User Groups and Permissions Guide

Overview

The CONTROL platform implements a **role-based access control (RBAC)** system to manage user permissions and data access. Access control is organized through **Groups** — collections of permissions that define which modules, actions, and data a user can access within the platform.

Users can be assigned to **multiple groups simultaneously**, and their effective permissions represent the **union** of all permissions from their assigned groups. This flexible approach allows organizations to create precise permission sets that match their operational roles and security requirements.

Key Concepts

Concept	Description
Group	A named collection of permissions. Users automatically inherit all permissions from their assigned groups.
Permission	A specific action allowed on a specific resource (e.g., "Can view device", "Can change parameter").
Organization	Users can only access data belonging to their organization and its sub-organizations. This organizational boundary is enforced independently of group permissions.
Expert Mode	An optional toggle that reveals advanced features and configuration options for experienced users. Requires assignment to the "Users: Expert mode" group.

Available Groups

The CONTROL platform provides standard groups organized by platform module and access level. These groups cover all core functionality areas:

Group Name	Module	Access Level

CONTROL account admins	CONTROL	Administration
CONTROL API Logs read-only	CONTROL	Read-only
CONTROL inventory admins	CONTROL	Administration
CONTROL inventory basic users	CONTROL	Basic
CONTROL inventory read-only basic users	CONTROL	Read-only (basic)
CONTROL inventory read-only users	CONTROL	Read-only
CONTROL inventory scripting	CONTROL	Specialized
CONTROL inventory users	CONTROL	Standard
CONTROL portal admins	CONTROL	Administration
Link admin users	Link	Administration
Link read-only users	Link	Read-only
SecureDNS admins	SecureDNS	Administration
SecureDNS reports	SecureDNS	Read-only
SONDA admins	SONDA	Administration
SONDA reports	SONDA	Read-only
Users	General	Basic
Users: Expert mode	General	Specialized

Detailed Group Descriptions

CONTROL Account Administration

CONTROL account admins

Description: CONTROL account administration access.

Purpose: Grants administrative control over account-level configuration of the CONTROL platform, including device profile management, parameter configuration, and service settings.

Key Capabilities:

Area	Permissions
Device Profiles (Types)	View, edit, and delete device profiles — the templates that define how the platform communicates with specific CPE device models.

Area	Permissions
Parameters & Groups	View, edit, and delete parameters and parameter groups — the configuration variables used by services (WiFi Analytics, throughput tests, etc.).
Lists & Options	View, edit, and delete list groups — dropdown/selection options used in service configuration.
WiFi Remediation	View remediation policies and manage remediation logs — automatic WiFi optimization actions.
Task Scheduler	View failed tasks and manage successful tasks in the background task queue.
SecureDNS	Add and edit DNS categories; view DNS transaction logs.
Service Settings	View extended service settings.
Revision History	Edit revision entries (audit log management).

Recommended For: Platform administrators responsible for configuring device profiles and service parameters.

CONTROL API Access

CONTROL API Logs read-only

Description: CONTROL read-only API Logs.

Purpose: Provides read-only access to API activity logs, enabling monitoring and auditing of all API transactions made to and from the platform.

Key Capabilities:

Area	Permissions
API Methods	View available API methods and their configurations.
API Transaction Logs	View API transaction logs — records of all API calls made to/from the platform including request/response details.
API Transaction Details	View detailed information for individual API transactions.

Recommended For: Operations staff, auditors, and support teams who need to monitor API activity for troubleshooting or compliance purposes.

CONTROL Inventory Management

CONTROL inventory admins

Description: CONTROL — inventory administration access.

Purpose: Full administrative access to the device inventory system, including device management, service configuration, reporting, and system tools.

Key Capabilities:

Area	Permissions
Devices	Add, edit, and view devices in the inventory. Manage device settings.
Service Configuration	Full CRUD on parameters, parameter groups, lists, list groups, and service classes — the building blocks of all services.
Schedules & Scripts	Create and manage inventory schedules and view script logs.
Reports & Dashboards	View dashboards. Manage report cache data.
Locations	Add locations and manage location groups.
Portal	View and manage portal profiles and templates.
Performance Profiler	Access the SQL query profiler for performance analysis.
User Management	Manage content types, permissions, user profiles, and sessions.
Data Replication	Full control over database replication processes.
WiFi Analytics	Manage WiFi remediation logs; view remediation policies.
SecureDNS	Manage categories, view rules and transaction logs.
Validators	Manage validation rules used by parameters.

