






# **OMC System Software**

**Platform**

**User Manual**

Notices
<ul style="list-style-type: none"> <li>● The reproduction, transmission or use of this document or its contents is not permitted without express written authority.</li> <li>● Information and specifications in this document are subject to change without notice.</li> <li>● While information in this document is well edited and checked, mistake or omission may exist. Please don't hesitate to contact SUPCON if you have any question about this document.</li> <li>● Please contact SUPCON via email "SMS@supcon.com" if you have any question.</li> </ul>

Trademarks
<p>Trademarks or marks SUPCON, SPlant, Webfield, ESP-iSYS, MultiF, InScan, SupField are all registered, registering or using by Zhejiang SUPCON Technology Co., Ltd., which owns the properties of all trademarks or marks above. Without the written authority from Zhejiang SUPCON Technology Co., Ltd, no individual or company shall use any trademarks or marks above. We reserve the right to take legal action for any individual or company using trademarks or marks above illegally.</p>

Symbol Definition	
	<b>WARNING:</b> Indicates information that a potentially hazardous situation which, if not avoided, could result in serious injury or death.
	<b>RISK OF ELECTRICAL SHOCK:</b> Indicates information that Potential shock hazard where HAZARDOUS LIVE voltages greater than 30V RMS, 42.4V peak, or 60V DC may be accessible.
	<b>ESD HAZARD:</b> Indicates information that Danger of an electro-static discharge to which equipment may be sensitive. Observe precautions for handling electrostatic sensitive devices
	<b>ATTENTION:</b> Identifies information that requires special consideration.
	<b>TIP:</b> Identifies advice or hints for the user.

# Table of Contents

<b>Platform .....</b>	<b>1</b>
<b>Section 1 Overview .....</b>	<b>1</b>
1.1 Key Functions.....	1
1.2 Logging in to the Platform.....	1
1.3 Platform Homepage.....	2
1.4 Initialization.....	2
<b>Section 2 System Management .....</b>	<b>4</b>
2.1 Menu Management.....	4
2.2 Login Logs .....	5
2.3 i18n Management.....	5
2.3.1 Creating i18n Key .....	6
2.3.2 Language Settings .....	7
<b>Section 3 User Security Management.....</b>	<b>8</b>
3.1 Role Management .....	8
3.2 Permission Query .....	10
3.3 User Management .....	11
3.4 User Permission Management .....	12
<b>Section 4 Favorites.....</b>	<b>13</b>
<b>Section 5 Appendix: Accessing DMZ Server Data .....</b>	<b>14</b>
<b>Section 6 Revision History .....</b>	<b>16</b>

# Platform

## Section 1 Overview

---


The Platform is integrated into the OMC (Intelligent Operation Management & Control) system to predictively manage and monitor safety production data and control loop data in the production process, enabling intelligent management of production operations.

### 1.1 Key Functions

- System management: Configure menus displayed in the Platform, view user login logs, and manage i18n (internationalization) settings.
- User security management: Manage roles in the production site and association between roles and users, assign user permissions, and manage users logged in.
- Favorites: Supports user-defined menus, allowing adding frequently-used menus to the favorites for quick navigation.

### 1.2 Logging in to the Platform

To log in to the Platform:

- If the current computer serves as the IAC or IES, click  on the header of the High-performanceHMI component.
- If the computer is used for third-party management, access the Platform through the Autonomous Operation Client.
- If the networks are separated and a DMZ server is required for data forwarding, refer to Appendix: Accessing DMZ Server Data.

