

swidch

OTAC auth Admin Manual



V 1.2.0

swidch Ltd.

swidch

Address: 1st floor, 3 More London Pl, London SE1 2RE

Tel: +44 (0) 2032834081

Mail : developer@swidch.com

Contents

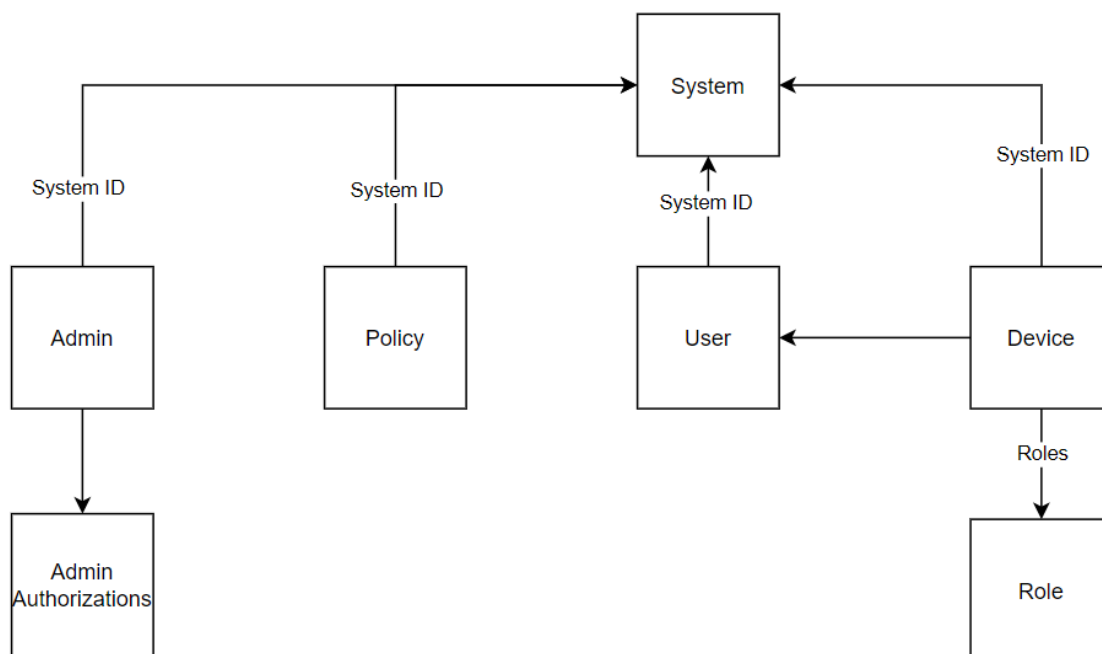
Introduction	3
The Data Model	3
The Admin Portal	4
Login	4
Dashboard	5
My Info	6
Change Password	7
Admin Management	8
Changing an Admin Account	9
Admin Authorization	10
Admin Registration	11
Logging in as the new Admin	12
Setup OTAC login for an Admin	13
Logging as the Admin using OTAC	15
Admin Login History	17
Admin Activity History	18
OTAC Management	19
Role Management	19
Role Registration	20
User Management	21
User Registration	21
Device Management	24
Device Registration	25
Modify Device	26
Policy Management	27
Create a new Policy	28
Modify an existing Policy	29
Server IP Management	30
License Management	31
Audit Logs	32
Authentication Success Events History	32
Authentication Failure Events History	33
Registered/Terminated User History	34

Introduction

This document is intended for admin user's who will be using the OTAC Admin Portal to manage and configure OTAC settings and users/devices. The Admin Portal allows you to:

- **Dashboard:** That shows high level stats on user registration and authentication requests
- **User Management:** Manage users and pair their mobile devices.
- **Policy Management:** Control the OTAC policies such as duration.
- **Role Management:** Manage roles than can be assigned to users and passed on the PLC for authorization
- **Audit Logs:** To view admin, authentication and user registration logs

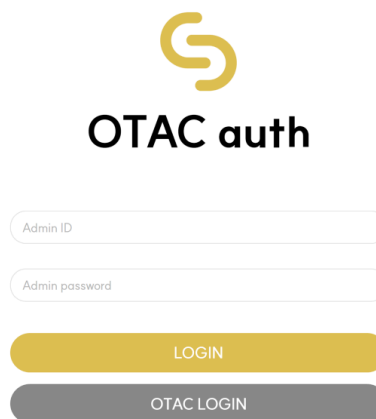
The Data Model



- **System:** A system is an arbitrary object that represents a group of PLCs. This is useful for management if you want to have separate policies, users and administrator for various PLCs
- **User:** A user represent the user who is able to login to the PLC
- **Device:** A device represents a PLC Device.
- **Roles:** Roles are the authorization role of what a user can do with in the PLC.
- **Policy:** The policy management shows the behavior of OTAC and how it is validated. You can have separate policies for different systems.
- **Admin:** Admin is the administrator user of the OTAC auth Admin Portal
- **Admin Authorizations:** Admin Authorizations are for delegated administration of the Admin Portal

The Admin Portal

Login

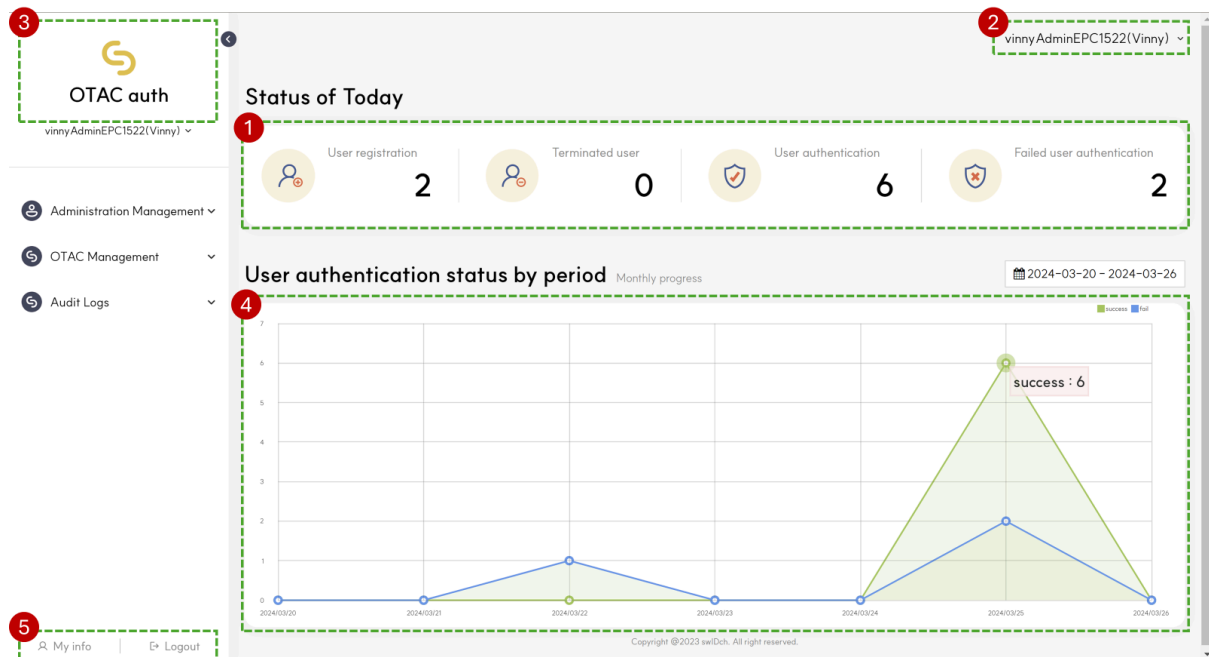


The image shows the OTAC auth login interface. At the top center is a yellow logo consisting of a stylized 'S' shape. Below the logo, the text 'OTAC auth' is displayed in a bold, black, sans-serif font. Underneath the text are two input fields: the first is labeled 'Admin ID' and the second is labeled 'Admin password'. Below these fields are two buttons: a yellow button labeled 'LOGIN' and a grey button labeled 'OTAC LOGIN'.

To log on as administrator on the default IP address goto <http://192.168.1.10:8443/otacadm> and follow these steps :

1. Admin ID “ otac_admin ”
2. The default password is “@TACaUth!12”
3. 'Login'. Press the button.
4. You will be prompted to change the password.
5. Please set a new password

Dashboard



This is the page you first see when you log in. The dashboard provides a central snapshot overview of your usage status .

① Today's statistics

Shows today's statistics for user authentication and registration

② My information

Proceed to edit my information, change password and log out

③ Main logo

The logo will be displayed and clicking it will take you to the main page

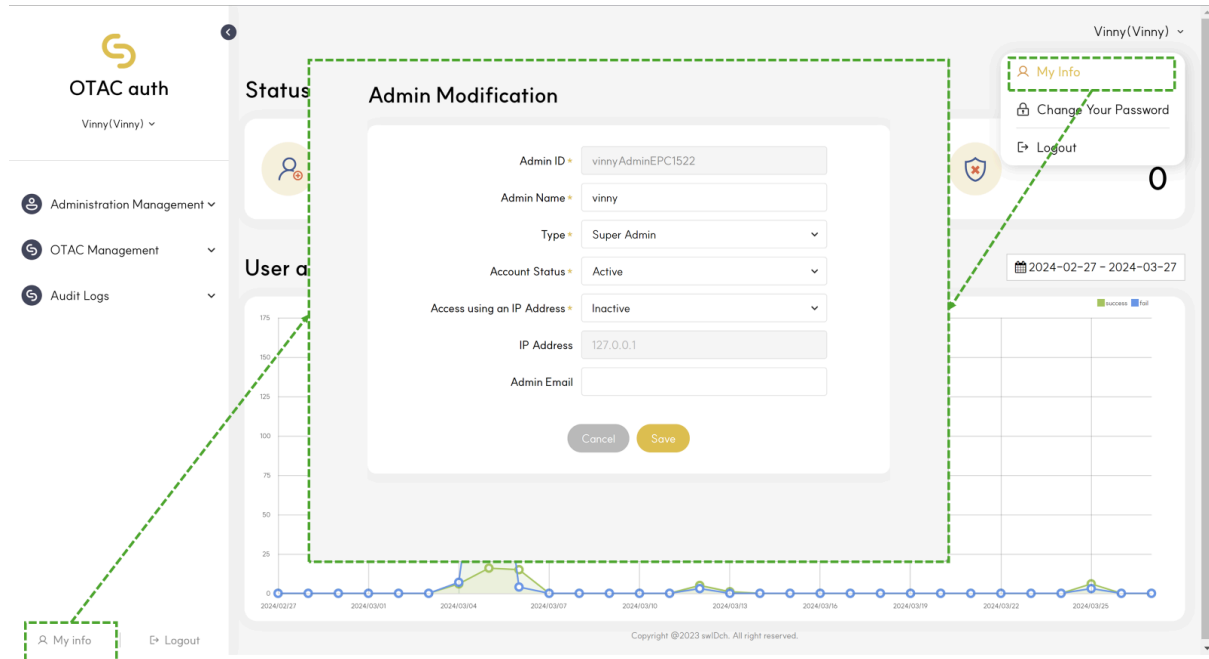
④ Dashboard

A graph of success and failure by period is displayed according to the date in the upper right corner of the dashboard . You can select the date through Datepicker.

