IT Automation
BASE
【Classroom】

※“Exastro IT Automation” is written as "ITA" in this document

Exastro IT Automation Version 1.10

Exastro developer

Table of contents

1. Introduction
    - 1.1 About this document

2. Management console
    - 2.1 System settings
    - 2.2 RBAC (Role Based Access Control)

3. Basic console
    - 3.1 Device Management in ITA
    - 3.2 Operation overview
    - 3.3 ER Diagram

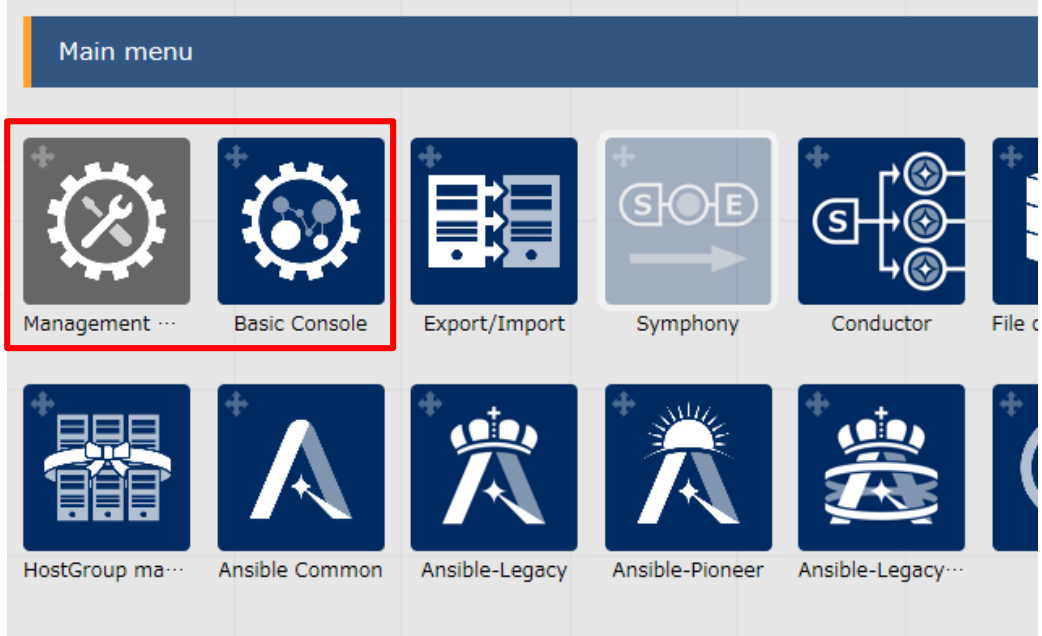
1. Introduction

Main Menu

- This document aims to describe the Management console and the Basic Console menu groups.

- **Management Console**
  - System settings
  - RBAC（Role Based Access Control）

- **Basic Console**
  - Device management in ITA
  - Operation overview



2. Management console

2.1 System Settings

In the “System Settings” menu, users can register all the necessary information for operating the system.
The settings items are as shown below.(See next page)

Item name	Description
IP address restrictions	Choose if access by IP address to be regulated or not
Upload prohibition extension	Extension file names that prohibit upload
Account lock duration (seconds)	Time period(seconds) to maintain locked state from start time of account lock.
Password error threshold (frequency)	Password failure threshold before locking account
Password error count upper limit (frequency)	Max amount of times continuous password errors
Password re-registration prevention period (days)	Time period (days) to prevent registration of same password
Password validity period (days)	Validity period of password (days)

2.1 System Settings

In the “System Settings” menu, users can register all the necessary information for operating the system.
The settings items are as shown below.

Item name	Description
Authentication duration: Not operated (seconds)	Session length without any user operations
Authentication duration: Maximum period (seconds)	Maximum session length
Screen design selection	Configures the design of the system
Symphony and Conductor Interval time (minutes)	Interval time between the scheduled Symphonies/Conductors changes their status to "Not executed (Scheduled)" after being registered.
Show / hide the “Role” button	Activates/Deactivates the "Role" button, which displays which role(s) the user belongs to.