## 1.3 Platform Homepage

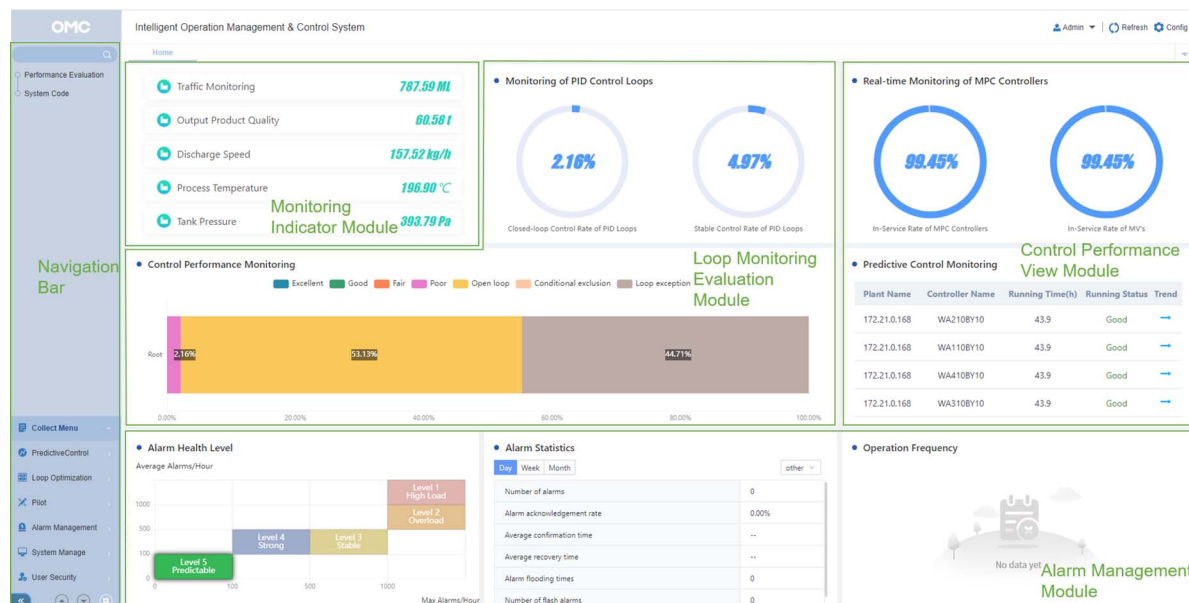



Figure 1-1 Platform homepage

## 1.4 Initialization

You can customize the items displayed on the homepage.

- 1) Click  on the upper-left corner to open **WEB Config** page.

The screenshot shows the 'WEB Config' page for the 'Intelligent Operation Management & Control System'. The page is divided into three main sections:

- Data Service Config:** Includes fields for Data Service IP (172.30.0.168), Data Service Port (5150), Data Service Username (administrator), and Data Service Password (masked). A green status indicator shows 'Connection succeeded.' and a 'Test Connection' button is available.
- Page Config:** A list of modules with toggle switches to enable or disable them:
  - Monitoring Indicator Module: ☒ Enable
  - Alarm Management Module: ☒ Enable
  - Control Performance View Module: ☒ Enable
  - Loop Monitoring Evaluation Module: ☒ Enable
- Parameter Config:** A table for defining parameters:
 

Parameter Name	Formula	Unit
Traffic Monitoring	(#pollinput003# + #pollinput002#) / 0.05	ML
Output Product Quality	(#pollinput003# + #pollinput004#) / 0.65	t
Discharge Speed	(#pollinput003# + #pollinput003#) / 0.25	kg/h
Process Temperature	(#pollinput003# + #pollinput003#) / 0.20	°C

 A '+ Add' button is at the bottom left, and 'Save' and 'Cancel' buttons are at the bottom right. A note states: 'It is recommended that the number of parameters configured should not exceed 5.'

Figure 1-2 Web Config page

2) Configure the settings according to the table below.

Items	Homepage Pane	Descriptions
Data service config	-	Data source (i-SYS) acquired by the Platform: <ul style="list-style-type: none"> <li>● Data Service IP: IP of i-SYS</li> <li>● Data Service Port: 5150</li> <li>● Data Service Username: administrator</li> <li>● Data Service Password: supcon</li> </ul>
Page config	Corresponds to the modules in Figure 1-2	Enable to show the corresponding module on the homepage.
Parameter config	Monitoring Indicator Module	Parameters shown in the Monitoring Indicator Module: <ul style="list-style-type: none"> <li>● Parameter Name: name of the parameter displayed</li> <li>● Formula: the formula for computing the parameter value. Tag names in i-SYS and four basic arithmetic symbols are supported. Use # to separate the tags. E.g. (#i-SYS tag name 1# + #i-SYS tag name 2)/2</li> <li>● Unit: the actual unit.</li> </ul>



**Tip:**

- If the operating system is Chinese version, please connect to the i-SYS 4.0 platform. If the operating system is English version, please connect to the i-SYS 3.1 platform.
- After switching the language version, reconfigure the connected i-SYS platform according to the language used in the environment.