⑤ Bottom menu

The Settings button sets my information, and the Power button logs out.

My Info

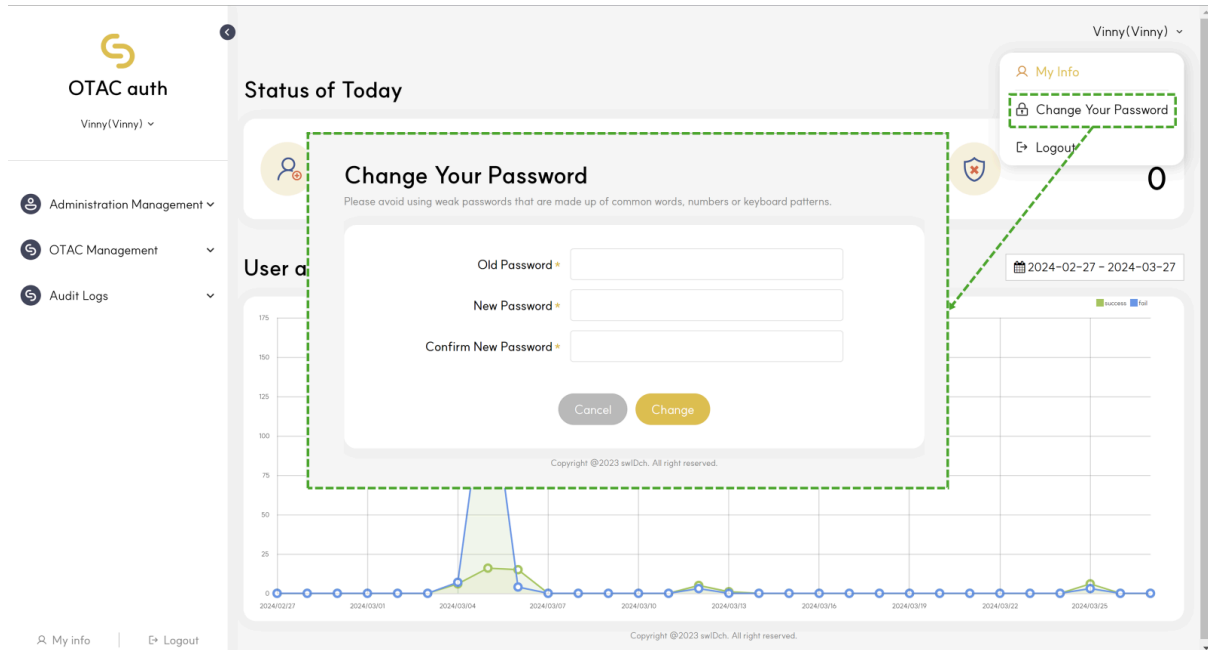


This is the pop-up that appears when you click My Info at the top right and the Settings button at the bottom left .

You can edit the information of the logged in account

- Admin ID: Displays the ID of the logged in account
- Admin Name: The logged in account's Displays the name
- Type: Displays the Type of the logged in account
 - super admin: Administrator with full authority
 - admin: Administrator with the authority granted by super admin
- Account status: Indicates whether the logged in account is being used
- Access using an IP address: Set an accessible IP
- Admin email: Displays the email of the logged in account

Change Password



This is the password change page .

You can access it through the Change Your Password menu in the top right.

- Old password: Enter the previous password
- New password: Enter a new password
- Confirm new password: Enter a new password again

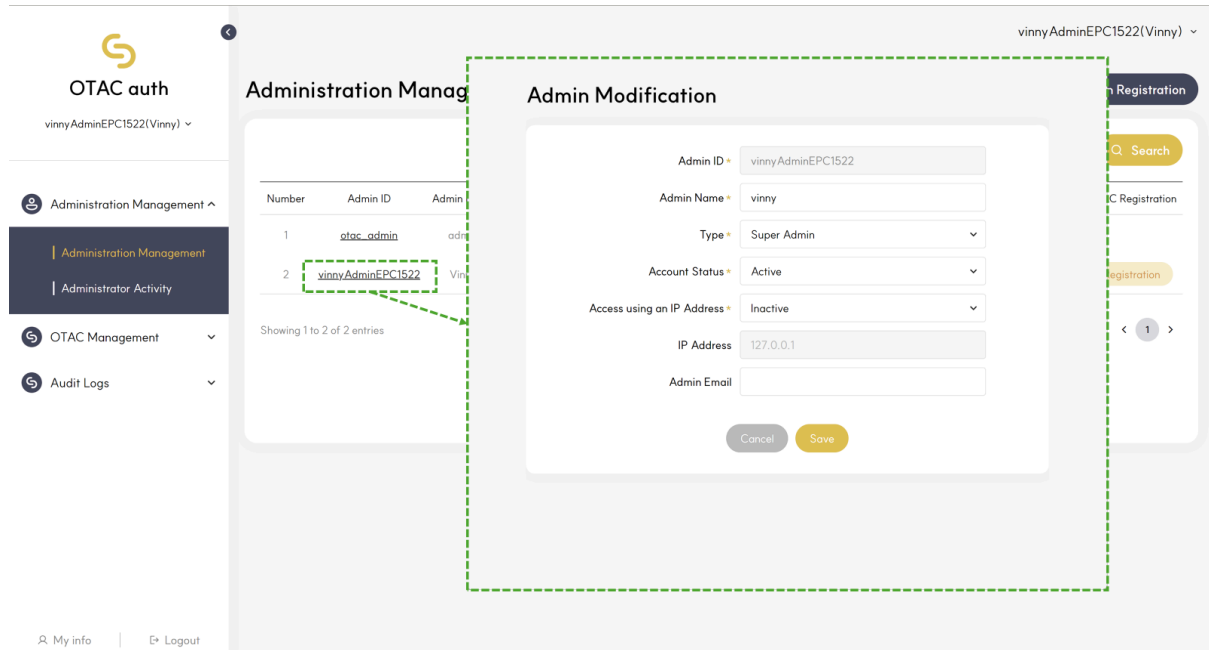
Admin Management

The screenshot displays the 'Administration Management' interface. At the top, there's a header with the 'swidch' logo and 'OTAC auth' text. A user profile 'vinnyAdminEPC1522(Vinny)' is shown in the top right. Below the header, there's a navigation sidebar on the left with options like 'Administration Management', 'OTAC Management', and 'Audit Logs'. The main content area features a table of administrator accounts. The table has columns for 'Number', 'Admin ID', 'Admin Name', 'Type', 'Account status', 'Number of login error', 'Reset', 'Last Modified', 'Admin Authorisation', and 'OTAC Registration'. Two entries are visible: 'otac_admin' (Super Admin, Active) and 'vinnyAdminEPC1522' (Super Admin, Active). The 'vinnyAdminEPC1522' entry is highlighted with a green dashed box, and a 'Registration' button is present next to it. A 'Reset' button is also visible for the 'otac_admin' entry. The page includes search filters for 'Type Select', 'Account status Select', and 'Admin ID/Admin Name'. At the bottom, there's a footer with 'Copyright ©2023 swidch. All right reserved.'

This is the administrator settings page. You can configure settings for other accounts, including the account you are logged in with .

- Admin ID: Displays the user ID of the administrator
- Admin Name: Displays the user name of the administrator
- Type: Displays the Type of admin account
 - super admin: Administrator with full authority
 - admin: Administrator with the authority granted by super admin
- Account status: Indicates whether the logged in account is in use
- Number of login errors: Indicates the number of login failures for the account
- Reset: Indicates whether password reset is required for the admin at the next login. When you click on the 'Reset' button, the password for that admin will be set to their Admin ID and they will be required to change their password at the next login.
- Admin Authorization : Set access permissions for the account.
- OTAC Registration : Register the current admin to set up OTAC to login to the admin portal.

Changing an Admin Account



This is the administrator edit page. The image above is the screen that appears when you click on the Admin ID .

- Admin ID: Displays the ID of the admin account
- Admin Name: Admin account's displays the name
- Type: Displays the Type of the logged in account
 - super admin: Administrator with full authority
 - admin: Administrator with the authority granted by super admin
- System Name: System that the administrator can manage
- Multiple selection is possible with Ctrl + left mouse click
- Only non super admin have this function
- Account status: Sets the status of the account to active or inactive
- Access using an IP address: Set an accessible IP
- Admin email: Displays the email of the logged in account

Admin Authorization

The screenshot displays the 'Admin Authorisation' page. At the top left, the user is identified as 'vinnyAdminEPC1522(Vinny)'. The page features a sidebar with navigation links: Administration Management, Administration Management (highlighted), Administrator Activity, OTAC Management, and Audit Logs. The main content area is titled 'Admin Authorisation' and includes a form with 'Admin ID' set to 'DelAdmin' and 'Type' set to 'Delegated Admin'. Below the form is a table with the following data:

