LABYRINTH

ROLE-BASED ACCESS CONTROL

Labyrinth Deception Platform, 2023

https://labyrinth.tech

info@labyrinth.tech

Labyrinth Development

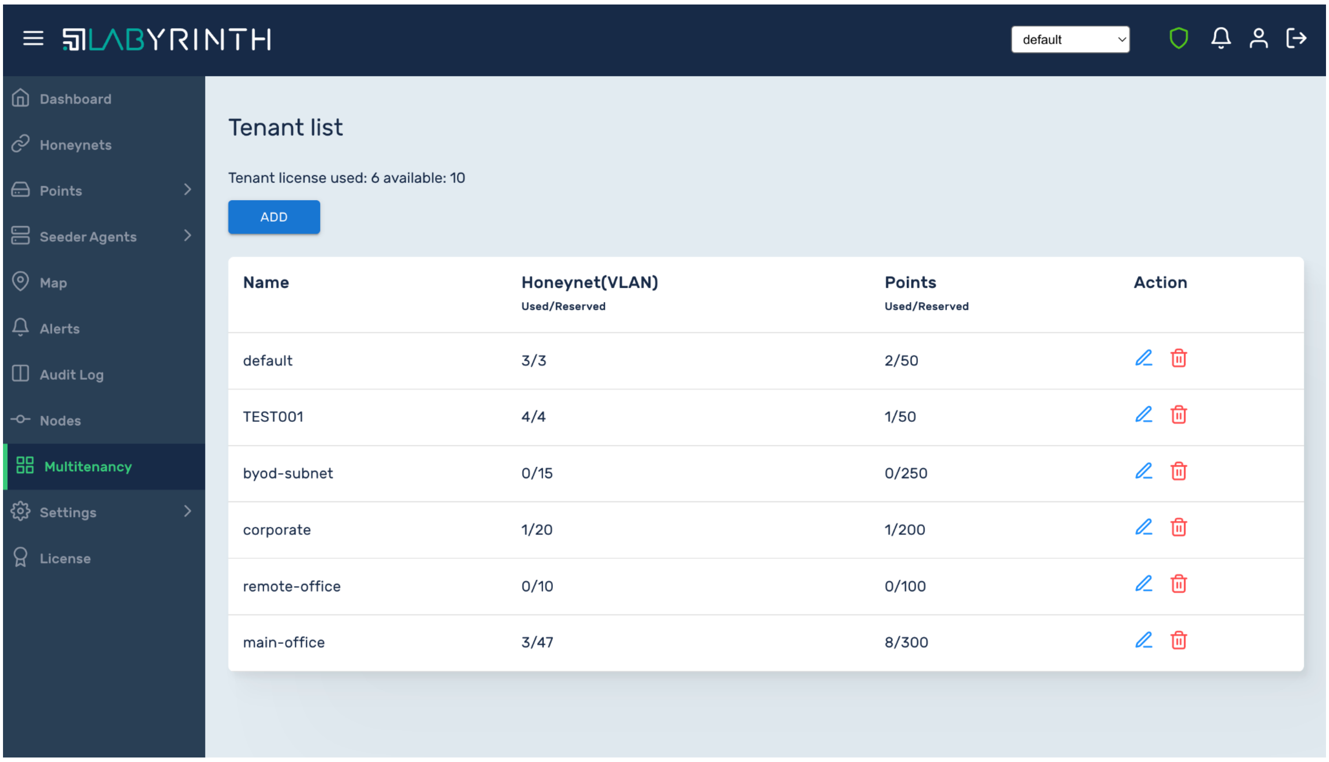
1. MULTITENANCY

In simple terms, multitenancy is the ability of different users or companies to use resources in **isolation** within the same service (one installation or deployment).

Thus, today's multi-tenant architecture is one of the most efficient models for delivering IT services and is a fundamental way to save computing resources and disk storage. A single instance of an application running on a single server infrastructure but available to multiple users and businesses simultaneously helps minimize the cost of providing IT services and maximize their quality.

The division into tenants within the Labyrinth has the following components:

1. **"Default" tenant** whose users have access to all tenants (superusers). The user's role determines access rights;
2. Other tenants have their own users with a scope limited only to their own tenants.



Tenant list

Tenant license used: 6 available: 10

Name	Honeynet(VLAN) Used/Reserved	Points Used/Reserved	Action
default	3/3	2/50	✎ 🗑
TEST001	4/4	1/50	✎ 🗑
byod-subnet	0/15	0/250	✎ 🗑
corporate	1/20	1/200	✎ 🗑
remote-office	0/10	0/100	✎ 🗑
main-office	3/47	8/300	✎ 🗑

The so-called "zero" tenant is an Organization/Division/Department whose task is to provide services for other Client Organizations.