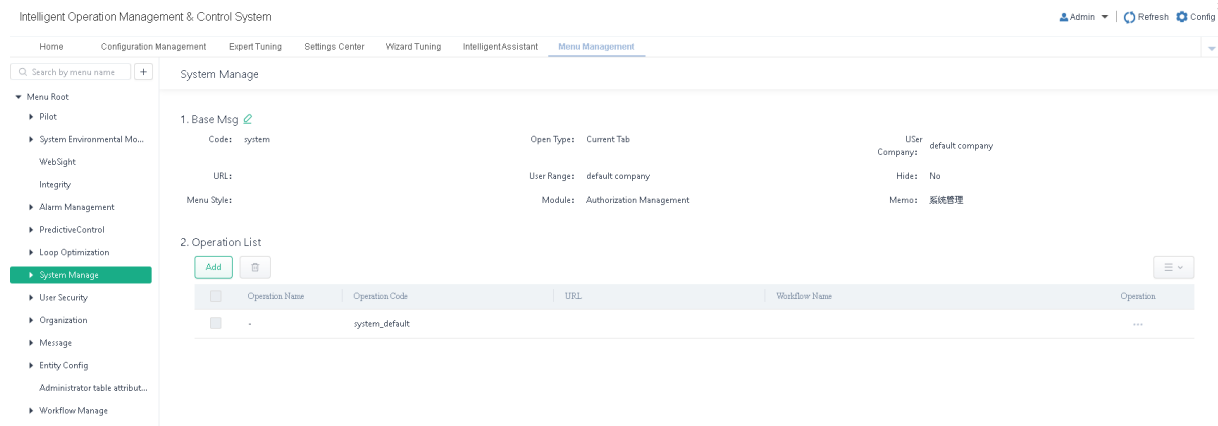
## Section 2 System Management

Through system management, you can manage menus, i18n (internationalization) codes, and logs.

### 2.1 Menu Management


With menu management, you can establish menus for various operations in the system and associate menus with operations.

Select **System Manage > Menu Management** in the navigation tree. The area on the right of the navigation tree will display the **Menu Management** page.



**Figure 2-1 Initial page of menu management**

As shown in the figure above, the **Menu Management** configuration page mainly includes:

- **Menu tree**  
Select a menu to modify, delete, sort, or move it. You can also create new menus.
- **Menu basic information:**  
Click  on a menu to open a dialog box where you can configure the menu's properties based on the table below.

Items	Function	Descriptions
Menu Code	Enter the code for the new menu.	-
Link URL	Enter the URL associated with the new menu.	-
Menu Style	Specify the CSS style for the new menu.	-

Items	Function	Descriptions
Open Type	Choose the desired opening type for the new menu.	"Current Tab": open the menu in the current tab. "New Tab": open the menu in a new tab.
Module	The module to which the new menu belongs.	Cannot be edited.
User range	The company to which the new menu belongs.	-
Hide	Hide this menu or not.	When checked, the menu will not be displayed in the navigation tree.
Memo	Enter the additional comments or notes about the new menu.	-

## 2.2 Login Logs

In the Platform, you can view the login logs of users.

Select the **System Manage > Log Manage > Log in** in the navigation tree. The area on the right of the navigation tree will display the login logs page.

**Figure 2-2 Login logs**

## 2.3 i18n Management

Through international management, you can maintain the i18n information in the web client and export the settings of the i18n module as a zip file.

To access i18n management, select **System Manage > International Management** in the navigation bar. The right area of the navigation bar will display the page as shown in Figure 2-3.