Recommended For: Senior administrators and engineering staff who need full control over the inventory and service configuration.

CONTROL inventory users

Description: CONTROL — inventory regular user access.

Purpose: Standard operational access to the device inventory, including device management, parameter editing, and report creation. This is the primary group for day-to-day operations.

Key Capabilities:

Area	Permissions
Custom Reports	Create custom reports for personal use.
Dashboards	Create new dashboards and manage elements.
Service Configuration	Full CRUD on parameters, lists, and validators — configure service behavior for devices.

Area	Permissions
Device Settings	Delete device settings (data cleanup).
Group Variables	Add group variables for device group configurations.
Combined Logs	Access combined device log views.
Portal Templates	Delete portal templates.

Recommended For: NOC operators, field engineers, and support staff who actively manage devices and service configurations.

CONTROL inventory basic users

Description: CONTROL — inventory basic user access.

Purpose: Limited access for users who need to perform basic inventory operations such as creating custom reports and managing specific settings.

Key Capabilities:

Area	Permissions
Custom Reports	Create and delete custom reports — personal report configurations with saved filters.
Dashboard Elements	Remove dashboard widgets from personal views.
Device Settings	Delete device settings (cleanup operations).
Parameters	Delete parameters; view and change validators.
Combined Logs	Access to combined device logs view.

Recommended For: Support staff who need basic report customization and limited inventory access.

CONTROL inventory read-only users

Description: CONTROL — inventory read-only access.

Purpose: Read-oriented access with the ability to create custom reports and dashboards for data visualization.

Key Capabilities:

Area	Permissions
Custom Reports	Create and delete custom reports.
Dashboards	Create dashboards and manage dashboard elements.
Combined Logs	Access combined device log views.

Area	Permissions
Device Settings	Delete device settings (for data cleanup).
Validators	Edit validator configurations.

Recommended For: Monitoring staff and analysts who need to view inventory data and create custom visualizations.

CONTROL inventory read-only basic users

Description: CONTROL — inventory read-only basic access.

Purpose: Minimal access for users who primarily need to view data and create personal reports.

Key Capabilities:

Area	Permissions
Custom Reports	Create and delete custom reports for personal use.
Dashboard Elements	Add widgets to personal dashboard views.
Validators	Edit validator configurations.

Recommended For: Users who need read-only access with the ability to create custom report views.

CONTROL inventory scripting

Description: CONTROL — inventory scripting management and execution.

Purpose: Access to script management and execution capabilities for automating device operations.

Key Capabilities:

Area	Permissions
Scripts	Execute and manage inventory scripts — automated procedures that run against devices (firmware upgrades, bulk configuration, diagnostics).
Script Logs	View execution logs and results from script runs.

Recommended For: Operations engineers who need to run automated scripts against the device inventory.

CONTROL Portal Management

CONTROL portal admins

Description: CONTROL — portal administration access.

Purpose: Administration of the CONTROL end-user portal — the customer-facing interface where end users can view their service status and device information.

Key Capabilities:

Area	Permissions
Portal Pages	Create, edit, and manage portal pages — the content displayed to end users.
Portal Templates	Design and manage page templates that control the portal's appearance.
Portal Profiles	Configure portal user profiles and access levels.
Portal Services	Manage which services are exposed through the portal.

Recommended For: Staff responsible for managing and customizing the customer-facing portal.

Link Management

Link admin users

Description: Link management application administration access.

Purpose: Full administrative access to the Link Management module — used for managing network link associations and interconnections between devices.

Key Capabilities:

Area	Permissions
Links	Create, edit, and delete network links and associations.
Link Services	Manage services associated with links.

Recommended For: Network engineers managing device interconnections and link topology.

Link read-only users

Description: Link management application read-only access.

Purpose: View-only access to the Link Management module.

Key Capabilities:

Area	Permissions
Links	View network links and associations without the ability to modify them.

Recommended For: Support staff who need visibility into network link topology without modification rights.

SecureDNS

SecureDNS admins

Description: SecureDNS — administration access.

Purpose: Administrative access to the SecureDNS module — the DNS-based security filtering system that protects devices from malicious domains.