2.2 RBAC (Role Based Access Control) (1/4)

About RBAC

RBAC is a method that allows users to assign authority by role.

Since authorization isn't given directly to each user, but by a role basis, the access authority management is allocated by local access.

● RBAC per menu

By being able to link each user to a role with permissions, users can control menu access for each user.
Users can also choose between two types of access when linking. "Can perform update" and "View only".
The "Can perform update" access permission will grant the user the ability to duplicate, update, delete data, as well as see it's history.
Users with the permission "View only" will only be able to see the data and it's history.

● RBAC per data record

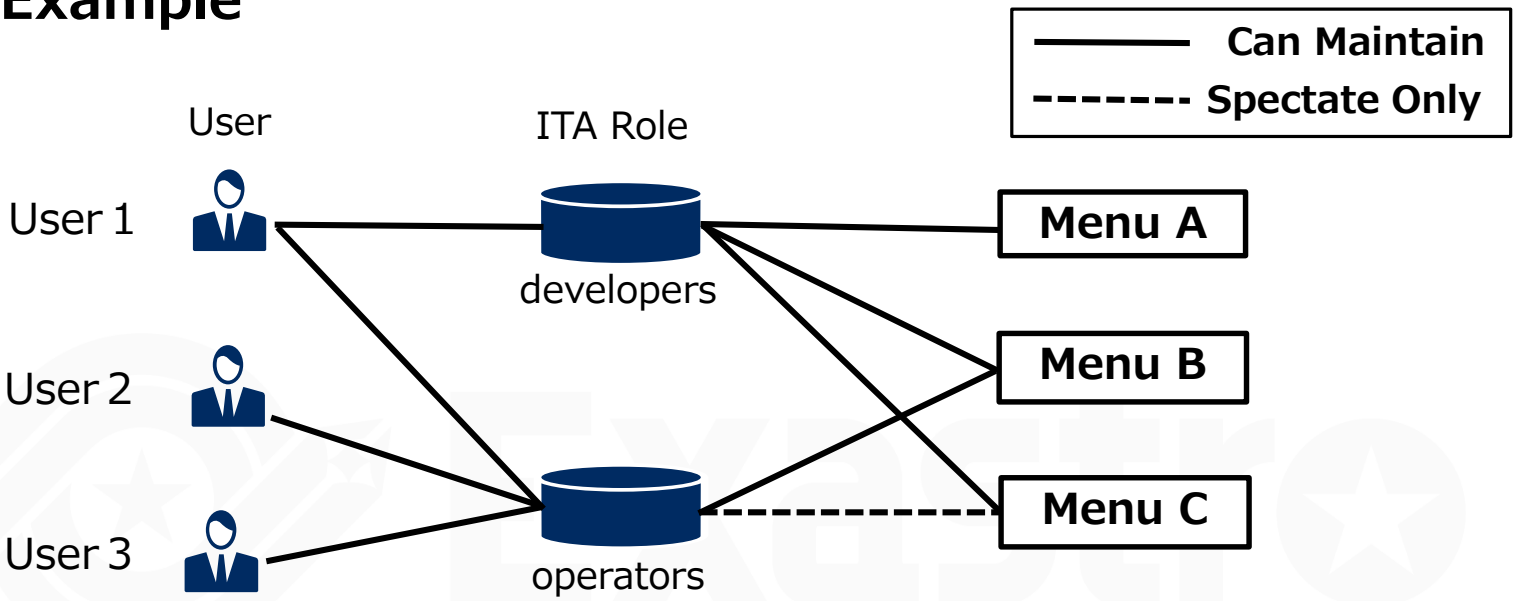
Users can also control access permission for individual data records by linking the data records to the user's respective roles.
If you are not using this function, you can change the default access permission / access permission role blank. This will make all the users able to see everything.
For more information, please see the user manual.

Description of the Menu groups inside “Management Console”

- **Menu group list**
  - Multiple groups bundled.
- **Menu list**
  - A Menu is always attached to a menu group.
- **Role List**
  - Role define access authority to Menus
- **User list**
  - A user can have multiple roles
  - It is possible to link with Active Directory and acquire user information.