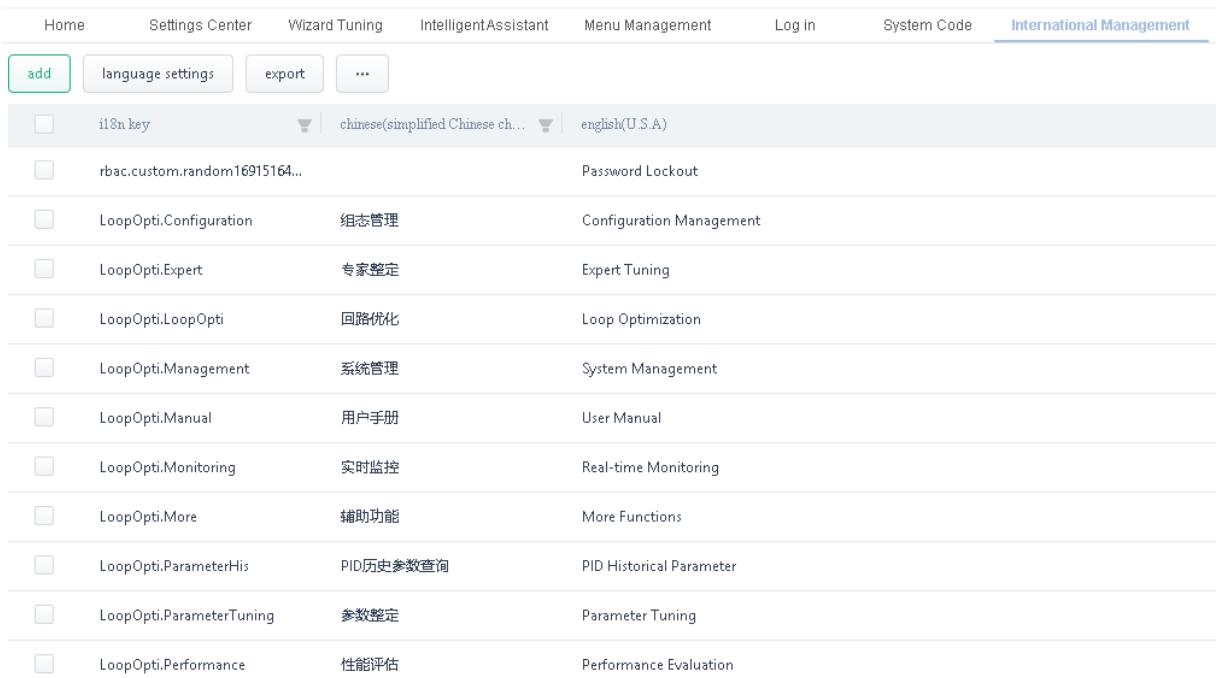


Figure 2-3 International management

### 2.3.1 Creating i18n Key

- 1) In the **International Management** page shown in Figure 2-3, select **add** to open the **Add i18n** window as shown in the figure below.

Add i18n

\* module

\* i18n key

chinese(simplified Chinese character)

english(U.S.A)

OK Cancel

Figure 2-4 i18n management

- 2) Configure the i18n key and its corresponding language information in the dialog box.
- 3) Click **OK**.

### 2.3.2 Language Settings

You can set the language according to your needs.

In the **International Management** page shown in Figure 2-3, select **language settings** from the dropdown menu to open the **i18n Management** dialog box as shown in the figure below.