Key Capabilities:

Area	Permissions
DNS Rules	Create, edit, and delete DNS filtering rules — define which domains are blocked, allowed, or redirected.
Categories	Manage DNS categories (malware, phishing, adult content, etc.).
Transaction Logs	View DNS query logs and filtering statistics.
Service Settings	Manage SecureDNS service configuration.

Recommended For: Security operations staff managing DNS-based protection policies.

SecureDNS reports

Description: SecureDNS — reports and transactions access.

Purpose: Read-only access to SecureDNS reporting and transaction data.

Key Capabilities:

Area	Permissions
Reports	View DNS filtering statistics, top blocked domains, category breakdowns, and response time metrics.
Transaction Logs	View DNS query logs to analyze filtering activity.

Recommended For: Analysts and managers who need visibility into DNS security metrics without the ability to modify rules.

SONDA (User Experience Monitoring)

SONDA admins

Description: SONDA / User experience — administration access.

Purpose: Administrative access to the SONDA module — the user experience monitoring system that runs automated tests (latency, jitter, throughput, WiFi quality) from probes and CPE devices.

Key Capabilities:

Area	Permissions
Events	View and delete events — automated alerts triggered by test results exceeding thresholds.
Event Patterns	Create event patterns — define which conditions trigger automated alerts.
Event Origins	Manage event origins — configure the sources (probes, devices) that generate events.
Event Logs	Add detailed event log entries.
Test Profiles	Configure test profiles that define which tests run on which schedules.
Test Services	Manage test service definitions (ping, throughput, WiFi analytics, etc.).

Recommended For: Engineers configuring automated quality of experience (QoE) monitoring and alert thresholds.

SONDA reports

Description: SONDA / User experience — reports and transactions access.

Purpose: Read-only access to SONDA test results, metrics, and event data.

Key Capabilities:

Area	Permissions
Event Logs	View and edit event log entries.
Event Origins	View and edit event origin configurations.
Test Results	View test results — latency, jitter, throughput, WiFi scores, and other QoE metrics collected from probes and devices.
Reports	Access SONDA dashboards and metric reports.

Recommended For: Operators and analysts monitoring service quality metrics.

General User Access

Users

Description: Regular users — access to user's profile, change password operations, etc.

Purpose: Minimal access for basic user self-service operations.

Key Capabilities:

Area	Permissions
User Profile	View own user profile and personal information.
Password	Change own password.
Site Settings	View basic site configuration.

Recommended For: Users who only need to manage their own account, such as portal-only users or external collaborators with limited access.

Users: Expert mode

Description: Expert mode users — users that can activate the "Expert Mode" option in admin interfaces.

Purpose: Enables the "Expert Mode" toggle in the admin interface. When activated, Expert Mode reveals advanced fields, options, and actions that are hidden by default to prevent accidental changes.

Key Capabilities:

Area	Permissions
Expert Mode Toggle	Access to the Expert Mode switch in the admin interface. When activated, shows advanced fields in device profiles, parameters, services, and other admin forms.
Configuration Profiles	Create new configuration profiles — advanced device provisioning templates.
Advanced Actions	In Expert Mode, additional actions become available on models that normally restrict certain operations (e.g., audit records, firmware logs).

Recommended For: Senior engineers and administrators who need access to advanced configuration options. This group should be assigned selectively to users who understand the implications of advanced configuration changes.

Recommended Group Combinations by Role

Users are typically assigned **combinations of groups** that together define their operational role. The following combinations provide templates for common organizational roles:

Monitoring and Read-Only Roles

Role	Recommended Groups	Description
Basic Monitoring	• CONTROL API Logs read-only • CONTROL portal admins	View the admin interface and manage the customer portal. Suitable for NOC operators focused on monitoring.
Monitoring + Inventory	• CONTROL API Logs read-only • CONTROL inventory users • CONTROL portal admins	Monitoring with additional inventory management capabilities.

Operations Roles

Role	Recommended Groups	Description
Standard Operations	• CONTROL account admins • CONTROL API Logs read-only • CONTROL inventory users	Account and inventory management for daily operational tasks.
Operations + Security	• CONTROL account admins • CONTROL API Logs read-only • CONTROL inventory users • SecureDNS admins	Full operational access including DNS-based security management.
Operations + Scripting	• CONTROL account admins • CONTROL API Logs read-only • CONTROL inventory scripting • CONTROL inventory users	Operational access with script execution capabilities for bulk device operations.