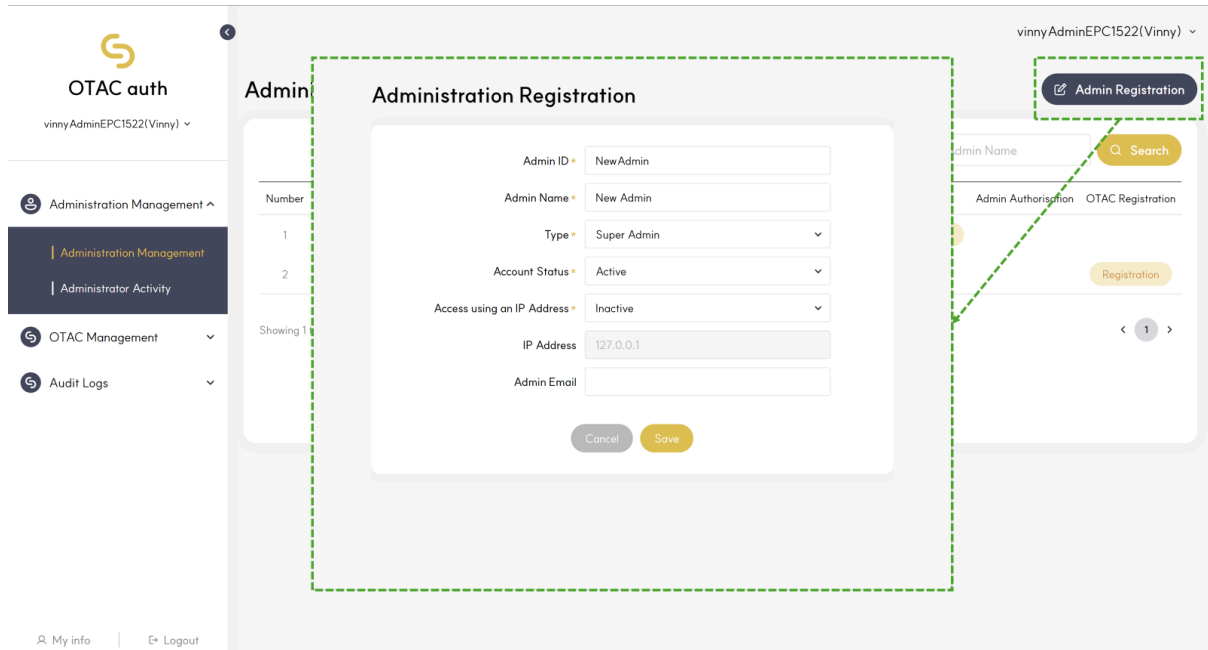
Select	Menu name	Top menu	URL
<input type="checkbox"/>	System Management		
<input type="checkbox"/>	> License Management	System Management	/system/mgmt/lic.do
<input type="checkbox"/>	> Server IP Management	System Management	/system/mgmt/serverip.do
<input checked="" type="checkbox"/>	Administration Management		
<input checked="" type="checkbox"/>	> Administration Management	Administration Management	/admin/mgmt/admin/list.do
<input checked="" type="checkbox"/>	> Administrator Activity	Administration Management	/admin/mgmt/log/login.do
<input type="checkbox"/>	FIDO		
<input type="checkbox"/>	OTAC Management		
<input type="checkbox"/>	> Successful Authentication Events History	OTAC Management	/otac/log/auth/list.do
<input type="checkbox"/>	> Failed Authentication Events History	OTAC Management	/otac/log/auth/fail/list.do
<input type="checkbox"/>	> Registered/Terminated User History	OTAC Management	/otac/log/user/list.do
<input type="checkbox"/>	> User Management	OTAC Management	/otac/user/list.do
<input type="checkbox"/>	> Policy Management	OTAC Management	/otac/policy/list.do

On the right side of the page, there is a search bar and a table with columns: Modified, Reset, Admin Authorisation, and OTAC Registration. The 'Admin Authorisation' column contains a button labeled 'Admin Authorisation', which is highlighted by a green dashed box. The 'OTAC Registration' column contains a button labeled 'Registration'.

This is the administrator privilege management page. It can only be granted to non super admin accounts .

- Admin ID: Displays the ID of the admin account
- Type: Displays the Type of the logged in account
 - super admin: Administrator with full authority
 - admin: Administrator with the authority granted by super admin
- By selecting multiple checkboxes, you give the administrator permission to access various menus in the admin portal.

Admin Registration



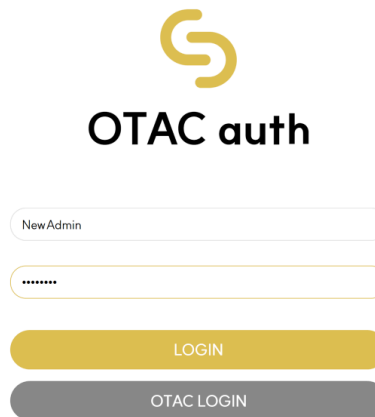
This is the administrator creation page to create an administrator and super administrator .

- Admin ID: Displays the ID of the admin account
- Admin Name: Admin account's displays the name
- Type: Displays the Type of the logged in account
 - super admin: Administrator with full authority
 - admin: Administrator with the authority granted by super admin
- Account status: Indicates whether the logged in account is being used
- Access using an IP address: Set an accessible IP
- Admin email : Displays the email of the logged in account

Please note the default password for a newly created admin is the same as their Admin ID. Upon first login the admin is required to change the default password.

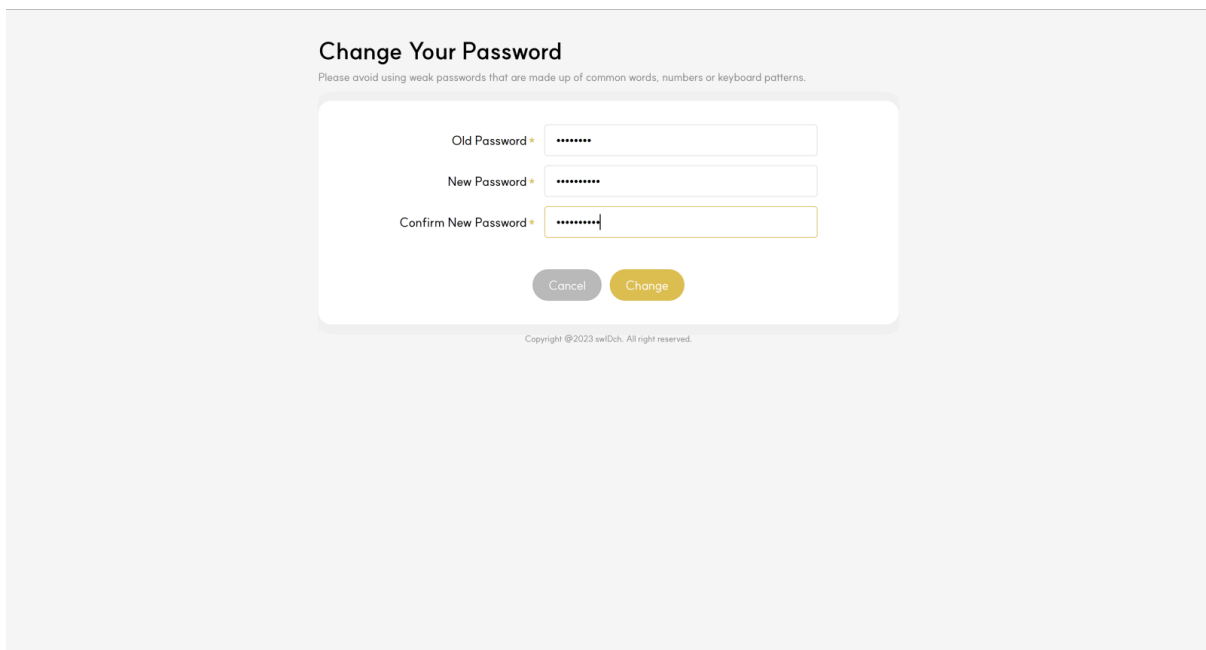
Logging in as the new Admin

Once you have created a new admin, logout and login as the new admin. Please note the default password for a newly created admin is the same as their Admin ID.



The image shows the OTAC auth login interface. At the top is the swidch logo, a stylized 'S' in yellow. Below it is the text 'OTAC auth'. There are two input fields: the first is labeled 'NewAdmin' and contains the text 'NewAdmin'; the second is a password field with seven dots. Below the input fields are two buttons: a yellow 'LOGIN' button and a grey 'OTAC LOGIN' button.

Login as the new admin with username and password as the Admin ID

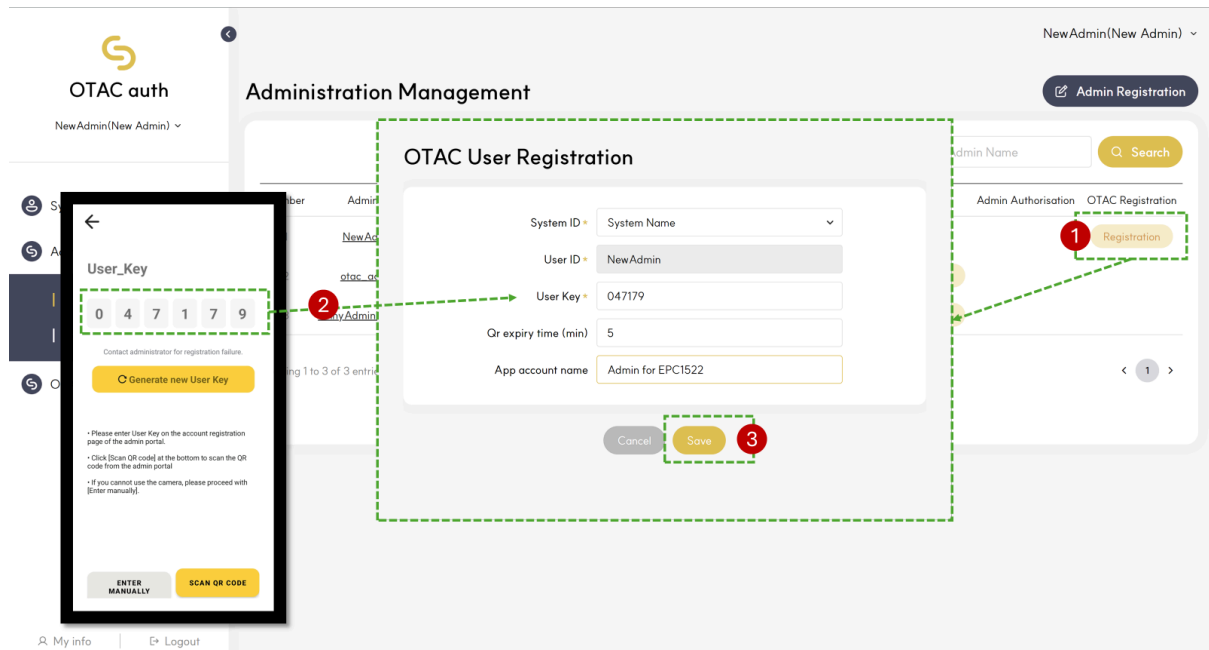


The image shows a 'Change Your Password' form. The title is 'Change Your Password' and there is a note: 'Please avoid using weak passwords that are made up of common words, numbers or keyboard patterns.' The form has three input fields: 'Old Password *' with seven dots, 'New Password *' with seven dots, and 'Confirm New Password *' with seven dots. Below the fields are two buttons: 'Cancel' and 'Change'. At the bottom, there is a small copyright notice: 'Copyright ©2023 swidch. All right reserved.'

In the next step you will be prompted to change your current password. Once you have changed the password you can now login to the admin portal with the new admin account.