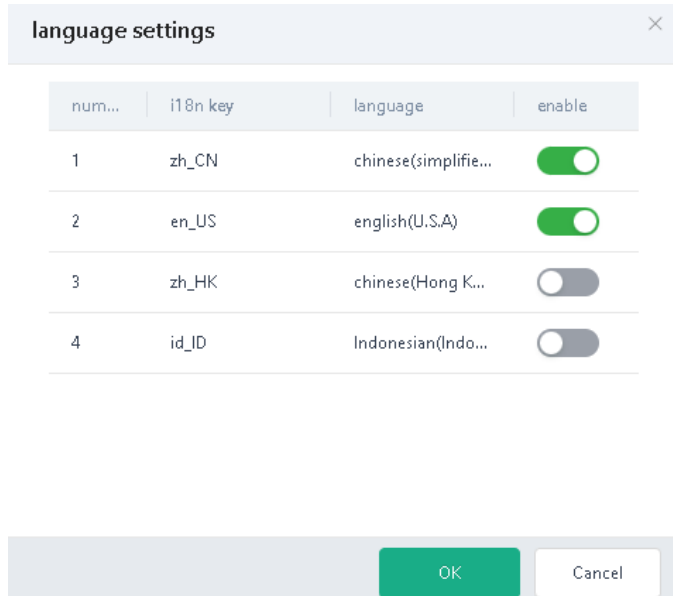


Figure 2-5 i18n language settings



**Tip:**

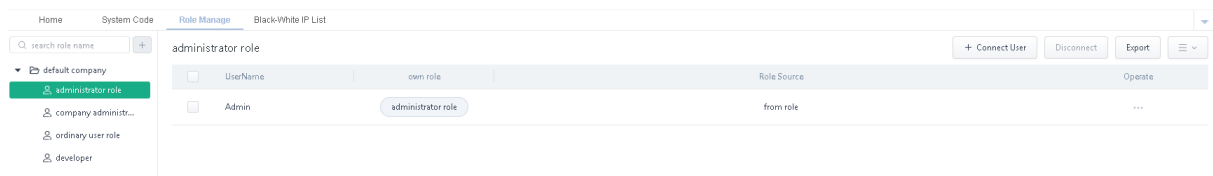
- Before deleting a language, make sure to disable it first.
- The Chinese (Simplified Chinese) is the default language, automatically enabled, cannot be disabled or deleted.

## Section 3 User Security Management

### 3.1 Role Management

In Role Management, you can uniformly manage the user permissions.

Select **User Security > Role Manage** in the navigation tree to open the role management page as shown in the following figure.



**Figure 3-1 Role Manage page**

After selecting a role from the tree on the Role Management page, the right side will show all users associated with the selected role. Additionally, you can search for users based on role name or username in the search bar.

In the above figure, roles and corresponding users can be managed.

#### Editing Role

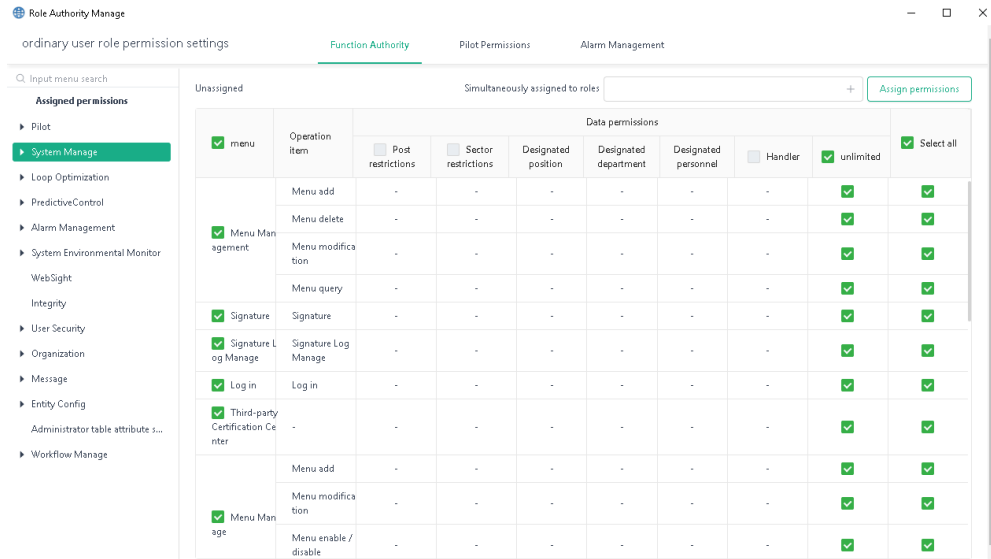
- 1) Hover over a role from the tree and click the ... button on the right side. From the popup menu, click **Edit** to open the **Edit role** dialog box as shown in the following figure.

**Figure 3-2 Edit role dialog box**

- 2) Complete the new role information by entering the **Code**, **Role Name**, and **Desc** text boxes. After a successful configuration, the new role will be updated in the tree.

## Configuring Role Permission

- 1) Hover over a role from the tree and click the ... button on the right side. From the popup menu, select **auth settings** to open the **Authority Manage** dialog box as shown in the following figure.