- **Role/Menu link menu**
  - Maintain each users access authority to menus
- **Role/User link menu**
  - Maintain each users affiliation to other users.

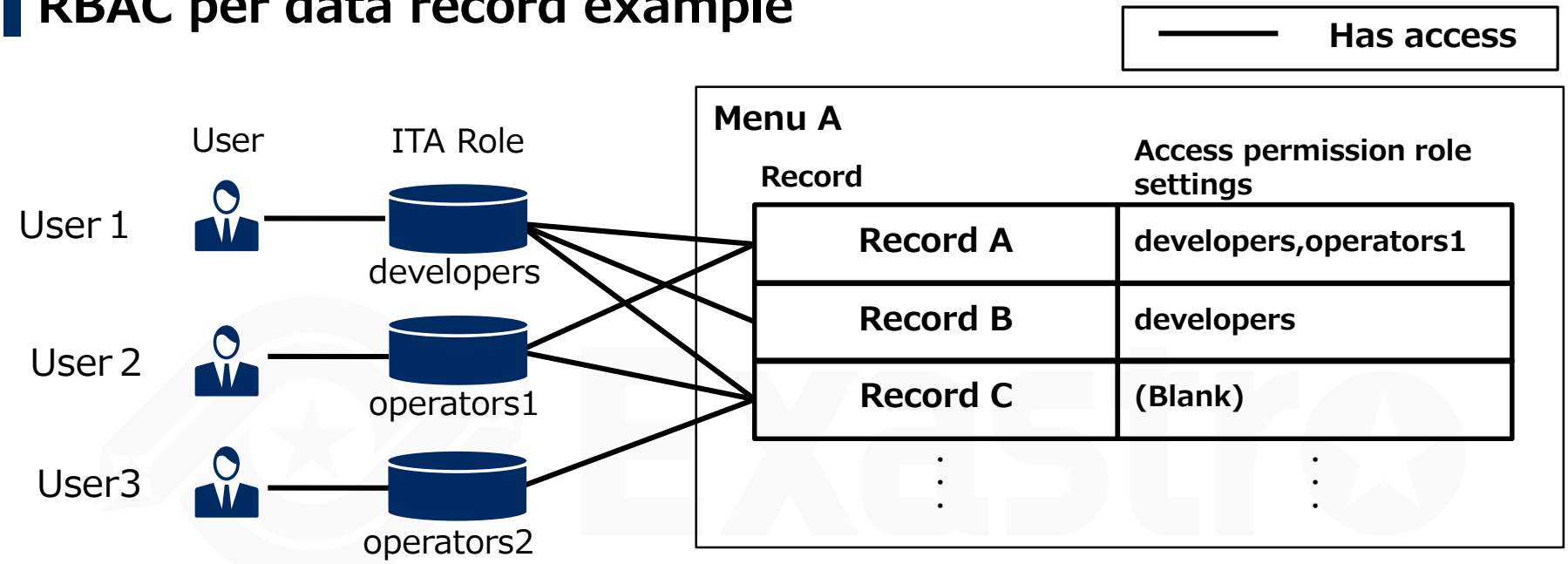
RBAC Example



- **Menu A・・・**
  Only User 1 can maintain
- **Menu B・・・**
  All users can maintain
- **Menu C・・・**
  User 1 can maintain, user 2 and 3 can only spectate

※ While user 1 has both the authorization “Can Maintain” and ”Spectate Only”, “Can Maintain” will be prioritized.

