LOGZILLA DOCUMENTATION

Role Based Access Control

Configure LogZilla RBAC with group-based permissions, UI component restrictions, host and subnet filtering, and fine-grained feature controls

Administration · Generated April 29, 2026 · logzilla.ai/docs/administration/role-based-access-control

LogZilla's Role-Based Access Control (RBAC) system provides granular control over user access to system resources, data, and functionality. RBAC enables administrators to create groups with specific permissions and restrict user access based on their organizational roles and responsibilities.

Important: RBAC must be enabled in the system settings before groups and permissions can be configured. Navigate to **Settings** → **System Settings** → **Generic** and ensure **RBAC_ENABLED** is set to **true**.

RBAC Overview

LogZilla's RBAC system provides access control through:

- **Group-Based Permissions**: Organize users into groups with specific access rights
- **UI Component Control**: Restrict access to dashboards, search, triggers, and other interface elements
- **Host-Based Filtering**: Limit data visibility to specific hosts, IP ranges, or subnets
- **User Management**: Assign users to multiple groups with inherited permissions
- **Granular Controls**: Fine-tune access to individual system features

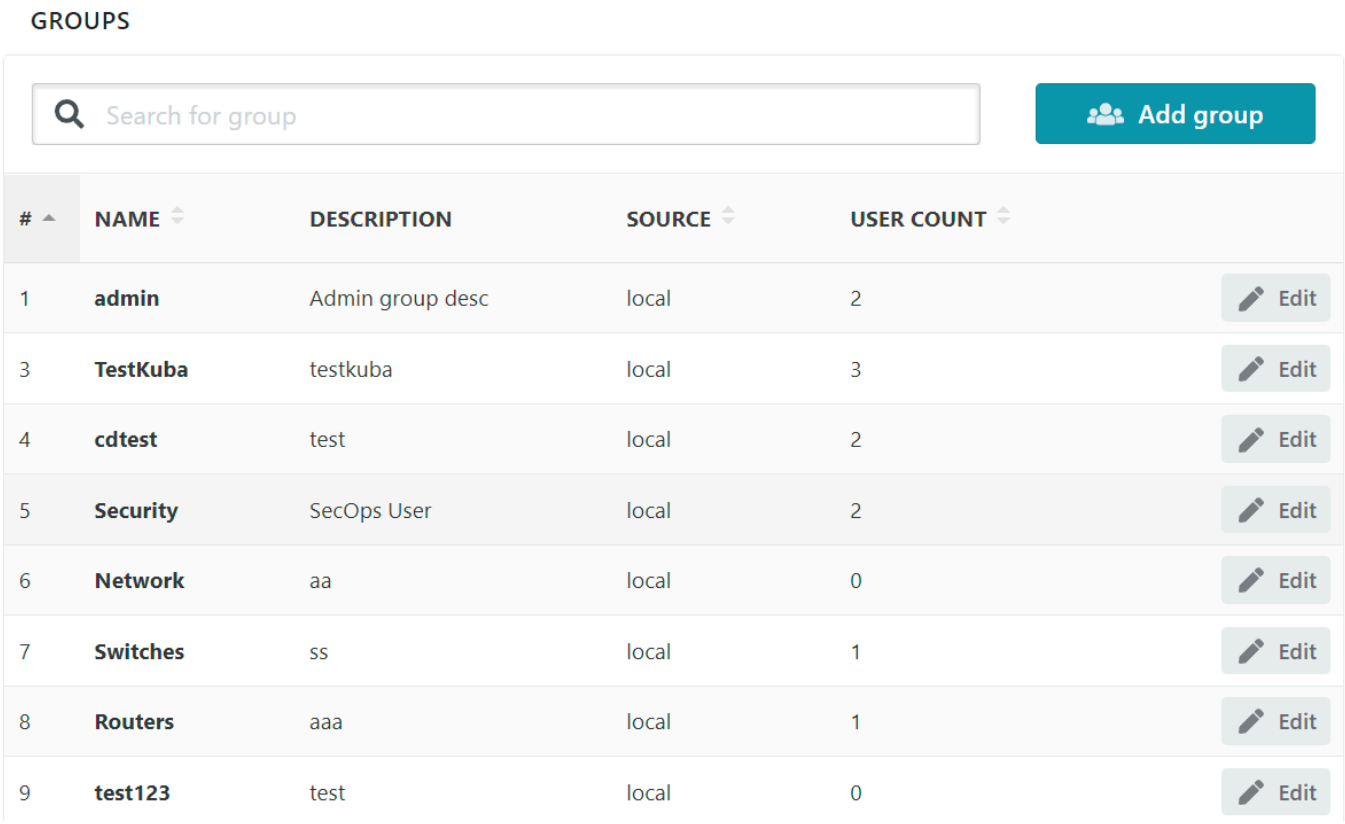
Managing Groups and Permissions

Web Interface Management (Recommended)