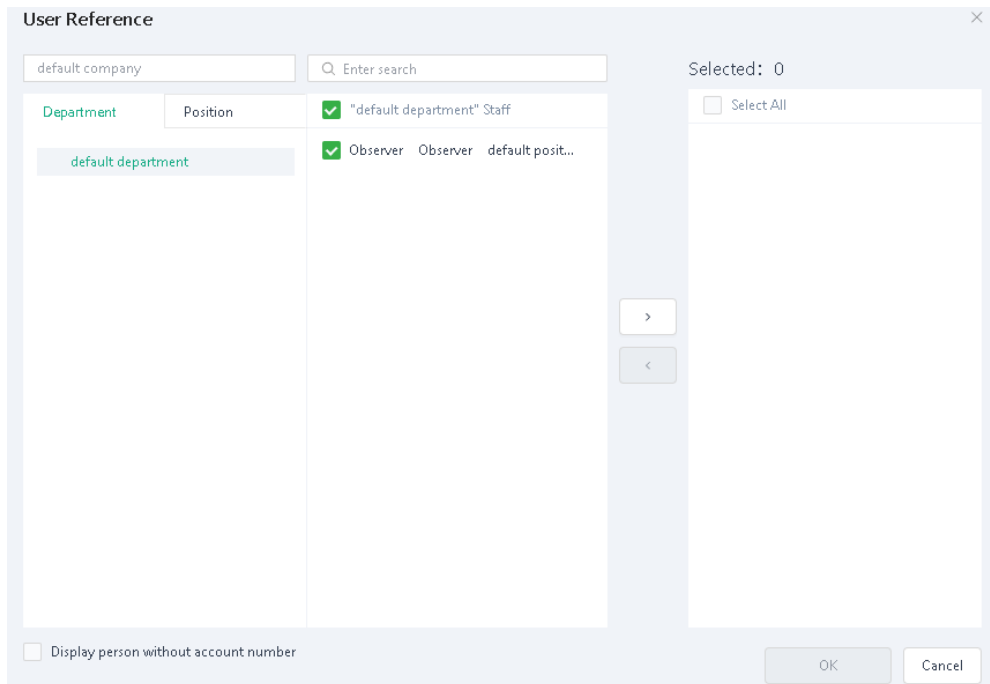
**Figure 3-3 Role authority management dialog box**

- 2) Check the permissions that need to be assigned in the permission list.

## Adding Users to A Role

After defining roles, users can be added to those roles. Steps

- 1) Select the role to which you want to add users from the tree.
- 2) From the right-side menu, select the **Connect User** command to open the **User Reference** dialog box as shown in the following figure.



**Figure 3-4 User reference dialog box**

- 3) Select users from the left area and click > to add them to the **Selected** area.
- 4) Click **OK**, and the selected users will be displayed as associated users for the current role in the role's user list.

## 3.2 Permission Query

The Permission Query function is mainly used for querying user permissions, role permissions, and permission change logs.

In the navigation bar, select **User Security > Permission Query**. The right panel will display the query page as shown in the following figure.

Intelligent Operation Management & Control System

Admin | Refresh | Config

Home System Code Role Manage Black-White IP List **Permission query** User Permission Management User Manage

Permission Query User Permission Query Role Permission Query Permission Changed Log

delete export

	User Na...	Menu Name	Operation Name	Process...	Group Rstr...	Position R...	Designate...	Designate...	Handler	Unrestricted	Permission...	Name of A...	Allocate Time	Role of Source
<input type="checkbox"/>	Admin	Pilot	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:36	
<input type="checkbox"/>	Admin	Procedure Buil...	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:36	
<input type="checkbox"/>	Admin	PID Historical ...	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:50	
<input type="checkbox"/>	Admin	System Manag...	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:50	
<input type="checkbox"/>	Admin	Setting Center	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:50	
<input type="checkbox"/>	Admin	Switch Project	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:50	
<input type="checkbox"/>	Admin	User Manual	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:50	
<input type="checkbox"/>	Admin	PredictiveCont...	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:55	
<input type="checkbox"/>	Admin	Watch	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:10:55	
<input type="checkbox"/>	Admin	Alarm Manage...	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:11:00	
<input type="checkbox"/>	Admin	Audit	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:11:00	
<input type="checkbox"/>	Admin	Audit Scheme	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:11:00	
<input type="checkbox"/>	Admin	Audit Progress	-		--	--	--	--	--	✓	User Auth...	virtual pers...	2023-07-28 07:11:00	

Figure 3-5 Permission query

### 3.3 User Management

Select **User Security > User Manage** in the navigation bar, and the **User Manage** dialog box will be displayed on the right side as shown in the following figure. It allows unified management of users within the OMC system.