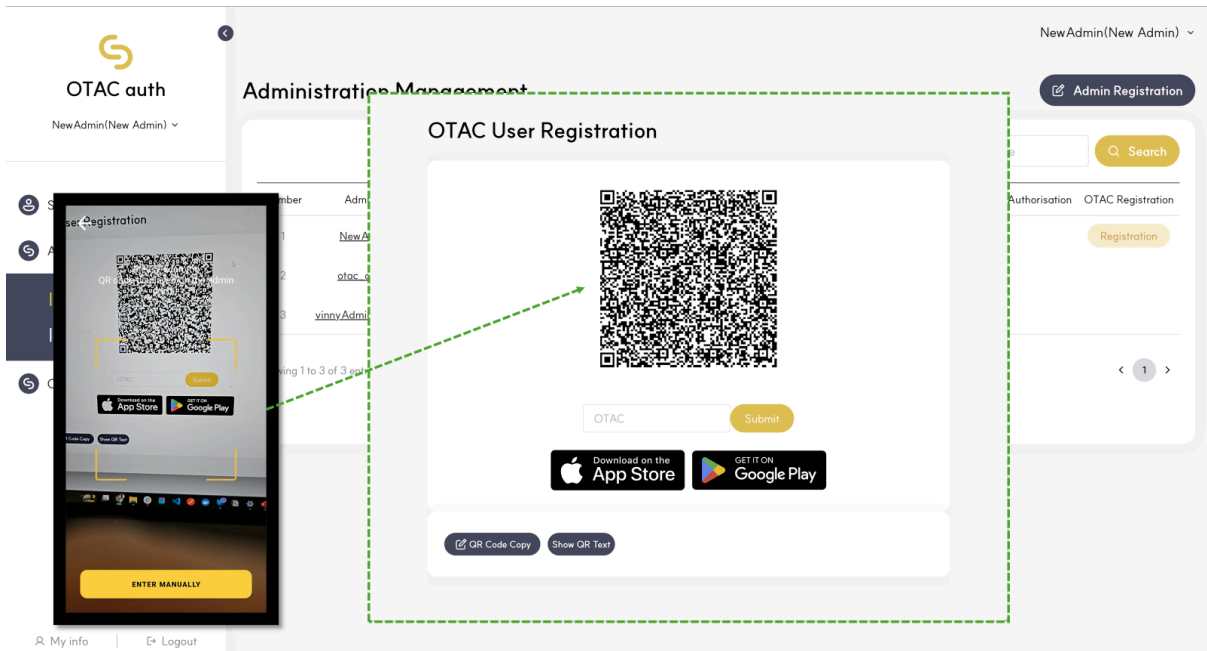
Setup OTAC login for an Admin

Once you have logged in as the new admin, Navigate to the Administration Management page.

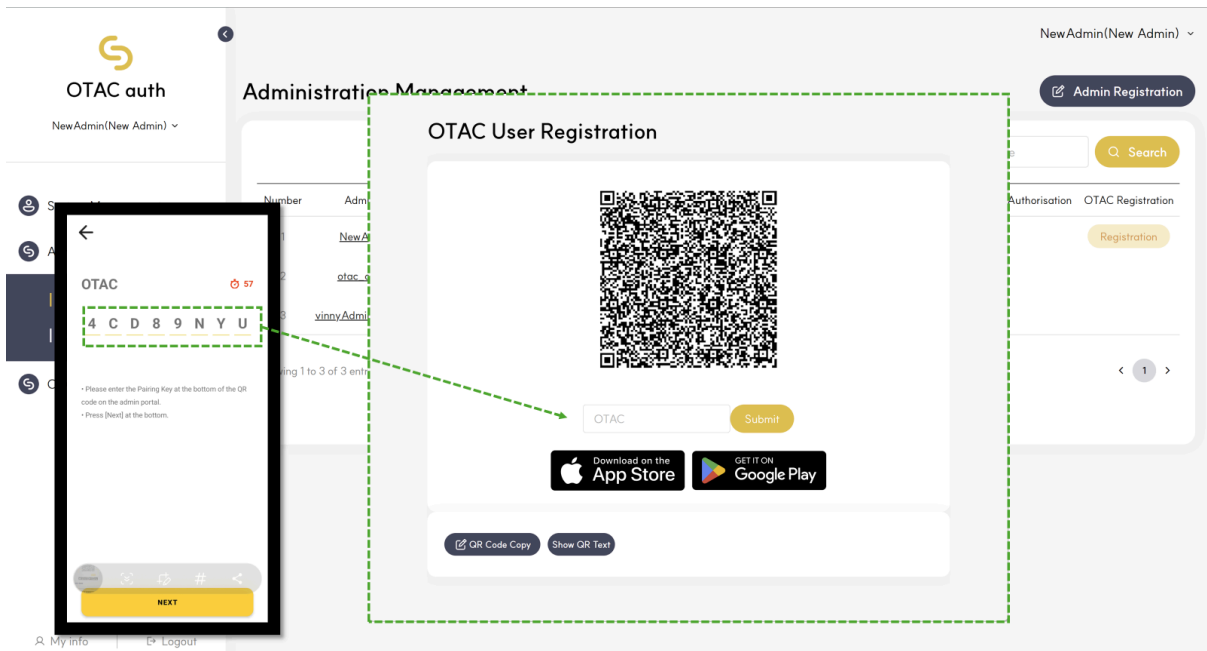


1. Click on Registration button in the OTAC registration columns
2. On the OTAC auth mobile app, click on Add Account and input the User Key from the mobile app onto the OTAC User Registration page in the admin portal along with other details:
 - a. System ID: The system the admin belongs to.
 - b. User Key: The user key from the mobile app
 - c. Qr expiry time (min): The number of minutes the QR code (shown in the next step) is valid for.
 - d. App account name: The display name shown on the mobile app when the pairing is complete.
3. Click on the Save button.

On the mobile app click on the SCAN QR CODE button.



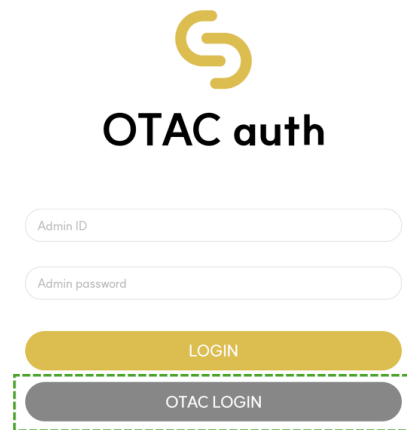
- Scan the QR code from the mobile app shown on the admin portal.



- Once the QR code is scanned, input the OTAC on the mobile app to the admin portal.
- Click on Submit on the admin portal.
- Click NEXT mobile app, check the account name and click on Finish to complete the pairing process.

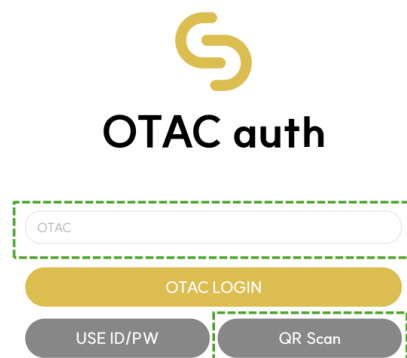
Logging as the Admin using OTAC

On the login screen, click on the OTAC LOGIN button.



The image shows the OTAC auth login screen. At the top is the Swidch logo (a stylized 'S' in a circle). Below it is the text 'OTAC auth'. There are two input fields: 'Admin ID' and 'Admin password'. Below these are two buttons: a yellow 'LOGIN' button and a grey 'OTAC LOGIN' button. The 'OTAC LOGIN' button is highlighted with a dashed green border.

- You can either input the OTAC for the admin account (generated on the mobile app) manually or by scanning QR code.
-



The image shows the OTAC auth login screen. At the top is the Swidch logo (a stylized 'S' in a circle). Below it is the text 'OTAC auth'. There is an input field for 'OTAC' which is highlighted with a dashed green border. Below this are three buttons: a yellow 'OTAC LOGIN' button, a grey 'USE ID/PW' button, and a grey 'QR Scan' button. The 'QR Scan' button is also highlighted with a dashed green border.

- To scan the QR code, click on the QR Scan mobile on the admin portal.
- On the mobile app click on the OTAC for the admin account, this will pop up a QR code.

- Place the mobile app screen in front of your PC's camera to scan the QR code and input the OTAC manually.



Admin Login History

This is the administrator login history page, you can view records of successful and failed logins.

The screenshot shows the 'Administrator Activity' page with the 'Administrator Login History' tab selected. The page includes a sidebar with navigation options like 'Administration Management', 'OTAC Management', and 'Audit Logs'. The main content area features a table of login records with the following data:

Number	Admin ID	Admin Name	Login success status	Login date and time	Connection IP
1	vinnyAdminEPC1522	Vinny	Success	2024-03-25 13:35	192.168.1.45
2	vinnyAdminEPC1522	Vinny	Success	2024-03-25 12:46	192.168.1.45
3			Failure	2024-03-25 12:45	192.168.1.45
4	vinnyAdminEPC1522	Vinny	Success	2024-03-25 11:44	192.168.1.45
5	vinnyAdminEPC1522	Vinny	Failure	2024-03-25 11:43	192.168.1.45
6	otac_admin	admin	Success	2024-03-25 10:31	192.168.1.45
7	vinnyAdminEPC1522	Vinny	Failure	2024-03-25 10:30	192.168.1.45
8	otac_admin	admin	Success	2024-03-22 16:32	192.168.1.45
9	otac_admin	admin	Failure	2024-03-22 16:32	192.168.1.45
10	otac_admin	admin	Failure	2024-03-22 16:32	192.168.1.45

You can use the tab to go to Admin Login History and Admin Activity History

- Admin ID: Displays the ID of the admin account
- Admin Name: Admin account's displays the name
- Login success status: Displays whether the login attempt failed or was successful
- Login date and time: Displays the date and time of the login attempt
- Connection IP: Displays the accessed IP

Admin Activity History

This is the administrator activity record page. You can view the history of modifications made by administrators.

The screenshot displays the 'Administrator Activity History' page in the OTAC auth system. The page includes a sidebar with navigation options like 'Administration Management', 'OTAC Management', and 'Audit Logs'. The main content area shows a table of activity records. A 'Download Excel' button is located in the top right corner. The 'Administrator Activity History' tab is highlighted with a green dashed box.

