playbook executions status, check playbook job-set details, list supported YANG modules, etc.) The READ permission allows you to view the applicable information (for example, check the job status, fetch job details, etc.). The WRITE permission is required for playbook job scheduling/execution. The DELETE permission is not applicable for these APIs.
	Playbook	Allows you to manage playbooks. The READ permission allows you to retrieve playbooks, params, and policy specs. The WRITE permission allows you to import/export, and generate playbooks. The DELETE permission enables you to delete playbooks.
	Play	Allows you to manage plays. The READ permission allows you to fetch or view plays, while the WRITE permission allows you to create, update or import a play. The DELETE permission allows you to delete a play.

Category	Global API Permissions	Description
Collection Infra	Collection APIs	Permissions for APIs to manage collection jobs. Based on the READ, WRITE, and DELETE permissions, you can view collection jobs, create or update new collection jobs (external), or delete existing collection jobs. System collection jobs (data collection setup internally for Crosswork Network Controller consumption) cannot be modified irrespective of these permissions (permitted for Administrators only), but users with the READ permission can view the details of all collection jobs including system collection jobs. For most users, READ-only permissions would be enough as it enables them to view Collection jobs detail (request and status) and actual data collection status/metrics per device/sensor path level.
	Data Gateway Manager APIs	Permissions to perform CRUD operations on Destinations, Data Gateways, Custom Packages, etc. The READ permission allows you to view the data, while the WRITE permission allows you to perform these actions: • Add, edit, or delete Data Gateways and Data Gateway instances. • View the vitals and system packages • Add, edit, delete, and view the custom packages • Add, edit, or delete data destinations • Update resources • Create, edit, or delete Data Gateway pools • Revoke the provisioning permission from task permissions • Restrict user access by revoking the Inventory API, Data gateway APIs, and Platform APIs permissions. • Troubleshoot data collection issues

Category	Global API Permissions	Description
Crosswork Optimization Engine	OPTIMA Analytics	Allows you to manage analytics in Crosswork Optimization Engine. The READ permission allows you to view/export historical data. The WRITE permission enables you to change the Traffic Engineering Dashboard settings. The DELETE permission is not applicable for these APIs.
	OPTIMA Analytics Service	Allows you to manage analytics service in Crosswork Optimization Engine. The READ permission enables you to get LSP events data, LSP utilization, LSP SR-PM metric, Link SR-PM and underutilized LSPs. The WRITE and DELETE permissions are not applicable for these APIs.
	Optima Engine RESTCONF and Optima Engine RESTCONF API for backwards compatibility	

Category	Global API Permissions	Description
		Allows you to customize the RESTCONF API permissions in Crosswork Optimization Engine. The READ permission grants access to perform these actions: • Fetch L2 and L3 topology details, as well as Segment Routing policy information • Preview SR Policy route and filter SR Policies on Interfaces and nodes • Preview RSVP-TE tunnels • Get LCM domains and LCM recommendation SR Policies • Preview LCM recommendations and get LCM configuration and managed interfaces • Get Circuit Style SR Policy paths on interfaces and nodes • Get all Circuit Style SR Policy paths • Get Circuit Style Manager interface bandwidth pool • Get a plan file for the network model The WRITE permission grants access to perform these actions: • Provision, modify, and delete SR policies • Provision, modify, and delete RSVP-TE tunnels • Provision, modify, and delete SR P2MP policies • Configure LCM configuration and managed interfaces • Remove LCM domains • Commit and pause LCM recommendations • Set CSM interface bandwidth pool • Create notification streams • Reoptimize Circuit Style SR policies The DELETE permission is not applicable for these APIs.
	Optimization Engine UI	