RBAC per data record example



- **RecordA・・・**
  developers and operators1 has access
- **RecordB・・・**
  only developers has access
- **RecordC・・・**
  the access permission value is blank(all users has access)

※This example is assuming that each role is linked to Menu A.
(Please see the page 7, "RBAC per menu")

3. Basic Console

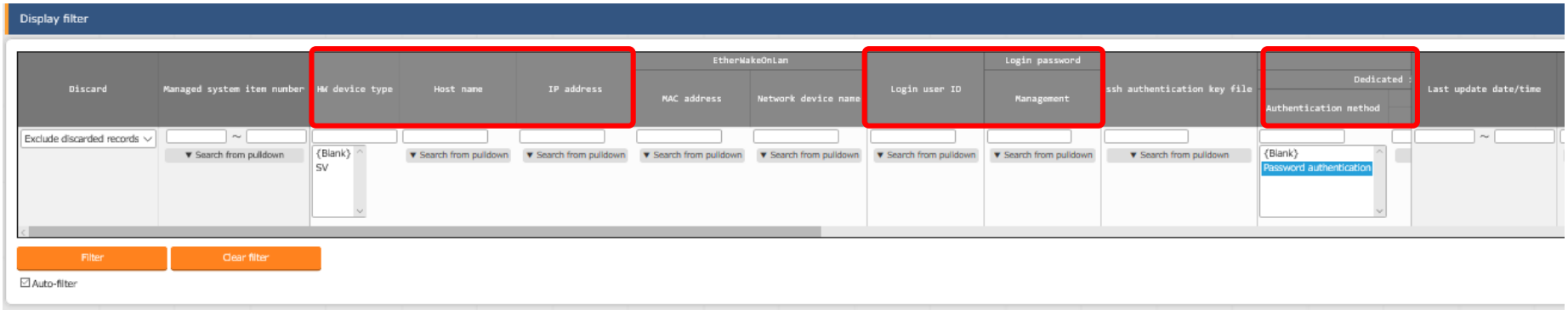
Device management in ITA

In the "Basic Console">"Device list" menu, users can register the needed information for the targeted host.

Users can check authorization information settings per host.
For authentication, it is possible to choose from Password authentication and Key authentication.

Main registration items

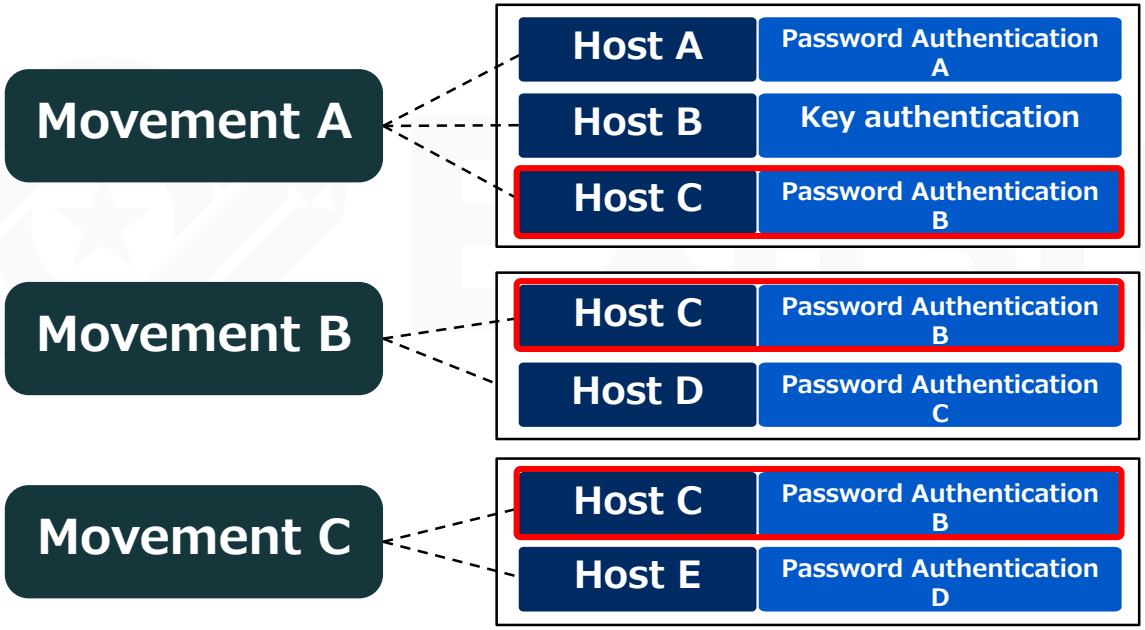
- **HW Device type**
- **Host name**
- **IP Address**
- **Log-in User ID**
- **Log-in Password**
- **Authentication method**



Device management in ITA（2）

in ITA, users can increase the reusability of device information as well as being able to respond flexibly to setting information changes by managing the user information separately.

