Role-Based Access Control Custom Roles

Product overview

Role-Based Access Control (RBAC) Custom Roles in the Cisco Meraki® dashboard introduces a more flexible and modern approach to access management. Network administrators can now create custom, product-level roles that align to how their teams work, starting with wireless, switching, and security and SD-WAN.

This capability gives you a secure foundation for a scalable IAM (identity and access management) experience - designed to evolve over time as additional product families, permissions, and levels of granularity are introduced.

Who it’s for

- Network and IT administrators managing access across teams, roles, and sites.
- Managed Service Providers (MSPs) and partners supporting customers with multi-environment operations and varying operational roles.

Benefits

As your organization grows and teams become more distributed, managing admin access with broad, pre-defined roles becomes increasingly difficult to scale. RBAC Custom Roles gives you flexibility to align permissions to real-world responsibilities, helping you improve security, simplify operations, and scale access with greater confidence across your environments.

Enhance security

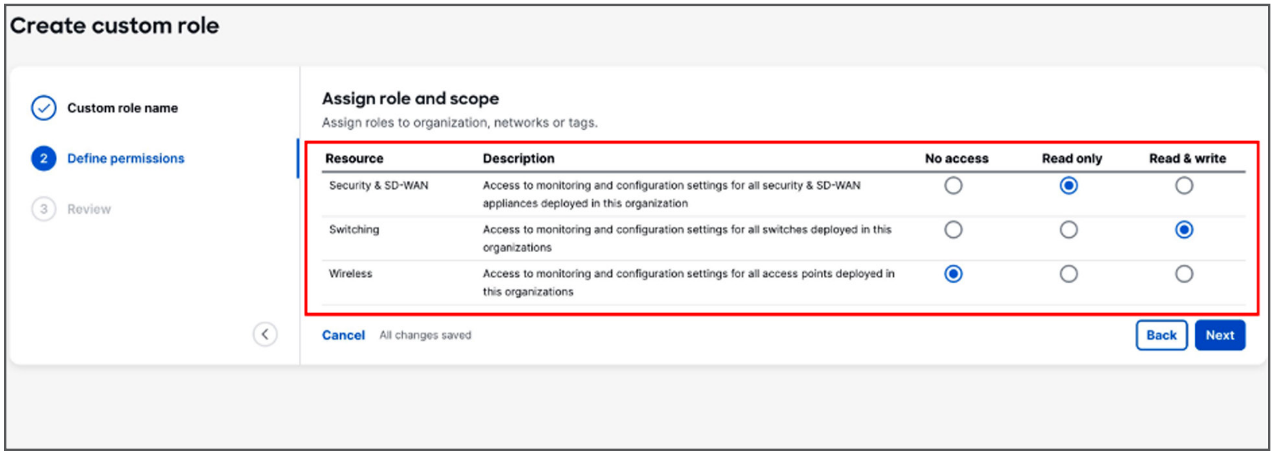
- Limit admin permissions to least-privilege access and reduce risk by only giving access to what’s required.
- Preview and validate role permissions before assigning access, to minimize misconfigurations.
- Increase governance through visibility into who can do what in the dashboard, letting you enhance security audits with a centralized admin profile page.

Simplify operations

- Make operations simpler across networking product families, starting with wireless, switching, and security and SD-WAN, and easily define the admin permission level for each product family to better reflect how your teams manage the network.
- Choose from product-level access options including “read only,” “read and write,” or “no access”.

Scale access

- Standardize roles such as “Switching Manager,” “Auditor,” or “Contractor,” to streamline onboarding and role changes with consistency and less manual effort.
- Perform bulk actions across the organization and create, edit, and manage multiple custom roles easily.



Create custom role

Assign role and scope

Assign roles to organization, networks or tags.

Resource	Description	No access	Read only	Read & write
Security & SD-WAN	Access to monitoring and configuration settings for all security & SD-WAN appliances deployed in this organization	○	●	○
Switching	Access to monitoring and configuration settings for all switches deployed in this organizations	○	○	●
Wireless	Access to monitoring and configuration settings for all access points deployed in this organizations	●	○	○

Figure 1. RBAC Custom Roles in the Meraki dashboard

Learn more

Ready to get started? Access any of our resources below.

- RBAC Custom Roles documentation guide.
- Visit the Meraki dashboard to sign up for the Role-Based Access Control beta.

Key use cases

- **Secure, least-privilege admin access:** grant precise read or write permissions by product to reduce risk while maintaining operational visibility. For example, grant a network engineer full write access to switching, but read-only access to security and SD-WAN appliances.
- **Flexible role-aligned access:** provide limited access without over-provisioning or creating exceptions that are hard to manage long term. For example, restrict contractors to “read only” or “no access” to your wireless devices.
- **MSP and multi-team operations:** standardize and reuse role definitions and assignments across teams or customers to simplify access management while maintaining clear separation of responsibilities.