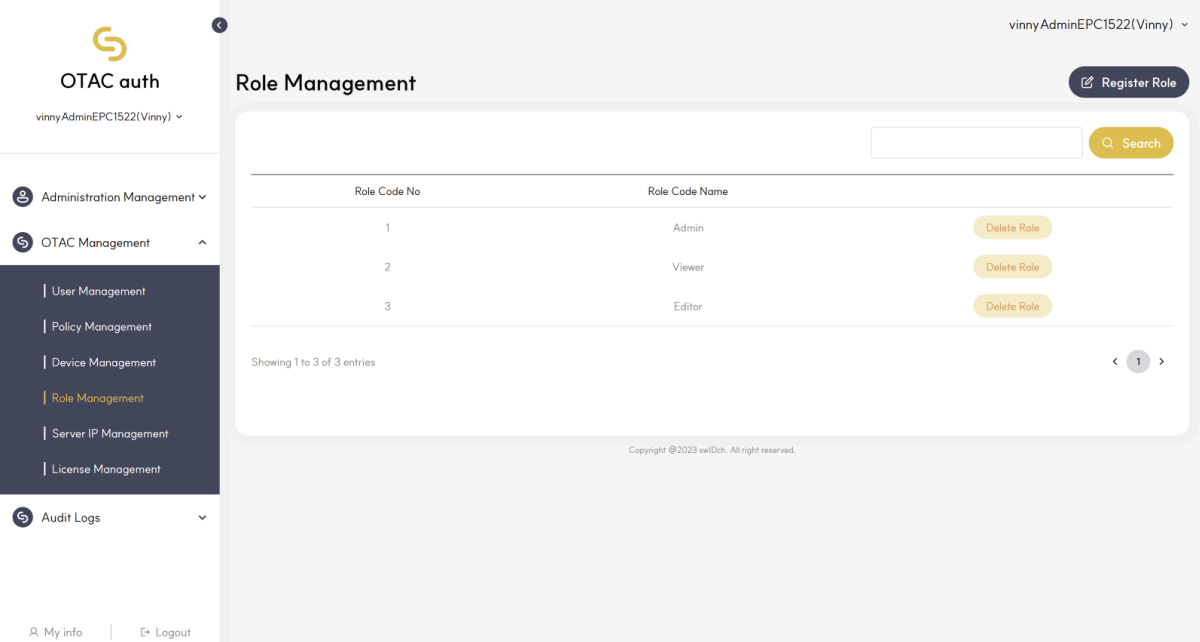
Number	Admin ID	Admin Name	Activity	Target	Type	Explanation	Date
1	vinnyAdminEPC1522	Vinny	Admin management	otac_admin	Update	Type Super Admin	2024-03-25 13:38
2	vinnyAdminEPC1522	Vinny	Admin management	otac_admin	Update	Type Delegated Admin Admin service addition plc	2024-03-25 13:38
3	vinnyAdminEPC1522	Vinny	Device Management	Declan	Update	Device : Role [1] Device : PLC DEVICE ID 192.168.1.100	2024-03-25 12:34
4	vinnyAdminEPC1522	Vinny	Role Management	2	Delete	Role [Role Code No 2]	2024-03-25 12:33
5	vinnyAdminEPC1522	Vinny	Role Management	2	Save	[Role Code No 2] [Role Code Name Editor]	2024-03-25 12:33
6	vinnyAdminEPC1522	Vinny	Role Management	2	Delete	Role [Role Code No 2]	2024-03-25 12:33
7	vinnyAdminEPC1522	Vinny	Role Management	2	Save	[Role Code No 2] [Role Code Name Editor]	2024-03-25 12:32
8	otac_admin	admin	Device Management	Declan	Save	Device : Role [1] Device : System id 1 Device : User ID Declan Device : PC DEVICE ID 127.0.0.1 Device : PLC DEVICE ID 192.168.1.10	2024-03-25 10:51

- Admin ID: Displays the ID of the admin account
- Admin Name: Admin account's displays the name
- Activity: Displays the executed menu page
- Target: Displays the ID of the modified target
- Type: Displays the type modified by the administrator , such as saving or deleting
- Explanation : Displays an explanation of the modification record

OTAC Management

Role Management

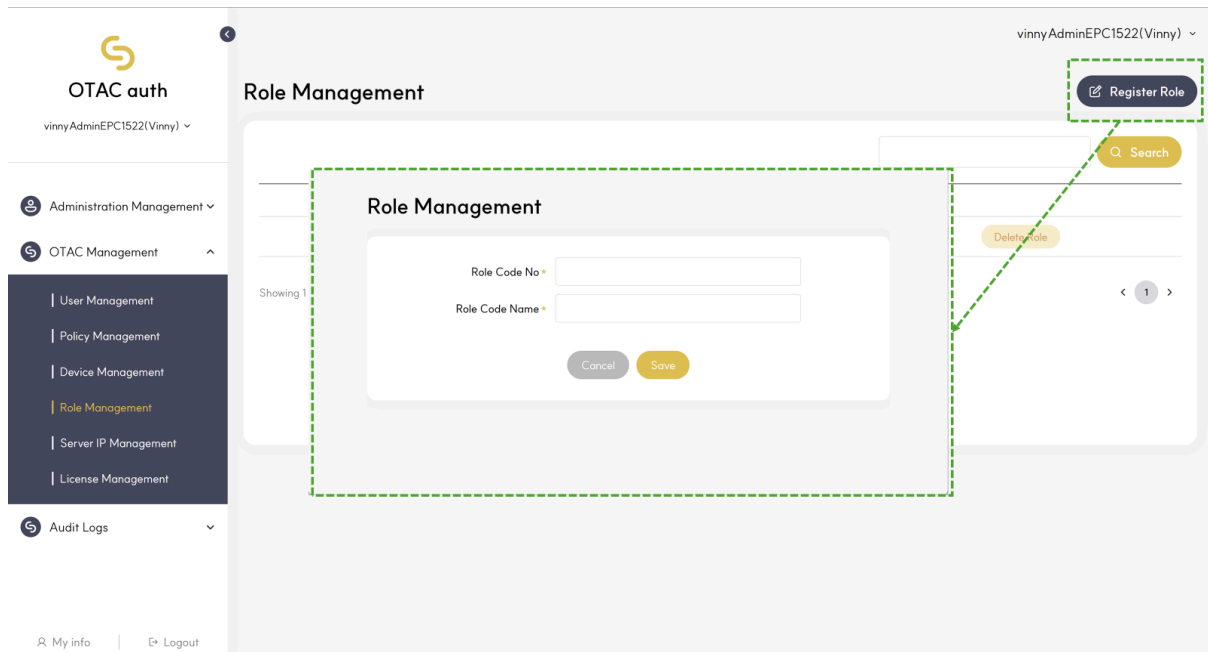
Role Management lets you define the various roles you can assign to a user in order for them to have the correct level of authorization in the PLC.



Role Code No	Role Code Name	
1	Admin	Delete Role
2	Viewer	Delete Role
3	Editor	Delete Role

- Role Code No : Displays the role number
- Role Code Name: Displays the role name
- Register Role: Go to the Role registration pop-up
- Delete Role: Deletes a role

Role Registration



To register a new role click on Register Role

- Role Code No : Enter the role number
- Role Code Name: Enter the role name

The valid roles for PLC are:

<ul style="list-style-type: none"> ● Admin ● SecurityAdmin ● SecurityAuditor ● SafetyFirmwareUpdater ● SafetyEngineer ● CertificateManager ● UserManager ● Engineer ● Commissioner ● Service ● DataViewer ● DataChanger ● Viewer 	<ul style="list-style-type: none"> ● EHmiLevel1 ● EHmiLevel2 ● EHmiLevel3 ● EHmiLevel4 ● EHmiLevel5 ● EHmiLevel6 ● EHmiLevel7 ● EHmiLevel8 ● EHmiLevel9 ● EHmiLevel10 ● FileReader ● FileWriter ● EHmiViewer ● EHmiChanger ● SoftwareUpdate
---	--

User Management

This page shows the list of users in the system along with their status.

The screenshot displays the 'User Management' page in the OTAC auth system. The page header includes the 'swidch' logo and the user's name 'vinnyAdminEPC1522(Vinny)'. The main content area features a table with the following data:

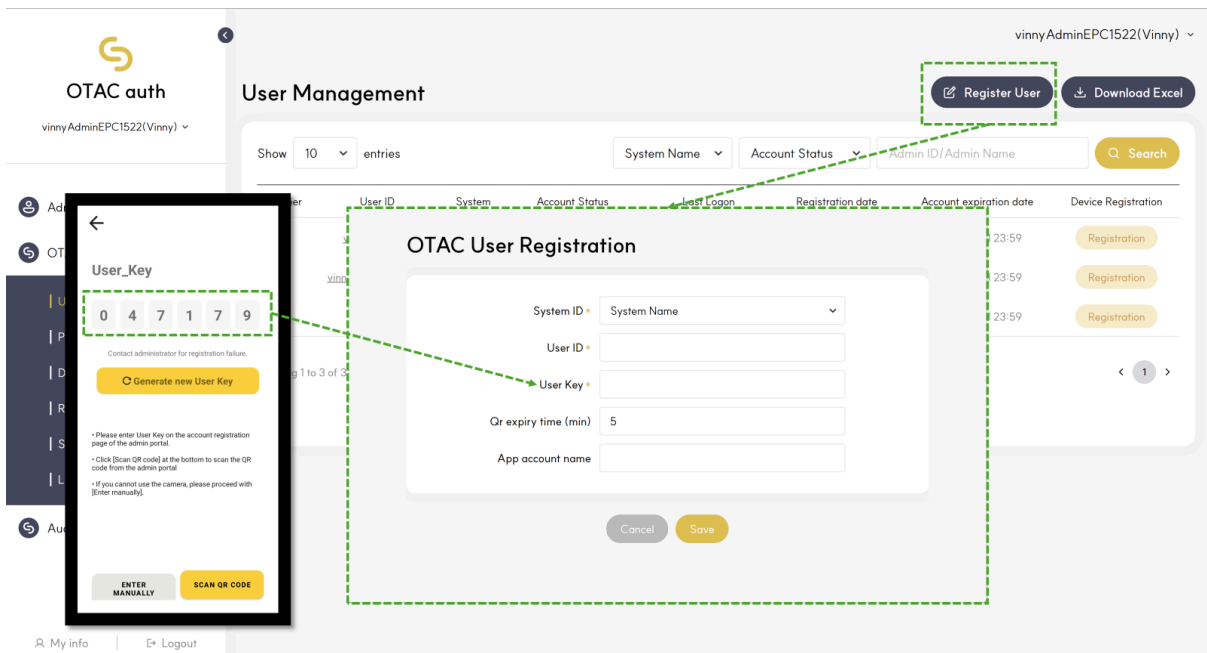
Number	User ID	System	Account Status	Last Logon	Registration date	Account expiration date	Device Registration
1	vinnyEPC1522	plc	Active	2024-03-26 10:46	2024-03-22 16:52	2059-12-31 23:59	Registration
2	vinnyAdminEPC1522	plc	Active	2024-03-26 10:43	2024-03-25 12:45	2059-12-31 23:59	Registration
3	Declan	plc	Terminated user	2024-03-25 10:51	2024-03-25 10:51	2059-12-31 23:59	Registration

The interface also includes a search bar, filters for 'System Name' and 'Account Status', and a 'Show 10 entries' dropdown. A sidebar on the left provides navigation for various management tasks.