The **recommended approach** for managing RBAC is through the LogZilla web interface:

Accessing RBAC Settings
Navigate to User Management:

- Log into LogZilla as an administrator
- Go to **Settings** → **Users & Groups**
- Select the **Groups** tab to view existing groups



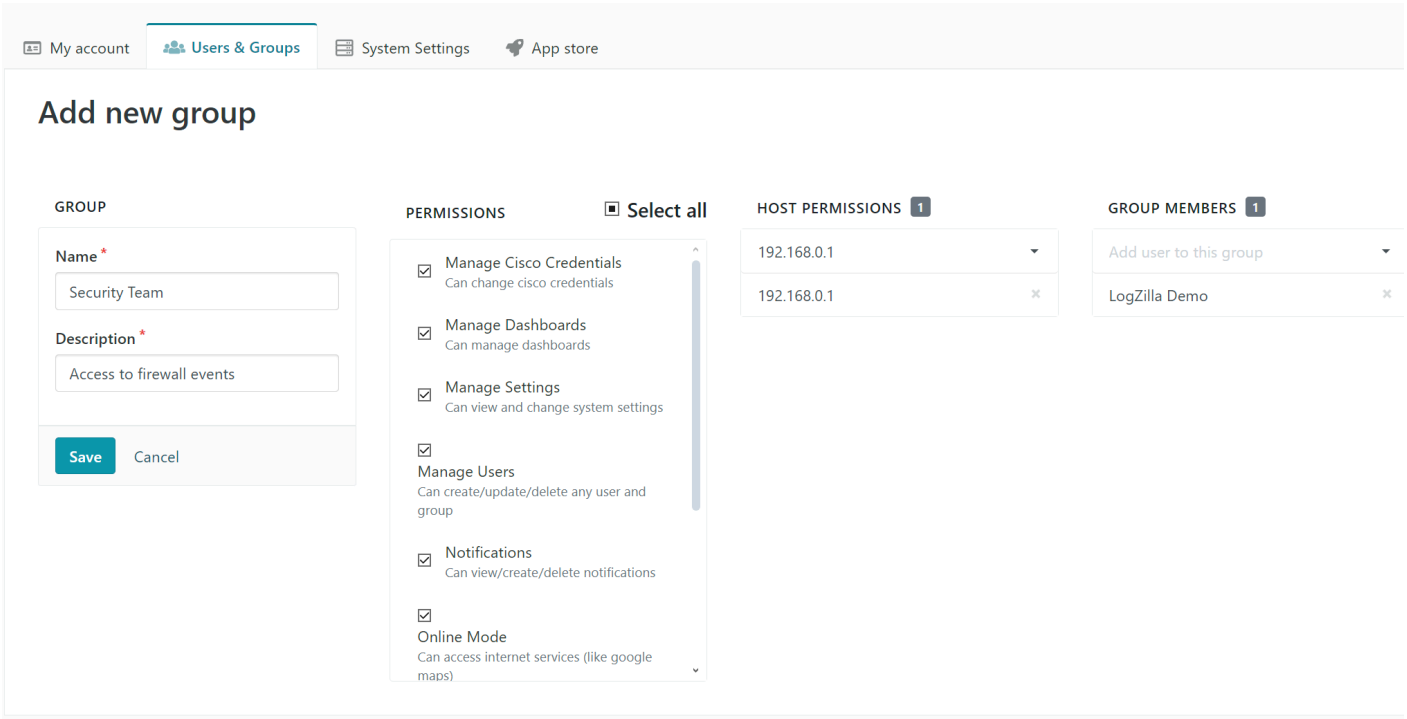
Creating New Groups

Start Group Creation:

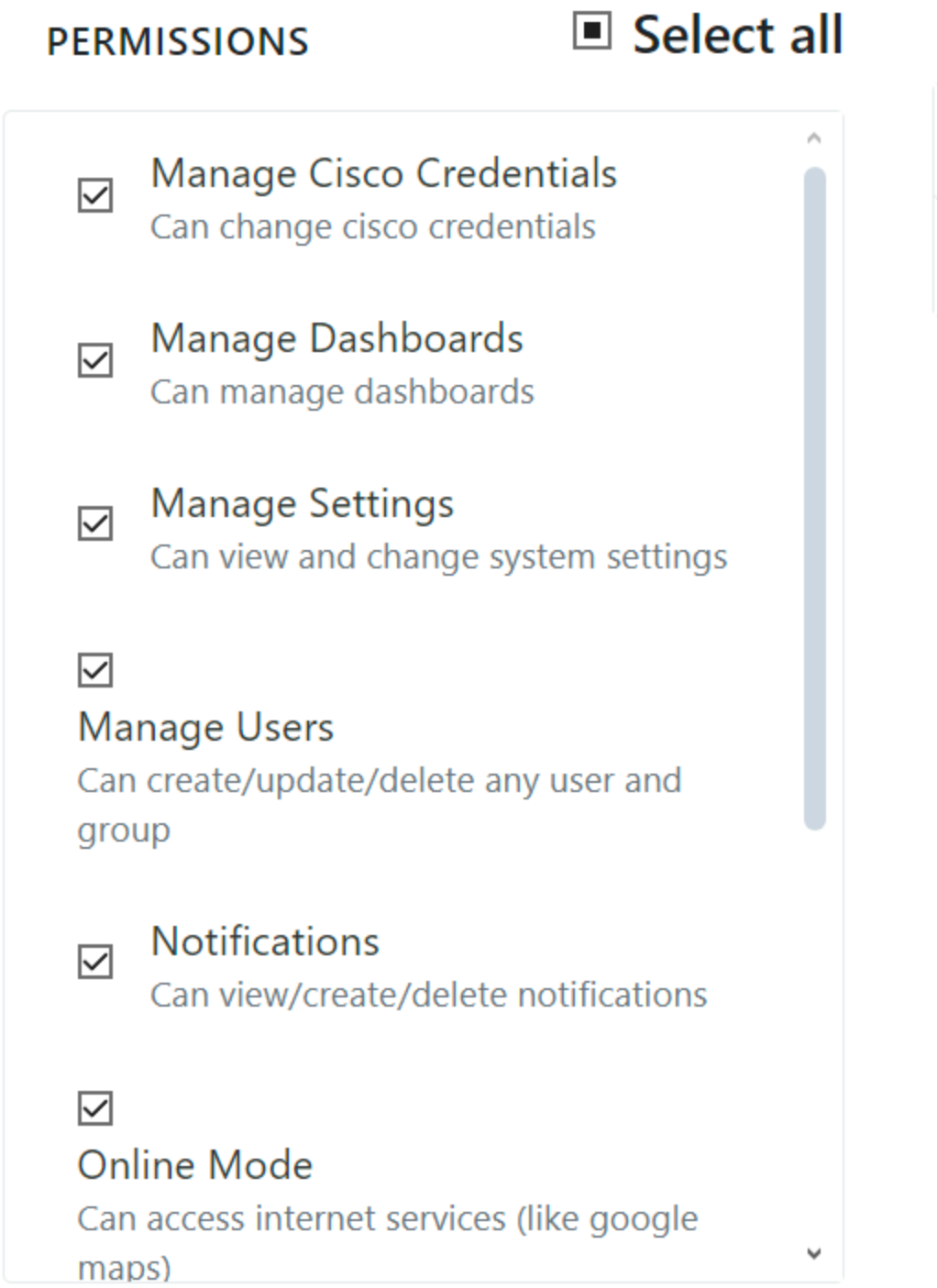
- Click the **"Add group"** button in the Groups interface
- This opens the group configuration form