※ Movement (original ITA terminology) means a work unit.



Example: Host C will need to change password and the changes will be carried out

↓

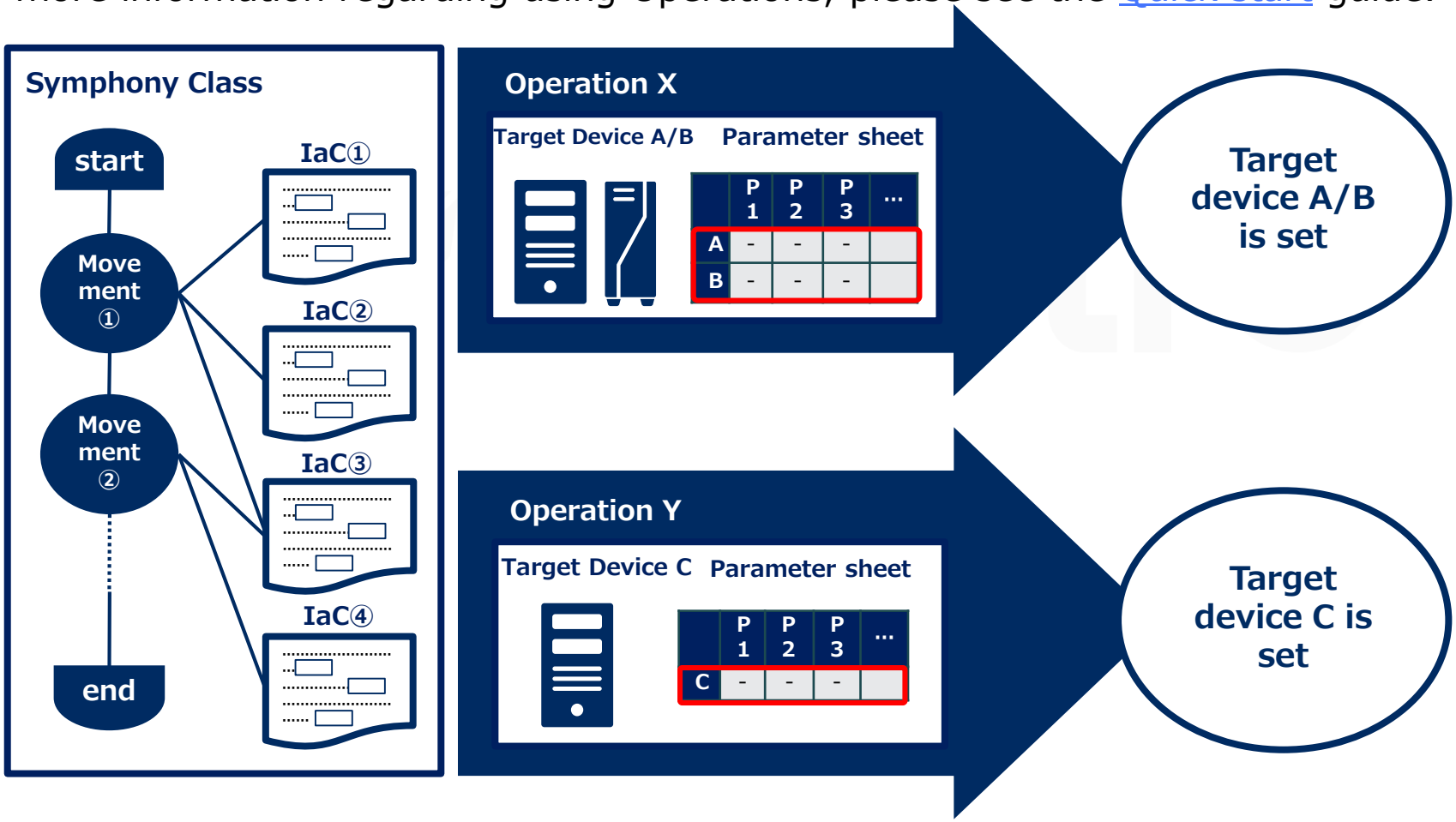
Result: All movements connected to C will be automatically updated to show the updated information

About Operation

Operation is an execution unit in ITA.