Category	Global API Permissions	Description
		Allows you to manage SR policies, RSVP tunnels, LCM, BWoPT, BWoD, Traffic Engineering settings, and Preview policies. The READ permission allows you to view deployed policies, settings, routes, LCM domain config/data, service overlay data, path queries, dashboard metrics, etc. The WRITE permission allows you to configure LCM, BWoD, BWopt, deploy policies, preview Crosswork Optimization Engine-managed policies, etc. The DELETE permission allows you to delete SR policies, RSVP tunnels, remove affinity mapping, and delete LCM domains.
Crosswork Optimization Engine v2	Optimization Engine RESTCONF API v2	Allows you to customize the RESTCONF interface permissions in Crosswork Optimization Engine. The READ permission enables you to fetch L2 and L3 topology details, and Segment Routing Policy details. The WRITE permission allows you to fetch policy routes, provision/modify/delete/preview SR policies, and manage LCM configuration. The DELETE permission is not applicable for these APIs.
Data Gateway Global Settings	Data Gateway Global Parameters API	There are certain parameters in the data gateway, which can be changed globally across all gateways in a Deployment. The READ permission allows you to view the data, while the WRITE permission is required to reset/update the data.
	Data Gateway Global Resources Reset API	Allows you to reset updates done to the Global Parameters. The READ permission allows you to view the data, while the WRITE permission resets the data.
	Data Gateway Global Resources Update API	Allows you to update the Global Parameters. The READ permission allows you to view the data, while the WRITE permission updates the data.
Data Gateway Troubleshooting	Data Gateway Reboot API	Reboots a data gateway. The WRITE permission allows you to reboot the data gateway.
	Data Gateway Showtech API	Generates and downloads showtech logs for a data gateway. The READ permission allows you to view showtech, while WRITE permission generates showtech. Write Permission allows u to generate showtech

Category	Global API Permissions	Description
Health Insights	Health Insights APIs	Allows you to manage Health Insights KPIs. The READ permission allows you to view all KPIs, KPI profiles, job details, alerts, etc. The WRITE permission allows you to create or update KPIs and KPI profiles, enable/disable KPI profiles, link KPIs to playbooks, etc. The DELETE permission allows you to delete custom KPIs and KPI profiles.
Inventory	Inventory APIs	Allows you to manage inventory. The READ permission allows you to • Fetch the list of nodes, the node credentials, and the count of nodes in the database. • Retrieve the list of HA pools, data gateway enrollments, virtual data gateways, and inventory job information. • Retrieve the list of policies, providers, and tags. The WRITE permission allows you to • Update device mapping to virtual data gateway pool. • Lock/unlock the requested nodes. • Remove tag associations from nodes. Does not support partial un-assignment. • Update input data to a set of devices. • Set API endpoint for provider onboarding. • Update collections job cadence The DELETE permission allows you to • Perform bulk deletion of credential profiles and nodes. • Upload CSV for delete operations. • Delete HA pools, Data Gateway enrollments, and virtual data gateways. • Delete policies, providers, and tags.

Category	Global API Permissions	Description
Platform	Platform APIs	The READ permission allows you to fetch the server status, cluster node information, application health status, collection job status, certificate information, backup and restore job status, etc. The WRITE permission allows you to • Enable/disable the maintenance mode • Enable/disable the xFTP server • Manage cluster (set the login banner, restart a microservice, etc.) • Rebalance cluster resources • Manage nodes (export cluster inventory, add VM, apply VM configuration, remove VM from a cluster, etc.) • Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, etc.) • Perform normal/data-only backup and restore operations. • Manage applications (activate, deactivate, uninstall, add package, etc.) The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.
	Grouping APIs	Grouping management and Topology groups selection tree. The READ permission allows you to view topology UI, while the WRITE permission allows you to create or update groups. The DELETE permission is needed to delete groups from the Grouping Management page. **Note** When READ access is removed for Grouping APIs, in addition to being blocked out of the Grouping window, the users also cannot access the Traffic Engineering, VPN Services, and Topology Services windows.
	View APIs	Views Management in Topology. The READ permission allows you to view views, the WRITE permission allows you to create or update views, and the DELETE permission enables delete capabilities.

Category	Global API Permissions	Description
Topology	Geo	Provides geo service for offline maps. The READ permission allows you to use Geo Map in offline mode, the WRITE allows you to upload Geo Map files, and DELETE permission allows you to delete the map files in settings.
	Topology	Allows you to manage topology pages, settings, or any other pages that uses the Topology visualization framework. The READ permission is mandatory for topology visualization. The WRITE permission enables you to update topology settings, and the DELETE permission allows you to delete a topological link if it goes down.
Proxy	Crosswork Proxy APIs	Permissions to manages Crosswork proxy APIs for NSO Restconf NBI. The READ permission allows all GET request for NSO REST conf NBI, the WRITE permission allows POST/PUT/PATCH operation, and the DELETE permission enables all delete APIs.
Software Image Management	SWIM	Allows you to upload images to the SWIM repository, distribute them to devices and install them. The READ permission allows you to list all images from the SWIM repository, view image information from a device, and check the details of any SWIM job. The WRITE permission allows you to upload/distribute and perform all install-related operations. The DELETE permission allows you to delete copied images from a device. You require WRITE/DELETE permission to execute software install/uninstall playbooks in Change Automation.