Intelligent Operation Management & Control System

Admin | Refresh | Config

Home System Code Role Manage Black-White IP List Permission query User Permission Management **User Manage** International Management

User Password Policy

Users

Import New Freeze Lock Delete

	Username	Description	Email	Phone	Lock	Lockout Reason	Date Locked	Freeze	Freeze Reason	Date Frozen	Password expires on	Manage
<input type="checkbox"/>	Admin				✓		--	✖		--	--	Edit Reset Password Delete
<input type="checkbox"/>	Observer				✓		--	✖		--	--	Edit Reset Password Delete

Total 2 records < 1 >

Figure 3-6 User manage page



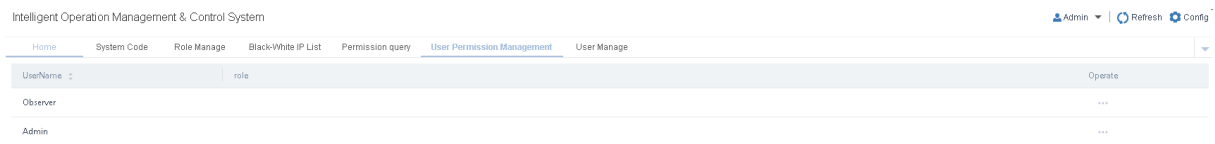
#### Tip:

- Admin and Observer are default users and cannot be deleted.
- The initial password for Admin is "admin," and this account supports password reset. The password for Observer is empty, and password reset is not allowed.
- For detailed instructions on user management, please refer to the *OMC User Service Configuration Guide*.

### 3.4 User Permission Management

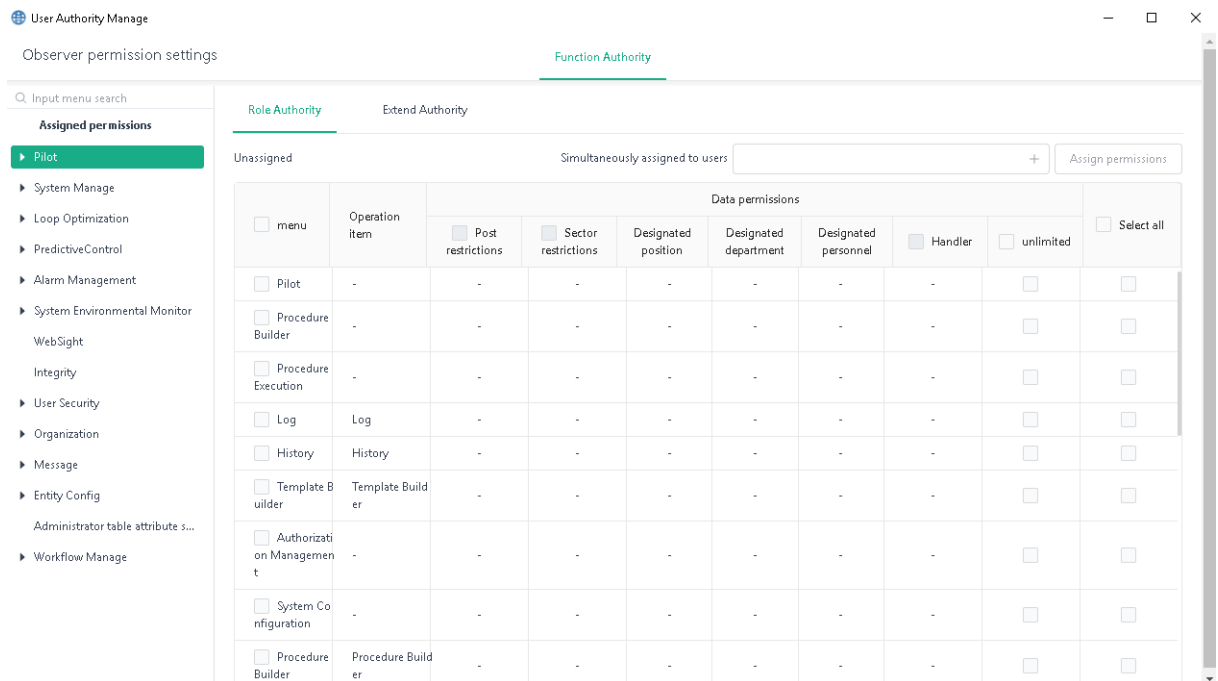
After configuring users, you can assign operational permissions to them.

- 1) Select **User Security > User Permission Manage** in the navigation bar, and the **User Permission Management** page will be displayed on the right side as shown in the following figure. In this page, you can configure operational permissions for the created users.



**Figure 3-7 User permission management page**

- 2) Select a user and click the **authority** button in the **Operation** column, to open the permission assignment page as shown in the following figure.




