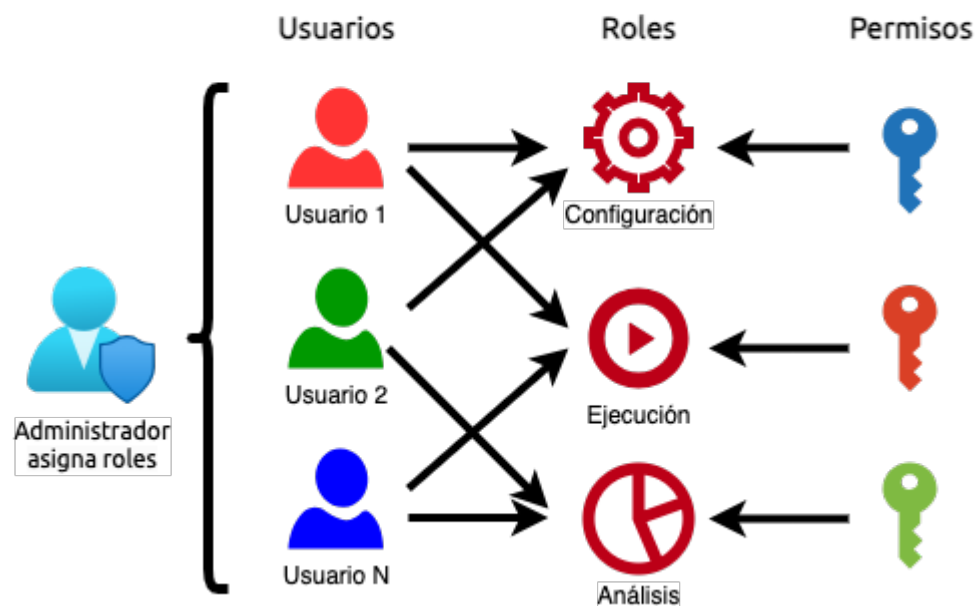


Orquestador Rocketbot – Acceso y Autenticación

El Orquestador de Rocketbot o R.O.C. cuenta con acceso basado en roles RBAC y doble autenticación o 2FA.

Control de Acceso Basado en Roles - RBAC



Importante: Deberá tener habilitado en su red/proxy y políticas de seguridad el ingreso por HTTPS a las url [REDACTED] y [REDACTED] para poder consumir las API's de orquestador

Acceso basado en Roles – RBAC

El acceso a las partes y componentes del Orquestador (R.O.C.) están controladas por RBAC (Role-Based Access Control) la cual permite dependiendo el ROL del usuario realizar una acción como ejecutar un robot o ver el log.

Cuando Rocketbot crea una cuenta para **EMPRESA** se genera un usuario administrador para esa empresa. Este administrador tiene la tarea de designar los roles necesarios además del rol "Administrador" existente.

Crear un ROL

Para crear un rol debe:

1. Hacer click en el menú **Users&Roles -> Roles**.
2. Click en el botón **Add Role**
3. Asignar un nombre y habilitar la acciones posibles



Asignar un ROL

Para asignar un ROL se debe crear o editar un Usuario y seleccionar el rol para ese usuario.

Ver imagen



Doble Autenticación 2FA

El Orquestador de Rocketbot cuenta con Doble autenticación o two-factor 2FA.

Esto exigirá que para el inicio de sesión debiera tener un token a través de una app de autenticación.

Aplicaciones móviles compatibles.

- [Google Authenticator](#)
- [Microsoft Authenticator](#)
- [Oracle Athenticator](#)
- etc

Habilitar 2FA

Para habilitar autenticación por 2 pasos o 2FA debe ingresar a su perfil y habilitar 2FA, aparecerá un QR en su vista de perfil y deberá escanearlo con su aplicación de Autenticación.



2FA QR



Name: ROC
Email: roc@rocke
Phone:
Role: Admin
Company: Rocke
2 Factor Authen

Seguridad

Todas las conexiones se encuentran protegidas por protocolo https TLS 1.2 y se envía información protegida con JWT.

Las contraseñas se guardan encriptadas en base de datos (Mysql/SqlServer/Postgres).

El método usado es pasar las contraseñas por Hash Argon2 y bcrypt.

JWT asegura la sesión y RBAC el acceso y permisos CRUD

Nomenclatura

JWT: JSON Web Token es un estándar abierto (RFC 7519) que define una forma

compacta y autónoma para transmitir de forma segura información entre las partes como un objeto JSON.

Más información: <https://auth0.com/docs/jwt>

bcrypt: es un algoritmo diseñado específicamente para hash de contraseñas. MD5 y SHA1 son algoritmos de hash de propósito general. Por diseño, además, bcrypt permite agregar un salt al proceso de generación del hash, lo que, de entrada, lo hace inmune a ataques de diccionario.

Más información: <https://en.wikipedia.org/wiki/Bcrypt>

Argon2i and Argon2id variants).: Argon2 es una función de derivación clave que se seleccionó como ganadora del concurso de hash de contraseñas en julio de 2015 siendo una de las más fuertes hasta el día de hoy.

Más información: <https://en.wikipedia.org/wiki/Argon2>

TLS 1.2: Transport Layer Security (TLS; en español seguridad de la capa de transporte) y su antecesor Secure Sockets Layer (SSL; en español capa de puertos seguros) son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Más información: https://es.wikipedia.org/wiki/Transport_Layer_Security