Category	Global API Permissions	Description
Service Health	Archiver APIs	The READ permission allows you to • Check if Historical Data exists for a given service. • Get the Historical Timeline series for a given service. • Get a Service Graph for a selected timestamp of the service. • Retrieve probe and 24 hours metric data for a given service. The WRITE/DELETE permissions are not applicable for these APIs.
	Assurance Graph Manager APIs	The READ permission allows you to: • Fetch details of a service. • Get the impacted list of services. • Retrieve the list of matching sub-services (transport or device only). The WRITE/DELETE permissions are not applicable for these APIs.
	CAT SH UI	The READ permission allows you to: • Retrieve service data, including the total number of monitored services, the count of basic services, and the count of advanced services. • Retrieve the number of services based on health status (for example, Good, Degraded, Down, Error, Initiated, and Paused). • Retrieve the number of provisioned and monitored services categorized by service type (L2 and L3). The WRITE/DELETE permissions are not applicable for these API.
	Config Manager APIs	The READ permission allows you to: • Retrieve advanced and total counts of services with monitoring enabled and published. • Force reconciliation with ISTP. The WRITE permission allows you to update the maximum number of services supported for Total and Advanced monitoring. The DELETE permission is not applicable for these APIs.
	Heuristic Package Manager APIs	

Category	Global API Permissions	Description
		Permissions for Heuristic package management and to manage plugins and config profiles for Service Assurance. The READ permission allows you to export heuristic packages, query for heuristic package details (Rules, Profiles, SubServices, Metrics, Plugins), and query for assurance options. The WRITE permission allows you to import heuristic packages and perform all create or update operations. The DELETE permission allows you to perform delete operations (for example, delete the RuleClass, MetricClass, etc.)
	Metric Scheduler APIs	Not Applicable

Category	Global API Permissions	Description
Zero Touch Provisioning	Config Service	The READ permission allows you to • List all day-0 configuration files stored in the ZTP config repository. • Fetch count of day-0 configuration files stored in the ZTP config repository. • Download the day-0 configuration file from the ZTP config repository. • List all device family/device versions and device platforms based on information associated with day-0 config files stored in the CW ZTP repository. The WRITE permission allows you to • Upload the day-0 config file or script to the ZTP config repository. • List/update relevant metadata associated with specific day-0 config files stored in the ZTP config repository The DELETE permission allows you to delete config files and scripts uploaded in the ZTP config repository.
	Image Service	The READ permission allows you to • List all device image files stored in the ZTP image repository. • List all device platform/family names associated with image files stored in the CW ZTP repository. • Download the device image file by ID. The WRITE permission allows you to update relevant metadata associated with specific image files stored in the ZTP image repository. The DELETE permission allows you to delete image files uploaded in the ZTP image repository
	ZTP Service	Allows you to manage the ZTP devices and profiles - add or update/delete into Crosswork Network Controller. The READ permission enables you to fetch ZTP devices, serial number/OVs, profiles, sample data CSV, list ZTP devices, profiles, and export ZTP devices and metadata. The WRITE permission allows you to add ZTP devices, serial numbers/OVs, profiles and add or update the ZTP device's attributes. The DELETE permission allows you to delete ZTP devices, profiles, serial numbers/ownership vouchers.

Category	Global API Permissions	Description
Licensing	Common Licensing Management Service (CLMS) APIs	Permissions for APIs to manage license registration in Crosswork Network Controller. The READ permission enables you to view Smart Licensing settings, registration status, and license usage while the WRITE permission is required to change any Smart Licensing setting such as register, re-register, de-register, renew a license etc. The DELETE permission is not applicable for these APIs.
te-manager	TE Auto Policy Binding Service	The READ permission allows you to view individual or all TE criteria and policy templates. The WRITE permission allows you to create or update TE criteria, criteria expression, and policy templates, and to associate or disassociate TE criteria with policy templates and vice versa. The DELETE permission allows you to delete TE criteria, criteria expression, and policy templates, and remove any residual data associated with a service.
NSO Management	Function Pack Deployment APIs	Permissions for APIs to manage NSO Function Pack deployment.
Path Analytics	Path Analytics - Get Paths	Permissions to access the GET request for Path Analytics paths.
	Path Analytics - Get Registrations/ Register/ Unregister	Permissions to manage the GET request for Path Analytics registrations, register, and unregister.
	Path Analytics - Subscribe	Permissions to manage the Path Analytics subscribe information.
	Path Analytics UI	Permissions to manage the Path Analytics UI.