**Figure 3-8 User permission assignment page**

- 3) Check the permissions that need to be assigned in the permission list.


## Section 4 Favorites

---

In the menu list, select a menu and click  on the right side to add it to favorites, as shown in the following figure.



**Figure 4-1 Example of navigation bar menu**

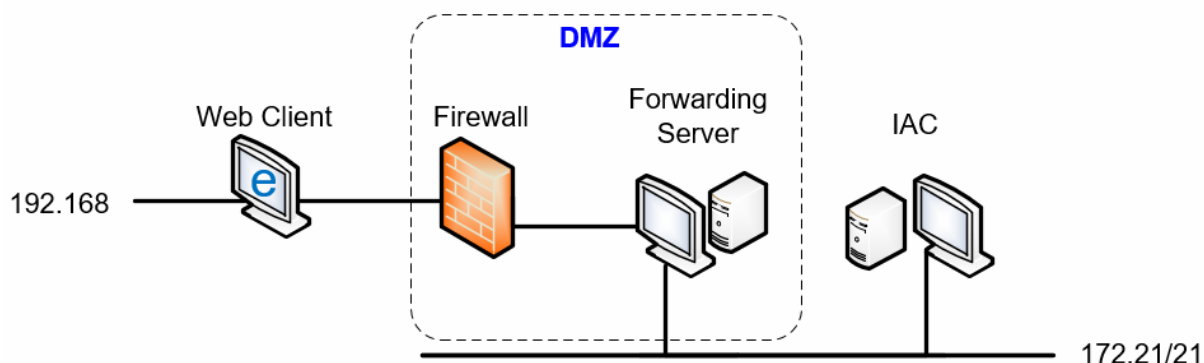
Once added to favorites, the menu will be displayed as . Click on Favorites to show the menus added to favorites, as shown in the figure above.



## Section 5 Appendix: Accessing DMZ Server Data

Because of the network policy adopted in the field, the control network and information network may not be connected and a DMZ server is used for forwarding. In this case, you need to install nginx to achieve network forwarding.

The following figure illustrates a typical network structure of accessing a DMC server from external network.



**Figure 5-1 Typical network structure of accessing a DMC server**

To install and configure nginx in DMC server:

- 1) In the *OMC installation directory\Setup\05\Add-on*, copy "nginx-dmz.zip" to any directory on the DMZ server and extract it (Note: The directory should not contain any Chinese characters).
- 2) Run the "installSupfusionNginx.bat" as an administrator in the \nginx-dmz\command directory.
- 3) Go to the "nginx-dmz\conf" directory and modify the "nginx.conf" configuration file. Change the IP address after "geo \$controller\_server\_address" to the actual IP address of the control network server. After making the modifications, save the file.

```

http {
    include      mime.types;
    default_type  application/octet-stream;
    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #            '$status $body_bytes_sent "$http_referer" '
    #            '"$http_user_agent" "$http_x_forwarded_for"';
    geo $controller_server_address {
        default http://127.0.0.1;
    }
    #access_log  logs/access.log  main;
    access_log off;
    sendfile    on;
    #tcp_nopush  on;

    #keepalive_timeout    0;
    keepalive_timeout    65;

    #gzip  on;

    client_max_body_size 2048m;
    client_body_buffer_size 128k;

    server {
        listen      17084;
        server_name  localhost;
        set $suposlite_controller_server_address $controller_server_address:17080;
        #charset koi8-r;
        #access_log  logs/host.access.log  main;
        proxy_read_timeout 300;
        include location/*.conf;
    }

    include server/*.conf;

    # another virtual host using mix of IP-, name-, and port-based configuration
    #
    #server {
    #    listen      8000;
    #    listen      somename:8080;
    #    server_name  somename  alias  another.alias;

    #    location / {
    #        root    html;
    #        index   index.html index.htm;
    #    }
    #
    #
    #

```

**Figure 5-2 Example file**

- 4) Open the service list in the Task Manager. Right-click the "supcon-nginx-middleware-dmz" and click **Start** to start the nginx service in the DMZ.
- 5) Access the suposlite login page by visit `http://DMZ_zone_server_IP:17084`.

## Section 6 Revision History

---

Document Version	Applicable Product Version	Remarks
V1.0 (20230911)	OMC V1.20.00.00-M	First release.