Salto KS - Dealer Documentation

The **Salto KS** driver suite enables seamless Control4 integration with **Salto Keys as a Service (KS)** cloud-based access control solution. The suite consists of two drivers:

- **Salto KS**: The main proxy driver for the Salto KS Connect API connection.
- **Salto Lock**: Represents the individual physical locks present in the Salto KS site.

Installation and Updating

Installation Steps

1. Unzip the driver zip file.
2. In Composer Pro:
   - Go to **Driver > Add or Update Driver or Agent**.
   - Add `salto_ks.c4z`, then `salto_lock.c4z`.
   - **Both drivers must be added before proceeding.**

Configuration

Prerequisites

Detailed user documentation is provided separately in the unzipped driver zip file. Send this documentation to the user.

1. User must have a Salto KS admin account: https://app.saltoks.com/login.
2. Locks must be configured in Salto KS.
3. User must configure a new remote unlock user for Control4.

The user does not need to share their password with the dealer. Password sharing is discouraged. Users can authenticate the driver themselves in the following steps.

Initial Setup

Note: The authentication process has a 30 minute timeout so ask the customer to be ready when you send the link. If the process times out, run the 'Authenticate' action again for a new link.

1. In **System Design**, search for **Salto KS** driver and add the driver to the project.

2. Select the driver in the project.

3. In the **Properties** tab:

   - In the **Actions** property dropdown, select `Authenticate` and click **Set**
   - Copy the `Authentication URL` that appears

4. Send the authentication link to the customer. The authentication link will direct them to the Salto KS authentication site where they will enter the credentials of the Control4 remote unlock user they created per the driver user documentation.

5. When the user successfully completes the authentication process, the Salto API Information properties will populate with the user's email address. Check that the user authenticated with the new remote unlock user they created and not their personal admin account.

Activate IQs

Activating the IQ is the process of retrieving a secret from the IQ and an initial pin code from the remote unlock user. With these pieces of information the driver can generate a One Time Password (OTP). This OTP is a second factor of authentication for important actions on API endpoints, such as remote unlocking. This ensures the highest security is maintained by this integration.