- User ID : Displays the user's ID
- System : Displays the name of the system used
- Account Status : View and change the user's status
 - Active : Activates the user
 - Suspended: Pauses user
 - Terminated User: De-registers a user
- Last Logon: User's Displays the last authentication date
- Registration date: Displays the user's registration date

User Registration

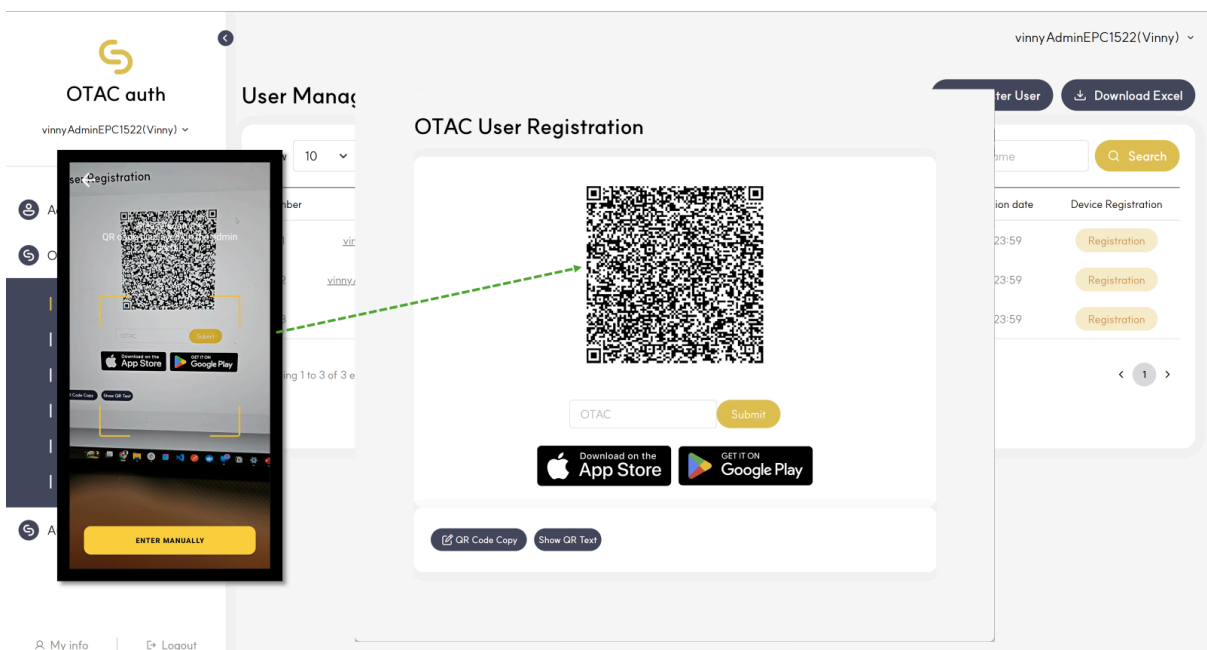
To register a new user make sure the user has the OTAC auth mobile app installed on their phone. The user registration happens in tandem with the administrator and user with the mobile app. For the user mobile follow Account Registration steps in the OTAC auth User Manual guide.



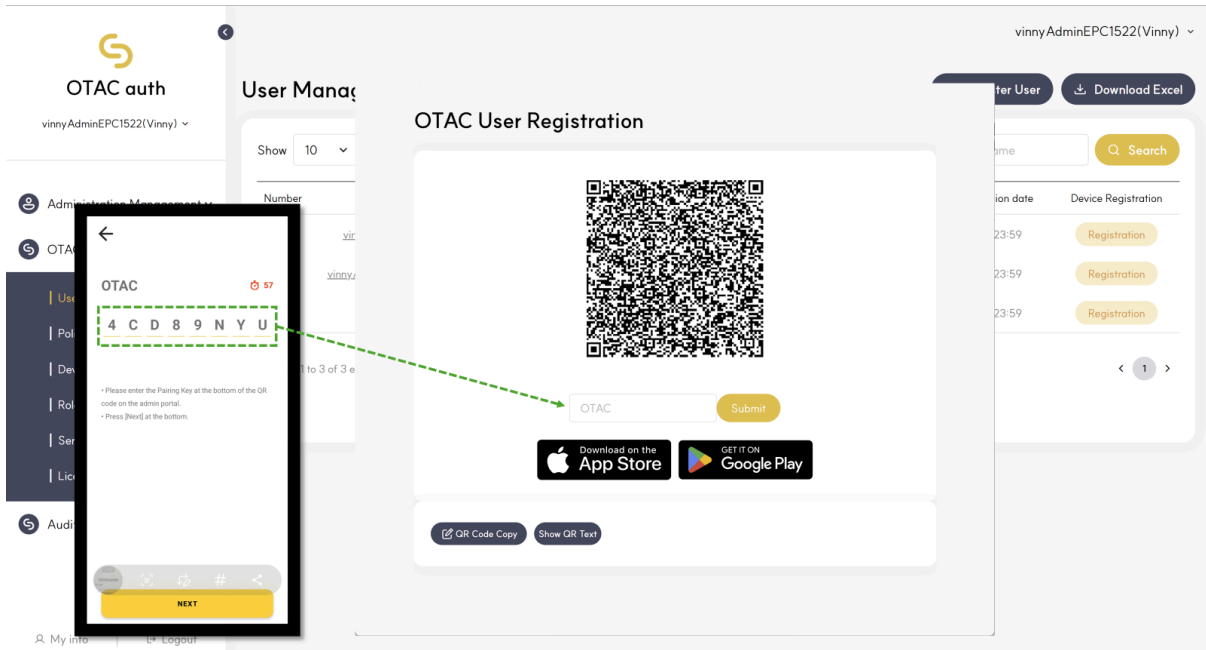
On the mobile app select the [Add Account] button on the main screen. This will show a 8 digit User Key

On the Admin Portal click on the Register User button,

- System ID : Set the ID of the system
- User ID : Set the user's ID
- User Key : Enter the User key information displayed in the mobile app
- QR Expiry Time : Set the QR code expiry time
- App Account Name : Enter the account name to be displayed in the app
- Save : Click the Save button to go to the QR authentication page



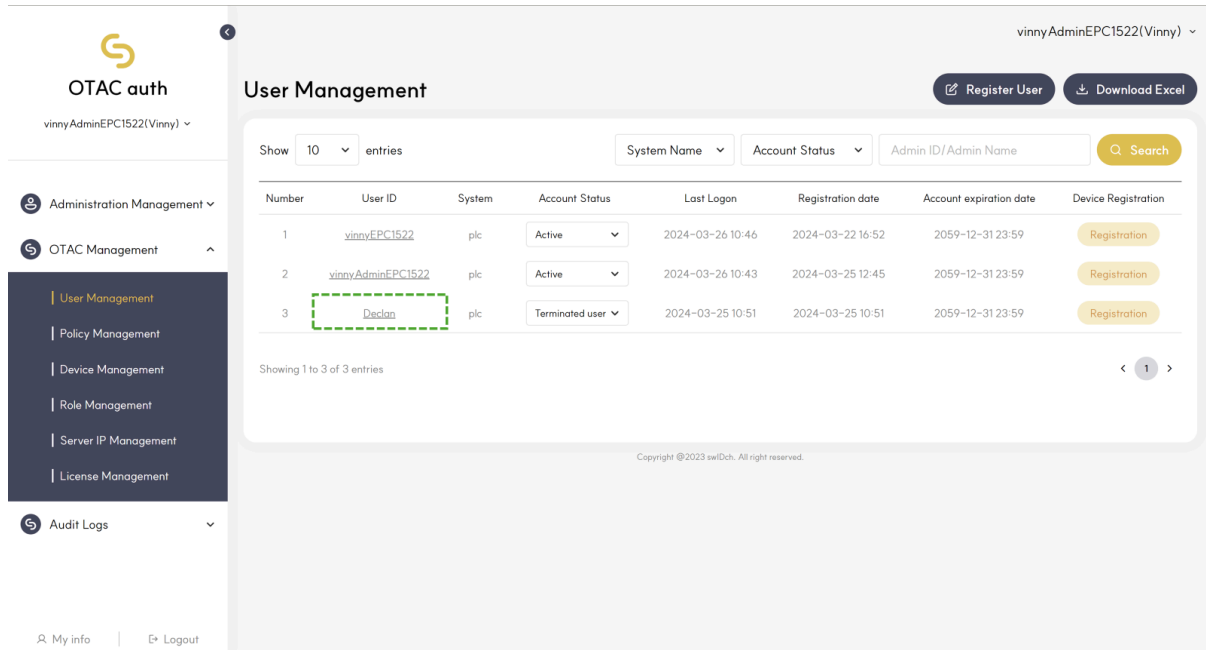
- On the mobile app click on [Scan QR Code] and scan the QR code on the admin portal.