2. RBAC'S ESSENCE

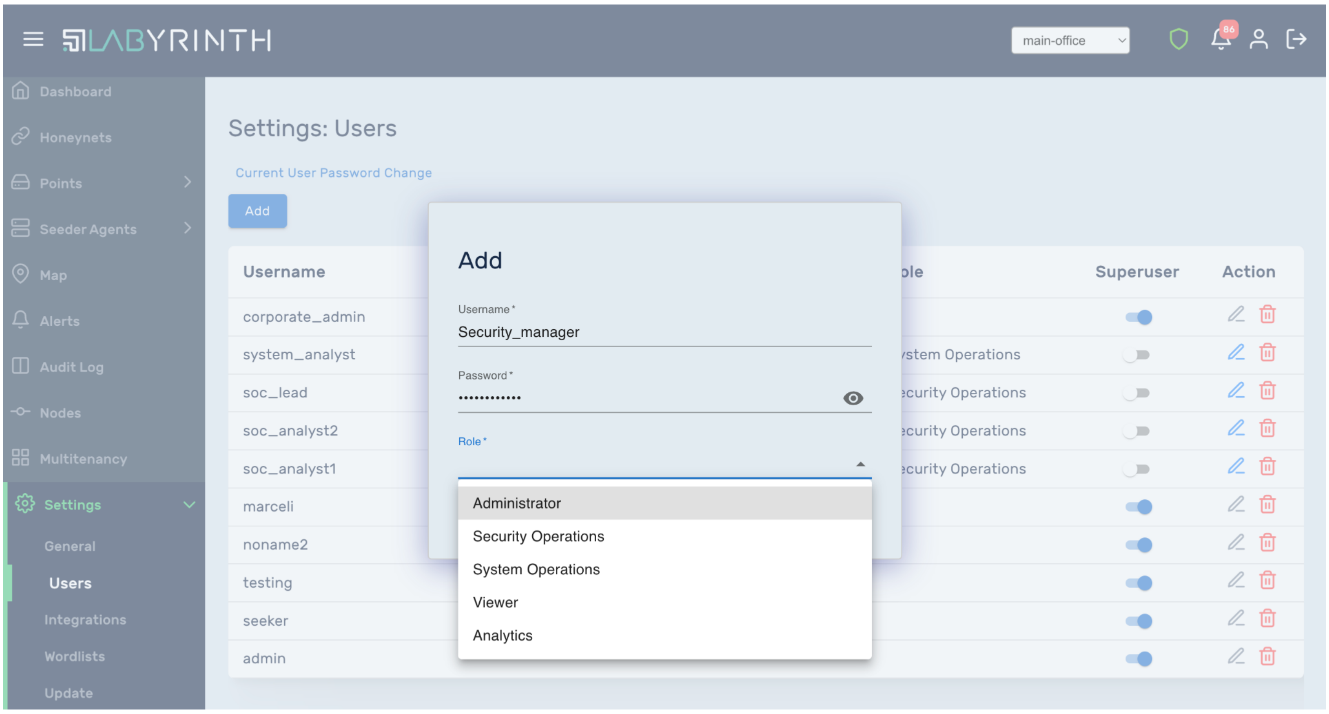
The essence of the RBAC (Role-based access control) approach is to create roles that mirror business roles in the company and assign them to users. The user's ability to perform a particular action is checked based on these roles.

2.1. Role

The role is a template of privileges and accesses in the system defined when a user is created. Later it can be changed by the Superuser or a user of this tenant with the Administrator role.

There are five roles for users within a tenant for a newly created user:

1. The **Administrator** is a role with full rights within a tenant. A user with this role can create other users within the tenant, including those with the Administrator role.
2. **System Operations** is a role that has access to system components for configuration. Data on security incidents is not available.
3. **Security Operations** is a role designed to handle security incidents. This role has access to data on detected attacks (Alerts) and Honeynet, Point, and Seeder management, but does not have access to system settings within the tenant.
4. **Analytics** - a role that only has access to data about security incidents.
5. **Viewer** is a role which is similar to the Administrator role but in read mode.