Engineering Roles

Role	Recommended Groups	Description
Engineering	• CONTROL account admins • CONTROL API Logs read-only • CONTROL inventory users • Users: Expert mode	Full configuration access with advanced/expert features enabled.

Role	Recommended Groups	Description
Engineering + Links	• CONTROL account admins • CONTROL API Logs read-only • CONTROL inventory users • Link read-only users • Users: Expert mode	Engineering access with network link visibility.

Administrative Roles

Role	Recommended Groups	Description
Full Administrator	• CONTROL account admins • CONTROL API Logs read-only • CONTROL inventory admins • CONTROL portal admins • Users: Expert mode	Full access to all CONTROL modules with expert capabilities.
SONDA Administrator	• SONDA admins • SONDA reports	Full access to user experience monitoring and reporting.
SecureDNS Administrator	• SecureDNS admins • SecureDNS reports	Full access to DNS security management and reporting.

Minimal Access Roles

Role	Recommended Groups	Description
Portal-only User	• Users	Basic self-service access only (profile, password).
API Auditor	• CONTROL API Logs read-only	Read-only access to API transaction logs for auditing purposes.

> **Note:** These are recommended starting points. Adjust group assignments based on your organization's specific needs and security policies.

Organization-Based Access Control

In addition to group-based permissions, the CONTROL platform enforces **organization-based data isolation**:

- **Organization Membership:** Each user belongs to a specific **Organization**.
- **Data Visibility:** Users can only see and manage data (devices, services, reports, etc.) that belongs to their own organization and its sub-organizations.

- **Public Groups:** Groups marked as "public" are shared across sub-organizations, allowing parent organizations to define standard roles for all child organizations.
- **Isolation Enforcement:** This organizational boundary is enforced independently of group permissions.

This means two users with identical group assignments but different organizations will see different sets of devices and data, ensuring proper data isolation in multi-tenant environments.

Best Practices

Security and Access Management

1. **Principle of Least Privilege**
   - Assign only the groups necessary for each user's role
   - Start with minimum required groups and add more as needed
   - Regularly review and remove unnecessary permissions
2. **Expert Mode Caution**
   - Only assign "Users: Expert mode" group to users who understand the implications of advanced configuration changes
   - Document which users have Expert Mode access and why
3. **Regular Audits**
   - Periodically review user-to-group assignments to ensure they match current job responsibilities
   - Audit organization assignments and data access patterns
   - Review and clean up unused or inactive user accounts

Role Management

4. **Use Standard Combinations**
   - Follow the recommended role patterns documented above to maintain consistency across your organization
   - Create standardized role definitions that can be applied consistently
5. **Document User Roles**
   - Use the user "klass" (class/role) field to document each user's organizational role
   - Maintain documentation of group combinations used for different job functions
   - Keep records of why specific permission combinations were granted

Multi-Organization Deployments

6. **Leverage Public Groups**
   - Use public groups for standard roles shared across sub-organizations

- Define parent-level role templates that can be inherited by child organizations
- Maintain consistent role definitions across organizational boundaries

Platform Modules Reference

Module	Description	Administrative Groups	Reporting Groups
CONTROL Inventory	Device management, profiles, parameters, settings, and monitoring	• CONTROL account admins • CONTROL inventory admins • CONTROL inventory users	• CONTROL inventory read-only users • CONTROL inventory read-only basic users
CONTROL Portal	Customer-facing portal for end-user access	• CONTROL portal admins	—
CONTROL Scripting	Automated script execution against devices	• CONTROL inventory scripting	—
CONTROL API	API transaction monitoring and auditing	—	• CONTROL API Logs read-only
Link Management	Network link and device interconnection management	• Link admin users	• Link read-only users
SecureDNS	DNS-based security filtering	• SecureDNS admins	• SecureDNS reports
SONDA	User experience monitoring (QoE tests, probes)	• SONDA admins	• SONDA reports
General	User profile and expert mode access	—	• Users • Users: Expert mode

Revision #1
Created 2026-04-07 03:06:57 UTC by mauro@zequenze.com
Updated 2026-04-07 03:06:57 UTC by mauro@zequenze.com