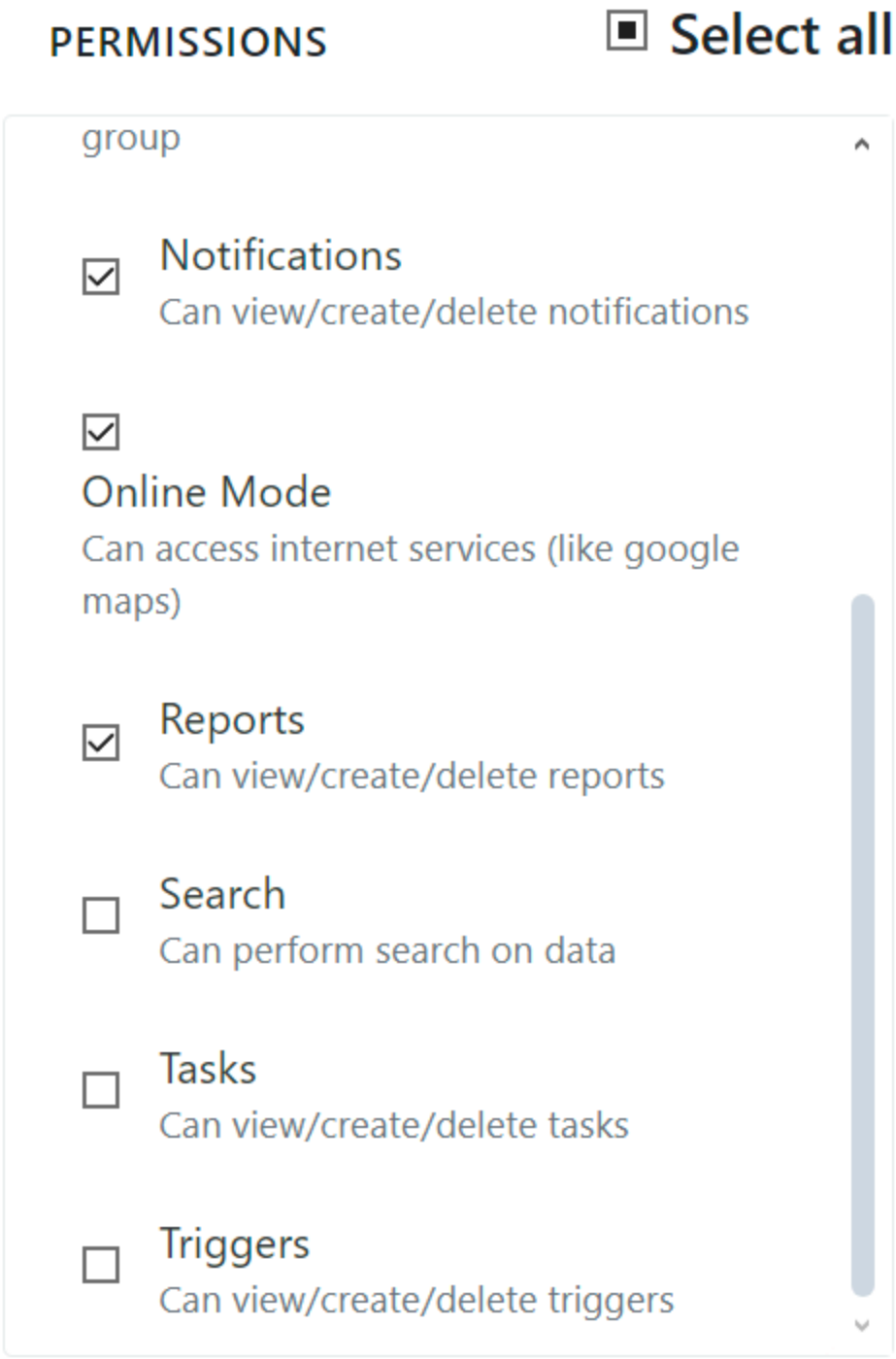
Configure Basic Group Information:

- **Name**: Enter a descriptive group name (e.g., "Security Team", "Network Operators")
- **Description**: Provide a detailed description of the group's purpose



Set UI Permissions:


PERMISSIONS
Select all
Manage Cisco Credentials
Can change cisco credentials
Manage Dashboards
Can manage dashboards
Manage Settings
Can view and change system settings
Manage Users
Can create/update/delete any user and group
Notifications
Can view/create/delete notifications
Online Mode
Can access internet services (like google maps)



- **Individual Permissions**: Check specific permissions for granular control:
  - **Manage Cisco Credentials**: Change Cisco credentials
  - **Manage Dashboards**: Create, edit, and delete dashboards
  - **Manage Settings**: Change system settings
  - **Manage Users**: Create, edit, and delete users
  - **Notifications**: View and manage alert notifications

  - **Online Mode**: Access external internet services
  - **Reports**: Can view/create/delete reports
  - **Search**: Perform log searches and queries
  - **Tasks**: Can view/create/delete tasks
  - **Triggers**: Create and manage automated triggers
- **Select All**: Enable all available UI permissions for full access
- **Permission Descriptions**: Each permission includes helpful descriptions