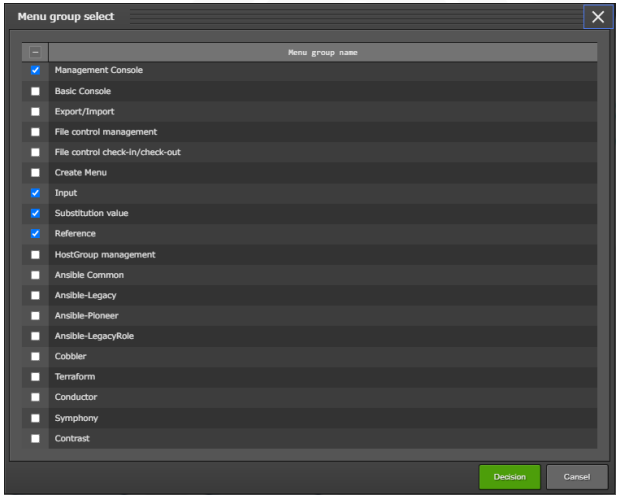
It is possible to manage execution history and execution schedule.

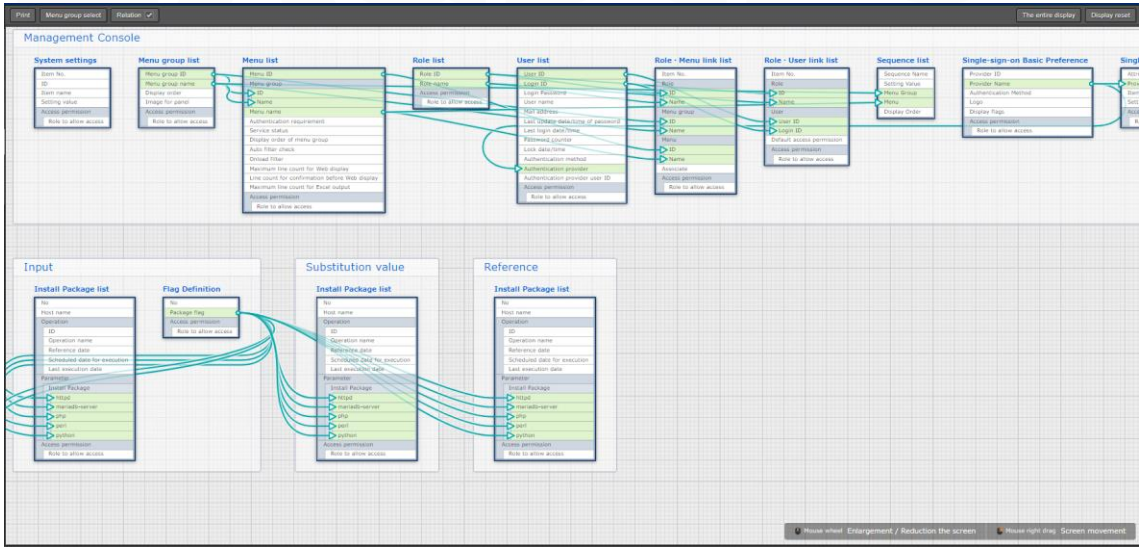
For more information regarding using Operations, please see the Quick start guide.



ER Diagram

Users can see an ER Diagram by going to the "Basic console" menu group >> "ER Diagram.
The ER Diagram is a diagram that displays the relation (reference data, etc.) between each Menu.
Users can also print out this diagram.
Note that only menus the user has permission to see will be displayed.
For more information, please refer to the user manual.





Exastro