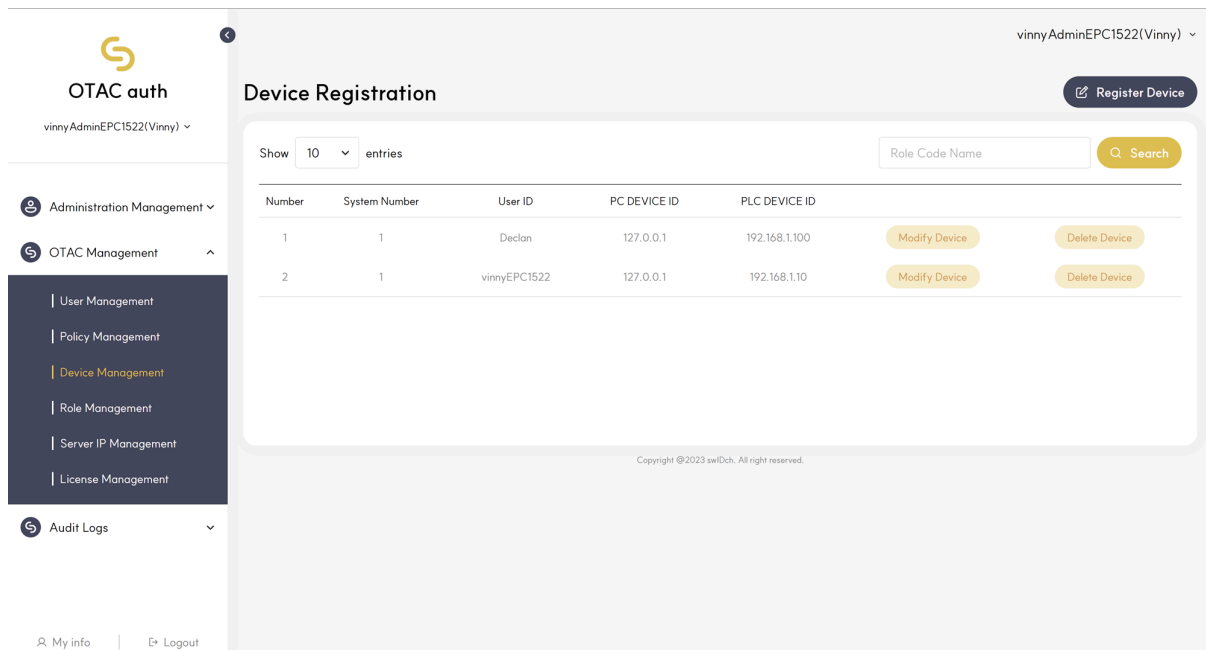
- The mobile app will generate an OTAC, input the OTAC in the admin portal below the QR code image.
- Click submit on the admin portal and next on the mobile app to finish the registration process.

Device Management

After registering a user you need to register a device in order for the OTAC verification to work. A device represents a PLC, to view devices a particular user has access to, click on the User ID from the User Management page.



This will bring you to the device page.



The Device page shows:

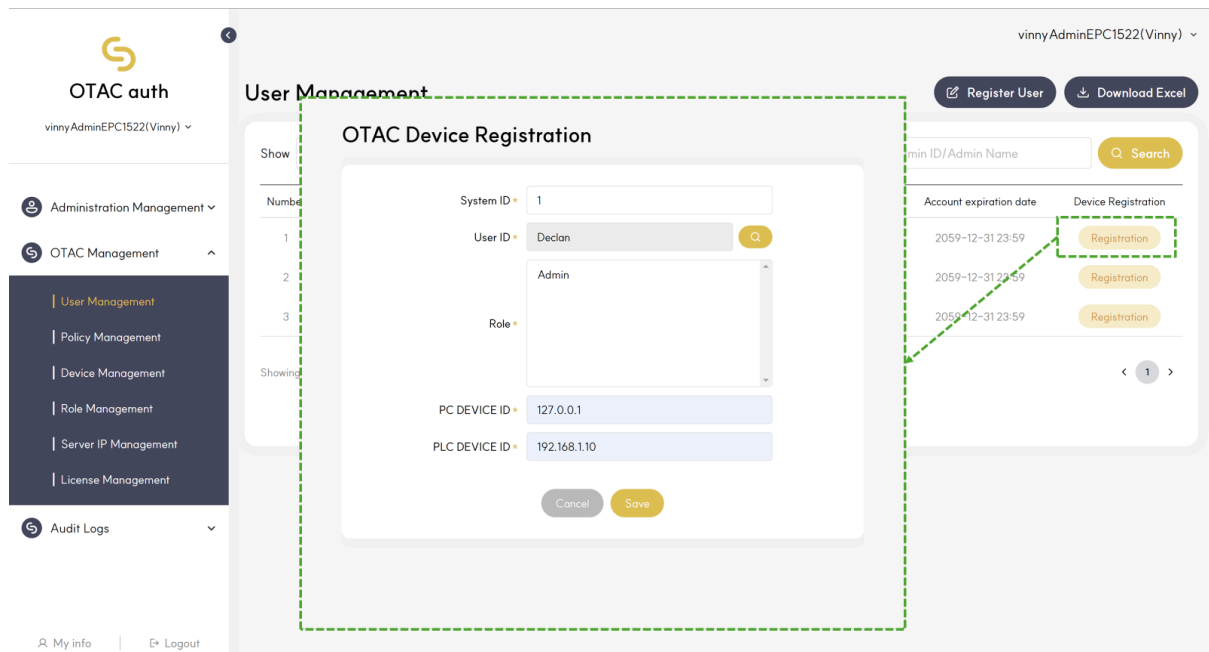
- System number : Displays the system number .
- User ID: Displays the user ID
- PC DEVICE ID: The ID of the PC from where the user is allowed to access the PLC
- PLC DEVICE ID: The ID of the PLC which the user is allowed to access

- Modify Device: Go to the device modification pop-up
- Delete a Device: Delete the device

Once a user has be registered you need to also register a device

Device Registration

You can register a new device for a user directly from the User Management page and clicking on the Registration button on the user, or by going to the Device Management page and clicking on Register Device.



On the OTAC Device Registration page fill in the following details:

- System number: Enter the system number
- User ID: Enter the User ID (If you are coming from the User Management, this will automatically be filled for you)
- Role : Select the role of the device .
 - - You can select multiple items by pressing Ctrl + clicking
 - - Role registration is possible on the role management page
- PC DEVICE ID : Enter the PC DEVICE ID the default can set to 127.0.0.1
- PLC DEVICE ID: Enter PLC IP address the default is 192.168.1.10

Modify Device

The screenshot displays the 'OTAC Modify Device' form within the 'Device Registration' section of the admin interface. The form contains the following fields and values:

- System ID: 1
- User ID: vinnyEPC1522
- Role: Admin, Viewer
- PC DEVICE ID: 127.0.0.1
- PLC DEVICE ID: 192.168.1.10

The 'Modify Device' button is highlighted with a green dashed box, and a green dashed line connects it to the 'Modify Device' button in the main interface. The interface also includes a sidebar with navigation options, a top navigation bar with a search bar, and a 'Register Device' button.

On the OTAC Device Modify page you can modify the following fields:

- System number : Enter the system number
- User ID: Enter your user ID
- Role : Select the role of the device .
 - - You can select multiple items by pressing Ctrl + clicking .
 - - Role registration is possible on the role management page
- PC DEVICE ID : Enter the PC DEVICE ID the default can set to 127.0.0.1
- PLC DEVICE ID: Enter PLC IP address the default is 192.168.1.10

Policy Management

The policy management shows the behavior of OTAC and how it is validated. You can have separate policies for different systems.

The screenshot shows the 'Policy Management' page in the OTAC auth admin interface. The page title is 'Policy Management' and the user is logged in as 'vinnyAdminEPC1522(Vinny)'. The interface includes a sidebar with navigation options: Administration Management, OTAC Management (expanded), and Audit Logs. The main content area displays a table with the following data:

Number	System Name	System number	Log Policy	Correction Policy	OTAC generation frequency	Number of checks policy
1	plc	1	Save all	No auto-correction	60Second	3 Multiple

Below the table, it says 'Showing 1 to 0 of 0 entries'. There are two buttons: 'Register policy' and 'Modify policy'. The footer of the page reads 'Copyright ©2023 swidch. All right reserved.'

- System Name : Displays the name of the system
- System number : Displays the system number
- OTAC generation frequency: Displays the system check cycle
- Number of checks policy: Displays the number of checks in the system
- Register Policy: Go to the system registration pop-up
- Modify policy: Go to the system modification pop-up
- Delete a policy: Delete the system

Create a new Policy

The screenshot displays the 'Policy Management' section of the OTAC auth admin interface. A sidebar on the left contains navigation options: Administration Management, OTAC Management (expanded), User Management, Policy Management (highlighted), Device Management, Role Management, Server IP Management, License Management, and Audit Logs. The main content area is titled 'Policy Management' and features a 'Register policy' button in the top right corner. Below this, the 'OTAC Policy Registration' form is visible, containing the following fields:

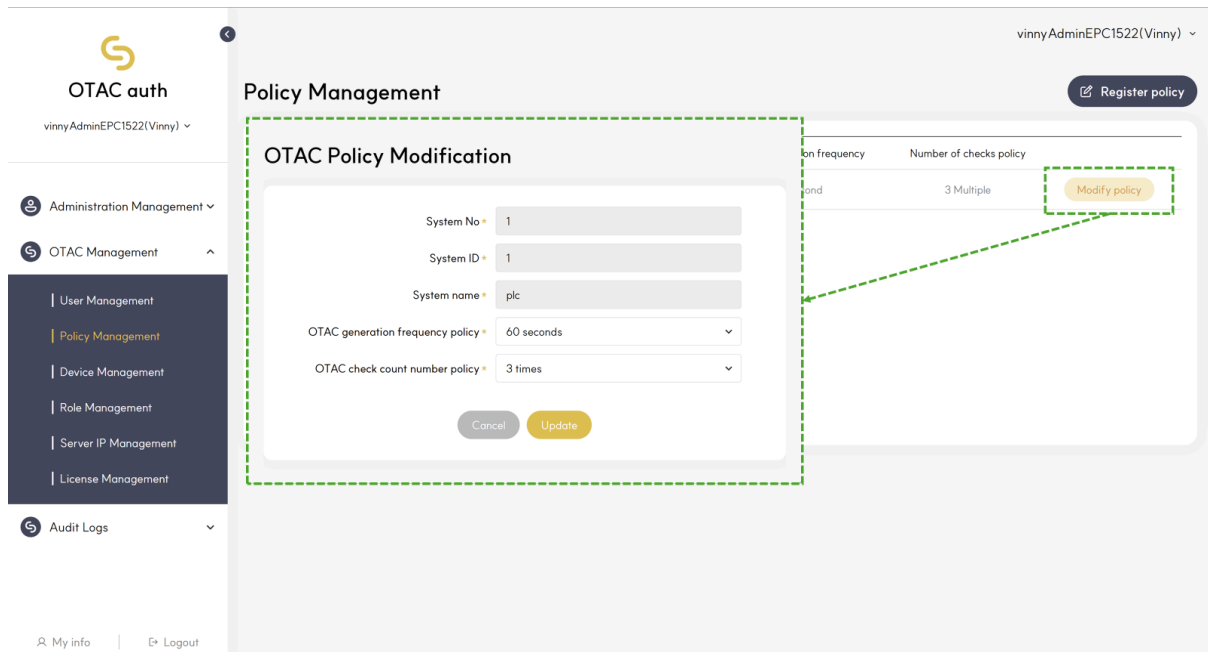
- System ID: 1-127
- System Name: (empty)
- OTAC generation frequency policy: 60 seconds
- OTAC check count number policy: 3 times

Buttons for 'Cancel' and 'Save' are located at the bottom of the form. A table on the right side of the interface shows a summary of the policy with columns for 'Generation frequency' and 'Number of checks policy', and a 'Modify policy' button. A green dashed box highlights the 'Register policy' button and the registration form.