Settings: Users

Current User Password Change

Add

Username * Security_manager

Password * ••••••••••••

Role *

- Administrator
- Security Operations
- System Operations
- Viewer
- Analytics

Username	ole	Superuser	Action
corporate_admin		●	
system_analyst	ystem Operations	○	
soc_lead	ecurity Operations	○	
soc_analyst2	ecurity Operations	○	
soc_analyst1	ecurity Operations	○	
marceli		●	
noname2		●	
testing		●	
seeker		●	
admin		●	

2.2. User type

The user type defines a set of access permissions to one or more tenants and the corresponding privileges.

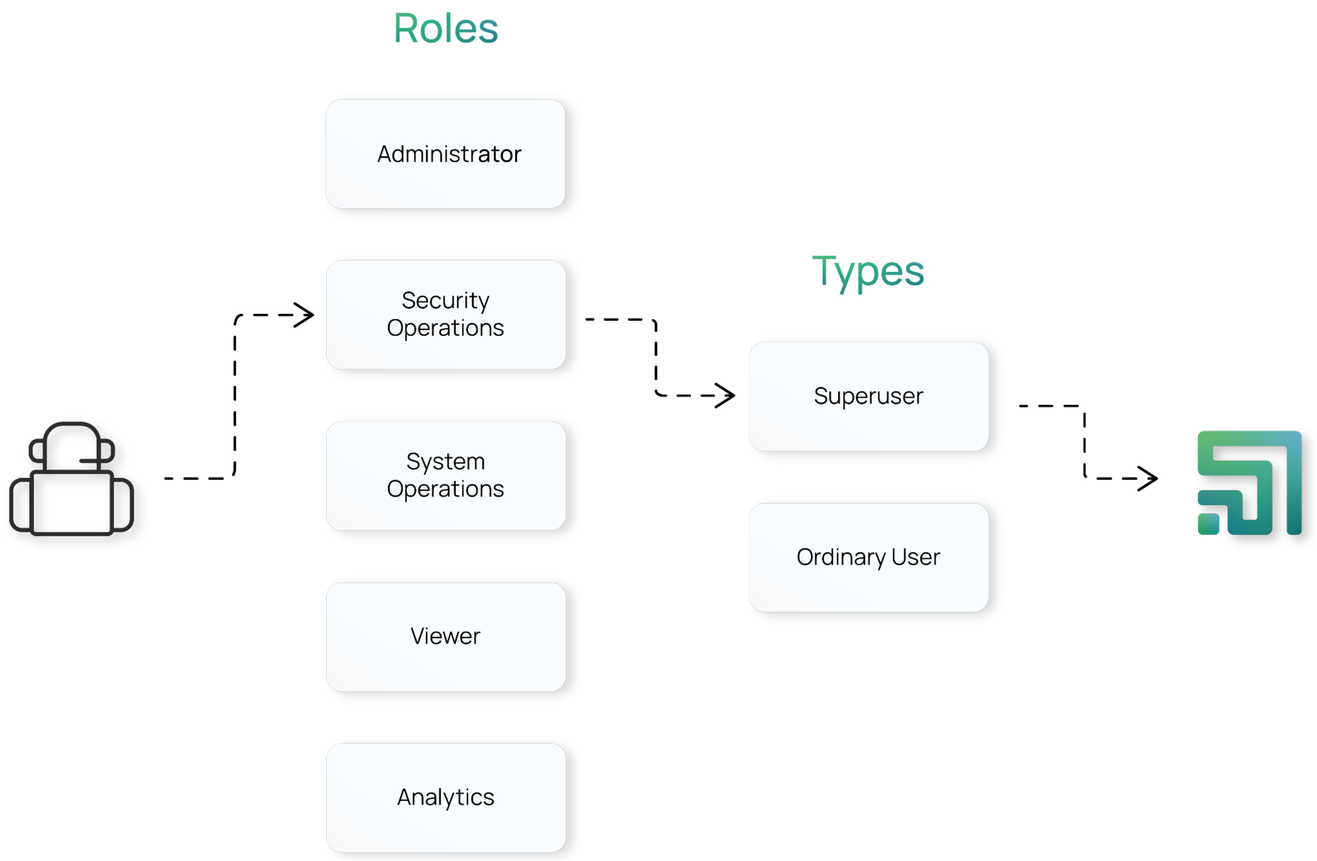
There are two types of users in the system:

1. Superusers;
2. Regular tenant users.

The Superuser type includes the highest privileges in the system:

- switching to any tenant;
- management of the Multitenancy menu section;
- system updates;
- global system settings;
- creating new users of the Superuser type.

Tenant users function only within their tenant based on their assigned role. They have access to the data of their tenant only.


Roles
Administrator
Security Operations
System Operations
Viewer
Analytics
Types
Superuser
Ordinary User