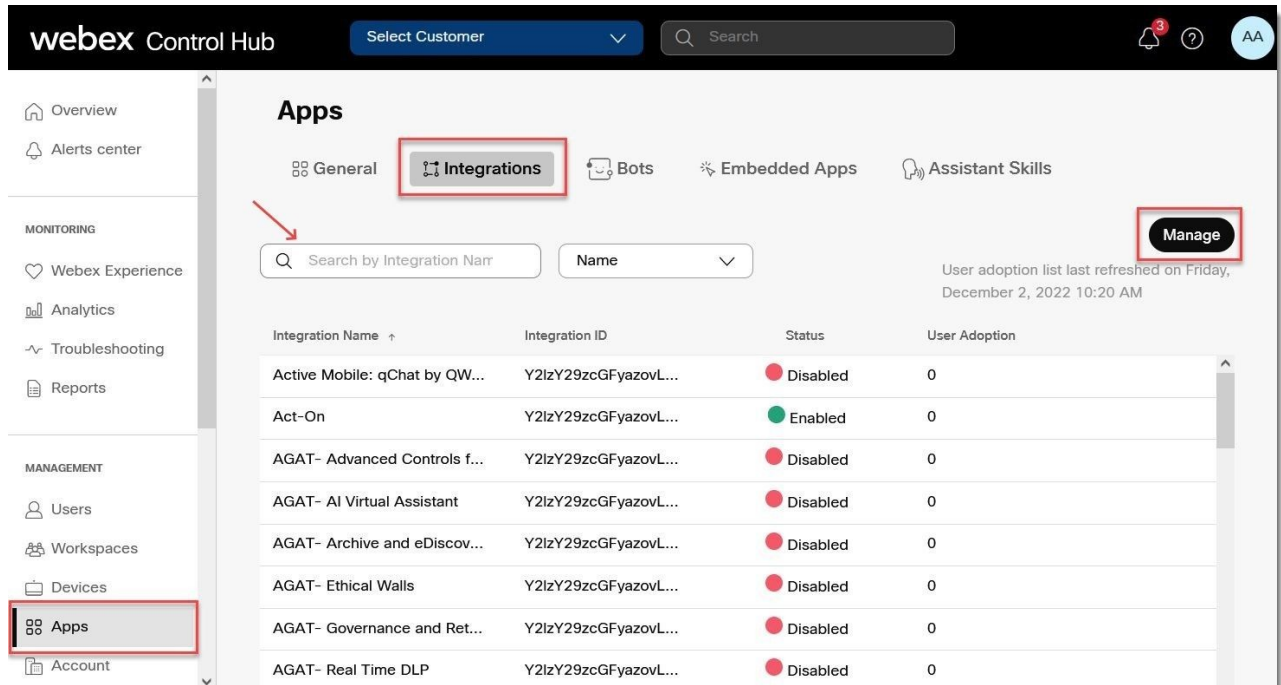


Troubleshooting Cisco Webex Calling Integrations Authorizations

If the authorization procedure for Imagicle apps fails with the following error message: "Access denied - Your administrator denied access to the integration you selected. We captured your request and will let them know".

Then you can selectively authorize Imagicle applications by accessing Webex Control Hub [Apps](#) [Integrations](#) and locate Imagicle apps [by Integration ID](#):



- Imagicle UCX Suite Users' Synch from Control Hub:

C89a4ba3aa80c33dd80bfc17a1572c5026049234c0aa90b7793b47dac37d7fa6c

- Imagicle Attendant Console Webex Presence Retrieval:

C1468e046a54f78620ca6d1b16eda8096165d0f960078c8e38c5ac09fb7f7f120

- Imagicle Attendant Console Call Control:

C143958d8c8645673914400fbf4b06fa022da2a7caeac67b5eb48d062709cf24e

- Imagicle Call Analytics CDRs retrieval from Control Hub:

C2b09ee9cb8a3ae94ae0e6417d7dcf7e33351ae00bbb22fb9937a79796a8371b5

- Imagicle SSO against Cisco Control Hub:

C287f727f93d20644fd10a5bd2d3c8b6796497bd21bd28d92e588f470ceb546c4

Please consult relevant Cisco documentation [here](#).

Admin User Authorizer

The authorization process involves a Full Admin user from the customer which, through own Webex account, authorizes Imagicle Integrations. This user should never disable presence status sharing. **The authorizations may automatically expire as soon as the authorizing user changes own password.** Once the authorization is removed, UCX Cloud Suite won't be able to retrieve events related to one or multiple authorizations. To recover the feature, a new authorization process must be executed.



This limitation does not apply if the authorizing user logs in Webex leveraging SSO using an external identity provider.

If SSO is not enabled, a user password by default expires after five years, as per the [documentation](#) (and an admin user can be created without requiring additional licenses).

This limitation is related to the authentication flow implemented by Webex, namely OAuth2 Authorization Code flow, that implies impersonating a user while accessing the Webex APIs. We are working with Cisco to remove this limitation.

The token is invalidated also in these two cases:

- Authorizing Webex user is deactivated
- Full Admin privileges are removed from the authorizing Webex user