You can create a new policy by clicking on the Register policy button:

- System ID: System ID of the policy
- OTAC generation frequency policy: The duration of the OTAC validity period
- OTAC check count number policy: OTAC is validated against time stamp on the PLC. To account for slight time difference between the mobile app and the PLC you can increase the check counter from 3 (default) to 5.

Modify an existing Policy



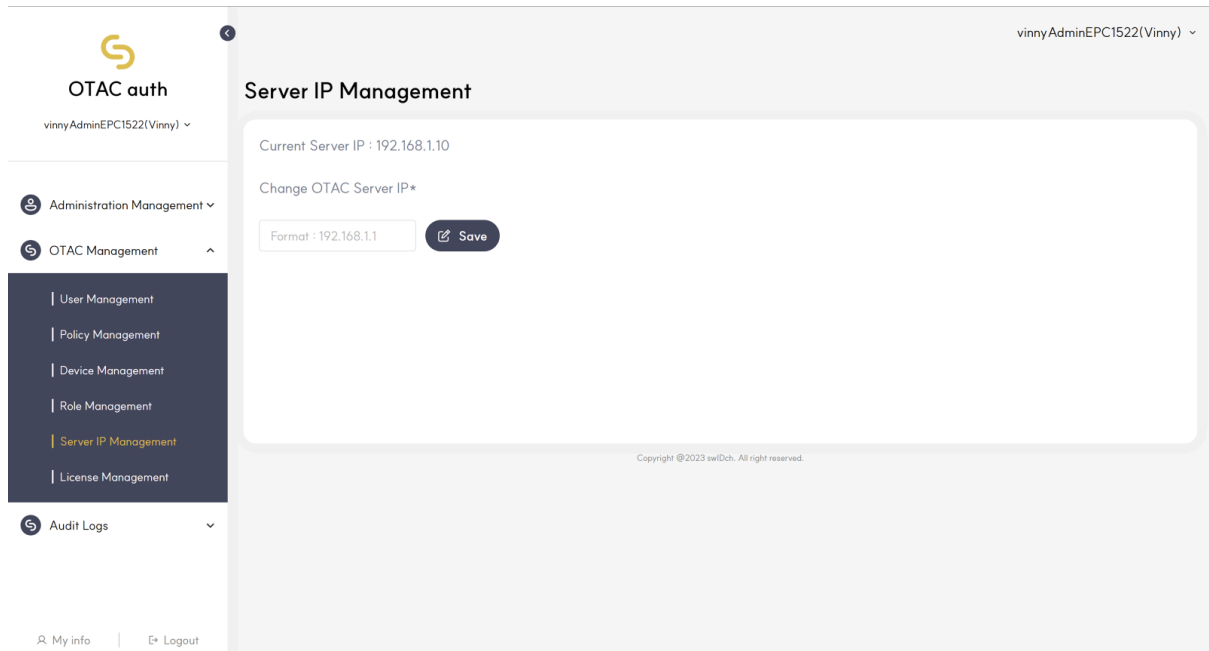
You can modify an existing policy by clicking on the Modify policy button:

- System ID: System D of the policy
- System name*: This is the display name of the system.
- OTAC generation frequency policy: The duration of the OTAC validity period
- OTAC check count number policy: OTAC is validated against time stamp on the PLC. To account for slight time difference between the mobile app and the PLC you can increase the check counter from 3 (default) to 5.

Please Note: If you change the property of an existing policy already in use, all users must be re-registered.

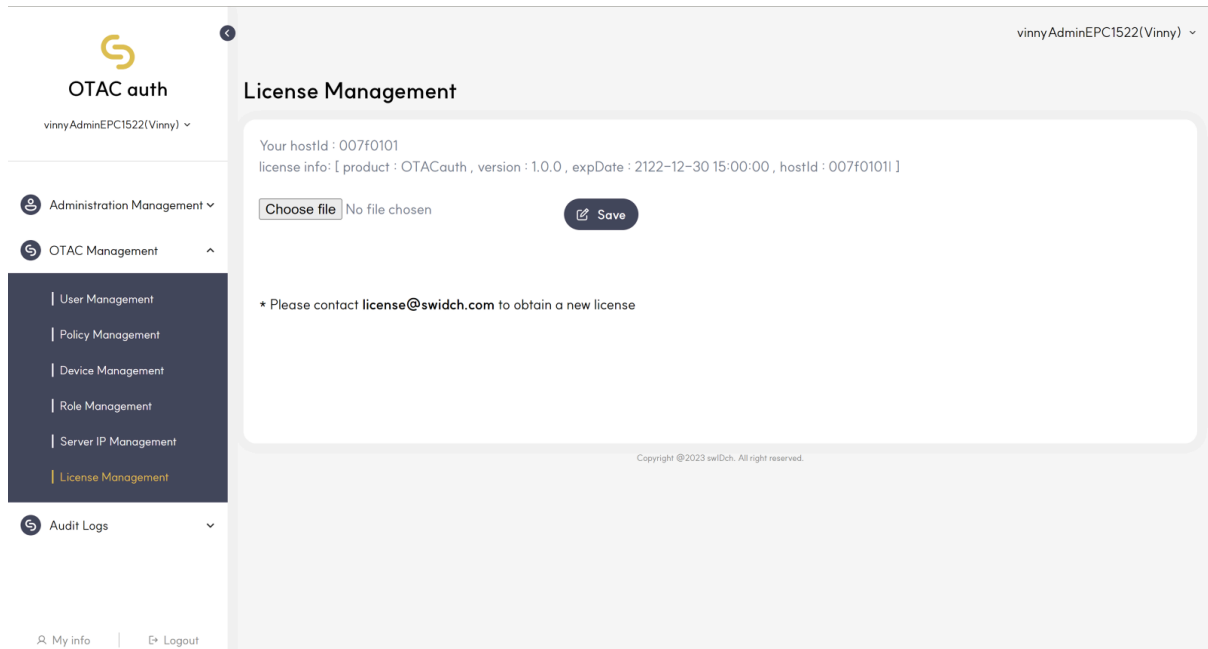
Server IP Management

If you have changed the default IP address of the PLC device, you can update the IP address of the OTAC server from this page:



License Management

This page is used to upload a new license file or update an existing one. Once you have uploaded a license, you will have to restart the PLC for the licenses to take effect.



Obtaining a license file: Please contact license@swidch.com to obtain a license file. You will need to provide us the hostid of the PLC which can be found on the Admin Portal under System Management > License Management

Audit Logs

Authentication Success Events History

The screenshot displays the 'Successful Authentication Events History' page in the OTAC auth Admin Manual. The page features a sidebar on the left with navigation options: Administration Management, OTAC Management, and Audit Logs. The main content area shows a table with 10 entries, each containing a Number, User ID, System, OTAC, and Authentication date. The table is filtered for the date range 2023-12-27 to 2024-03-26. A 'Download Excel' button is visible in the top right corner of the table area. The footer includes 'My info' and 'Logout' links, and a copyright notice for 2023 swidch.

Number	User ID	System	OTAC	Authentication date
1	vinnyEPC1522	plc	DM9Y7SFR	2024-03-26 10:46
2	vinnyEPC1522	plc	1PA0TH85	2024-03-26 10:44
3	vinnyAdminEPC1522	plc	MR.JICCGH	2024-03-26 10:43
4	vinnyAdminEPC1522	plc	ZZFV64MU	2024-03-26 10:43
5	vinnyAdminEPC1522	plc	16SS57JJ	2024-03-25 13:35
6	vinnyAdminEPC1522	plc	A0TIXMMH	2024-03-25 12:46
7	vinnyAdminEPC1522	plc	BZ70L41S	2024-03-25 12:45
8	Declan	plc	SLOP2M4B	2024-03-25 10:51
9	vinnyEPC1522	plc	KGHONU97	2024-03-25 10:37
10	vinnyEPC1522	plc	MOF1CVMA	2024-03-25 10:35

This page shows a log of successful logon events

- User ID : Displays the user's ID.
- System : Displays the name of the system used.
- OTAC: used Displays OTAC.
- transaction-linked data: Displays any transaction data.
- Authentication date : Displays the authentication date

Authentication Failure Events History

The screenshot displays the 'Failed Authentication Events History' page. On the left is a navigation sidebar with 'OTAC auth' and 'vinnyAdminEPC1522(Vinny)'. The main content area has a title 'Failed Authentication Events History' and a 'Download Excel' button. Below the title are filters for 'Show 10 entries', a date range '2023-12-27 - 2024-03-26', 'System Name', and 'Admin ID/Admin Name'. A search button is also present. The table below contains one entry:

Number	User ID	System	Activity	OTAC	Authentication Failure	Status code	Description
1	vinnyAdminEPC1522	plc	Registration	BZ70L41S	2024-03-25 12:45	O900	ALREADY_USED_OTAC

Below the table, it says 'Showing 1 to 1 of 1 entries' with a pagination control showing '1'. At the bottom of the page, there is a footer: 'Copyright ©2023 swidCh. All right reserved.' and navigation links for 'My info' and 'Logout'.

This page shows a log of failed logon events

- User ID : Displays the user's ID.
- System : Displays the name of the system used.
- Activity : Displays the type of use, such as registration or authentication.
- OTAC: The OTAC used to logon.
- Authentication date : Displays the authentication date .
- Status code : Displays the failure code .
- Description : Displays the description of the corresponding failure log .

Registered/Terminated User History

The screenshot shows the 'Registered/Terminated User History' page in the OTAC auth Admin Manual. The page features a sidebar with navigation options: Administration Management, OTAC Management, and Audit Logs. The main content area displays a table with columns for Number, User ID, System, Category, and Date. The table contains 6 entries. A search bar and a date range filter are also visible.

Number	User ID	System	Category	Date
1	vinnyEPC1522	plc	Reregistration	2024-03-26 10:44
2	vinnyAdminEPC1522	plc	Reregistration	2024-03-26 10:42
3	vinnyAdminEPC1522	plc	Registration	2024-03-25 12:45
4	Declan	plc	Registration	2024-03-25 10:51
5	vinnyEPC1522	plc	Reregistration	2024-03-25 10:35
6	vinnyEPC1522	plc	Registration	2024-03-22 16:52

This page shows an audit log of users who have been registered and terminated.

- User ID : Displays the user's ID
- System : Displays the name of the system used
- Category : Displays types such as registration, suspended or de-registered
- Date: Displays registration and cancellation dates