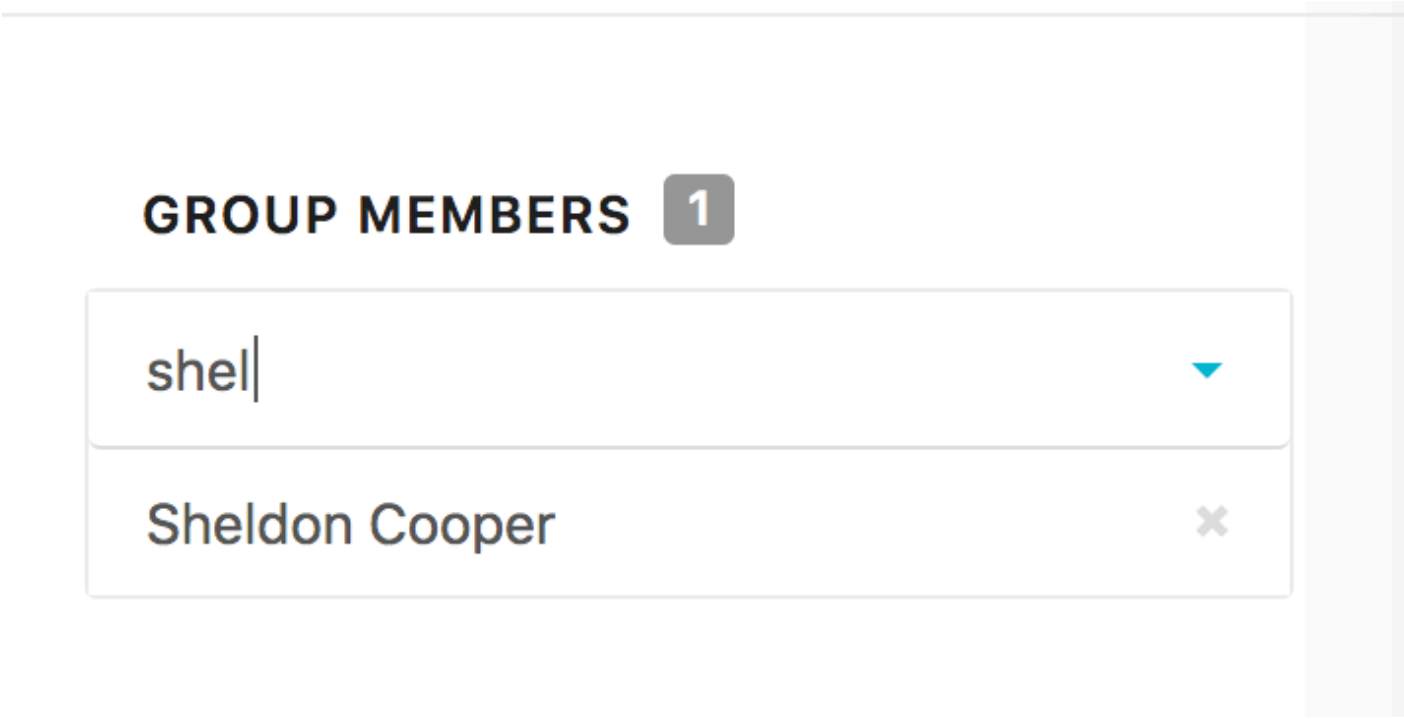
Configure Host Permissions:

- **Add Specific Hosts**: Enter individual hostnames or IP addresses
- **Use Wildcards**: Implement pattern-based filtering:
  - `192.168.28.*` - Entire subnet access
  - `web-server-*` - All hosts matching pattern
  - `*.company.com` - All hosts in domain
- **Multiple Entries**: Add multiple host patterns for complex filtering

Assign Group Members:

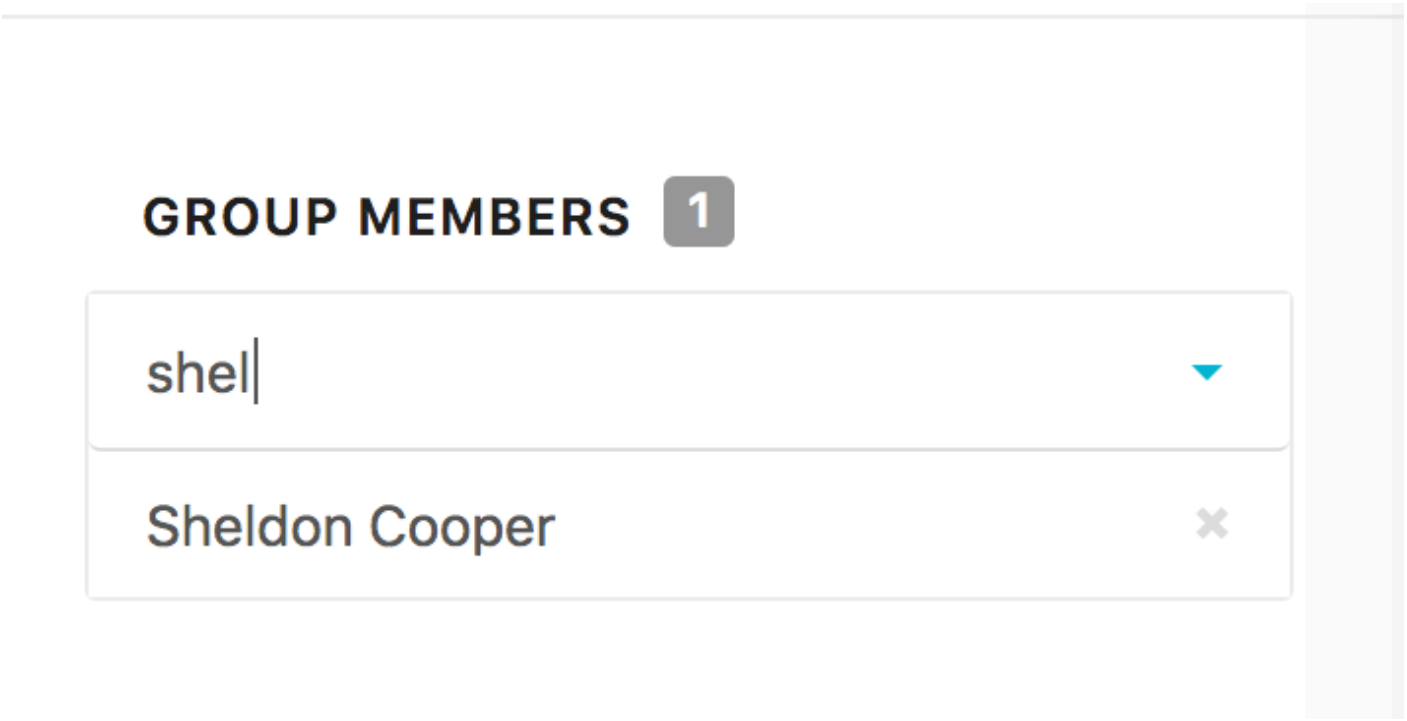
- **Search Users**: Type to search for existing users
- **Select Members**: Choose users to add to the group
- **Multiple Selection**: Add multiple users simultaneously

- **User Display**: Shows full names for easy identification



Assign Group Members:

- **Search Users**: Type to search for existing users
- **Select Members**: Choose users to add to the group
- **Multiple Selection**: Add multiple users simultaneously
- **User Display**: Shows full names for easy identification



Save and Apply:

- Click **"Save"** to create the group
- Changes take effect immediately
- Users receive new permissions upon next login

Advantages of Web Interface:

- **Visual permission management** with clear descriptions
- **Real-time validation** of host patterns and user selections
- **Intuitive group creation** with guided workflows
- **Immediate feedback** on configuration changes
- **No command-line knowledge required**

Advanced: Command Line Management

Note: Command-line RBAC management is provided for advanced users who specifically require shell access or automated group management. Most users should use the web interface above for better user experience and validation.

For advanced users who prefer command-line administration:

```
# Enable RBAC system-wide
logzilla settings update RBAC_ENABLED=true
```

```
# View current RBAC settings
logzilla settings list generic | grep RBAC
```

- Users receive new permissions upon next login

Advantages of Web Interface:

- **Visual permission management** with clear descriptions
- **Real-time validation** of host patterns and user selections
- **Intuitive group creation** with guided workflows
- **Immediate feedback** on configuration changes
- **No command-line knowledge required**
- **Built-in help text** for each permission type

