RUCKUS One Online Help (index.html)

Search

RBAC and ABAC Support

Role-based access control (RBAC) and attributes-based access control (ABAC) are functionalities that provide a structured and efficient approach to managing administrator permissions and access rules in RUCKUS One.

Feature Overview

The RBAC system supports role-based assignments and centralized administration, and operates based on three fundamental principles:

- **Role-Based Assignments**: Assigns users to specific roles based on their responsibilities, job functions, or organizational hierarchy. Roles define sets of permissions and privileges associated with various system resources and operations. For the existing set of roles, refer to *Understanding Administrator Roles and Privileges (GUID-1EB23842-21DF-4A2A-8017-2E70E99511A7.html)*.
- **Permission-Based Access**: Grants permissions to roles rather than individual users. Users inherit the permissions associated with their assigned roles. This approach simplifies access control management by focusing on role assignments rather than individual user accounts.
- **Least Privilege**: Provides the minimum necessary permissions for users to perform their assigned tasks. This principle minimizes the risk of unauthorized access and reduces the potential impact of security breaches.

RUCKUS One allows an administrator in an RBAC system with the required privileges to perform the following actions on a tenant portal:

- Define user roles by customizing permissions and using preconfigured role types and associated privilege groups. Roles can be assigned to different objects, such as venues, networks, and services, and only the users with these roles will have access to those objects. Each user role must have a name and can have multiple resources or access rights mapped to it. For example, a user role

named "Wi-Fi-admin" can be mapped to a custom privilege group called AP-Management with read-write access.

- Create a map that links users with one or more privilege groups, access rights, and hierarchy levels. For example, a custom privilege group named "Wi-Fi-custom-xxx" can be assigned privileges for managing a Wi-Fi network only (AP, WLAN, and associated services such as DHCP and Portal). A Prime Admin can then assign access rights to each of the resources within the Wi-Fi group, such as read-write access to AP settings and read-only access to AP licenses, and assign the privilege group to a "Wi-Fi-custom-admin-xxx" role at a global level or for a specific venue.
- Define permissions by selecting the level of control for each technology, such as Wi-Fi, switch, and RUCKUS Edge.

The ABAC model supports attribute-based access rules based on the user role scoped to a specific entity instance, such as a specific venue instance, with any of the permissions (Read (default), Create, Write, and Delete) assigned.

Correlation between RBAC and ABAC: For example, in an RBAC system, the user roles, such as Administrator and Prime Admin managing configuration templates, can create an ABAC role to apply configuration templates on a specific venue instance.

Requirements

RBAC and ABAC Support feature is being released in the following three phases:

- IEA: Invitation only, please reach out to your Sales representative
- EA: To enable early access features, refer to *Enabling or Disabling RUCKUS One Early Access Features (GUID-406F16F2-39F0-4426-AA80-C15B09CFF494.html)*
- GA: General availability of the feature

Considerations

Consider the following with regards to the RBAC system:

Supported Functionalities

- Supports backward compatibility with existing roles.
- Allows tenant administrators to create custom roles using the composition of scopes defined by the system.
- Allows tenant administrators to restrict access to specific object (venue, network, and so on).
- Allows Managed Service Provider (MSP) tenant administrators to create configuration templates with permissions that can be shared with delegated MSP-EC accounts in a read-only scope. MSP-EC can apply these templates but cannot modify these templates. For more information, refer to "Configuration Template" in the *RUCKUS One MSP Guide*.
- Supports different delegation flows including but not limited to the following customer account types: value-added reseller (VAR), RA, integrator, installer, MSP. For more information on the various customer account types, refer to the *RUCKUS One Software Licensing Guide*.

Hierarchy

The RBAC rules defined at the global level are inherited by all MSPs and tenants. The following hierarchy is supported:

- Global level
- Managed Service Provider (MSP)
- Venue
- Device Group, Services, and other settings

System Resources

When creating roles, the administrator selects the resource groups from the user interface. The following resources are supported:

1. Every UI menu option (level 1 and level 2 menus, including the Dashboard)
2. License management
3. API access
4. Configuration templates
5. RBAC management

Access Rights

- Full access: Read, Create, Write, and Delete operations
- Read only
- No access (feature is not visible)
- Execute (allows a function to be performed, but the function is not editable; for example, an MSP-EC account may apply a configuration template but cannot modify the template)

Best Practices

This feature has no special recommendations for feature enablement or usage.

Prerequisites

This feature has no prerequisites to feature enablement or usage.

800-73730-001 Rev E 29 May 2025