Permission Types and Capabilities

UI Permissions

Permission	Description (paraphrased)	Impact
Manage Cisco Credentials	Modify stored Cisco device credentials for integrations	Integration access and device connectivity
Manage Dashboards	Create, update, and remove dashboards	Full dashboard control
Manage Settings	Change global system configuration	System-wide configuration changes
Manage Users	Create, edit, and delete user accounts	User lifecycle and access management
Notifications	View and manage alert notifications	Alert system access
Online Mode	Allow access to external internet services	External connectivity
Reports	View, create, and delete reports	Reporting data creation and removal
Search	Perform log searches and queries	Core search functionality
Tasks	View, create, and delete tasks	Task workflow management
Triggers	Create and manage automated triggers	Automation control

Host Permissions

Exact Matching:

- `192.168.1.100` - Specific IP address
- `web-server-01` - Specific hostname
- `mail.company.com` - Specific FQDN

Wildcard Patterns:

- `192.168.1.*` - Entire subnet (192.168.1.0/24)
- `192.168.*.*` - Larger subnet range
- `web-server-*` - All hosts starting with "web-server-"
- `*.company.com` - All hosts in company.com domain
- `*database*` - Any host containing "database"

Multiple Patterns:

- Combine multiple patterns for complex filtering
- Each pattern is evaluated independently
- Users see logs from ANY matching pattern

User Management

Assigning Users to Groups

During Group Creation: Add users when creating new groups
Edit Existing Groups: Modify group membership anytime
Multiple Group Membership: Users can belong to multiple groups
Permission Inheritance: Users inherit ALL permissions from ALL groups

User Permission Resolution

Additive Permissions: Users receive the union of all group permissions **Host Access**: Users can access hosts from ALL assigned groups **UI Access**: Users get the broadest UI permissions from any group

Best Practices

Security

- **Principle of Least Privilege**: Grant minimum necessary permissions
- **Regular Audits**: Periodically review group memberships and permissions
- **Role-Based Design**: Create groups based on job functions, not individuals
- **Host Segmentation**: Use specific host patterns rather than broad wildcards

Organization

- **Descriptive Names**: Use clear, meaningful group names
- **Detailed Descriptions**: Document group purposes and intended users
- **Logical Grouping**: Organize permissions by department or function
- **Documentation**: Maintain records of RBAC decisions and changes

Performance

- **Efficient Patterns**: Use specific host patterns to reduce processing overhead
- **Group Optimization**: Avoid excessive group proliferation
- **Regular Cleanup**: Remove unused groups and inactive users

Common Use Cases

Network Operations Team

Permissions: Search, Dashboards, Notifications **Host Access**: `router-*`, `switch-*`, `firewall-*` **Purpose**: Monitor network infrastructure

Security Team

Permissions: All UI permissions **Host Access**: `*` (all hosts) **Purpose**: Full system access for security monitoring

Application Support

Permissions: Search, Dashboards **Host Access**: `app-server-*`, `web-server-*` **Purpose**: Monitor specific application infrastructure

Database Administrators

Permissions: Search, Dashboards, Triggers **Host Access**: `db-*`, `*database*` **Purpose**: Monitor and manage database systems

Troubleshooting

Common Issues

Users Cannot Access Expected Data:

Verify RBAC is enabled in system settings
Check user group memberships
Verify host permission patterns
Confirm UI permissions are granted
Host Patterns Not Working:

Test patterns with specific examples
Verify wildcard syntax (`*` for any characters)
Check for typos in hostnames or IP addresses
Ensure patterns match actual log data
Permission Changes Not Applied:

Users may need to log out and back in
Verify group configuration was saved
Check for conflicting group memberships
Confirm RBAC system is enabled

Verification

```
# Check if RBAC is enabled
logzilla settings list generic | grep RBAC_ENABLED

# Verify user can see expected hosts in search results
# (This verification is done through the web interface)
```

Example: Security Team Configuration

This example demonstrates creating a security team group:

Group Configuration:

- **Name**: "Security Team"
- **Description**: "Full access for security monitoring and incident response"
- **UI Permissions**: All permissions enabled
- **Host Permissions**: `*` (all hosts)
- **Members**: Security analysts and incident responders

Result: Security team members can:

- Access all system logs from any host
- Create and manage dashboards
- Set up automated triggers for security events
- Receive and manage security notifications
- Perform searches across all data

In this configuration, a user like "Sheldon Cooper" assigned to a group with `192.168.28.*` host permissions would only see log events from devices in the 192.168.28.0/24 subnet, providing effective data segmentation for role-based access control.