Single Sign On for Imagicle UC Suite

Overview

Starting from 2022.Winter.2 release, Imagicle UCS supports Single Sign On (SSO) functionality. The integration with the customer's Identity Provider (IdP) must be intended in this way:

- a user can leverage the same corporate authentication method to log into Imagicle applications. The same corporate authentication method means the same Identity Provider and same credentials
- it does not mean that a user can log into his/her PC and he/she is automatically logged into Imagicle applications
- to leverage the SSO on the Imagicle applications, the UCS must be integrated with the corporate IdP

SSO is supported only in the SP-initiated mode, that is:

- the user first opens the Imagicle suite login form and enter his/her IdP username
- the user gets redirected to his/her IdP login form for authentication (possibly with MFA)

Imagicle SSO is based on Amazon Web Services "Cognito", that can be federated with many Identity Providers available on the market, like Azure AD or Cisco DUO. Imagicle Cloud is integrated with AWS that in turn are compatible with different Identity Providers. Before to be able to use SSO on their own Imagicle UCS, a configuration is required on both corporate IdP (this must be done by the customer) and Imagicle Cloud/AWS (this part is managed by Imagicle team).

Applications supporting SSO

- UCS Web Portal
- Jabber and Webex gadgets (both desktop and mobile)
- Finesse gadgets
- MS Teams gadgets (both desktop and mobile. Web app not supported)
- Attendant Console
- Manager Assistant
- Imagicle Voice Analytics

Other applications not listed here are not yet compatible with SSO (*). Please, check this kb to be always updated about the compatibility list.

*** NOTE**: there is not a fallback method, so if a user is configured to use SSO, that user can **only** use SSO. This means that if that user needs to access an application not listed here (so an application that does not yet support SSO, like the mobile apps), he/she will not be able to log into that application. So, in this case, do not configure SSO for that user.

Requirements

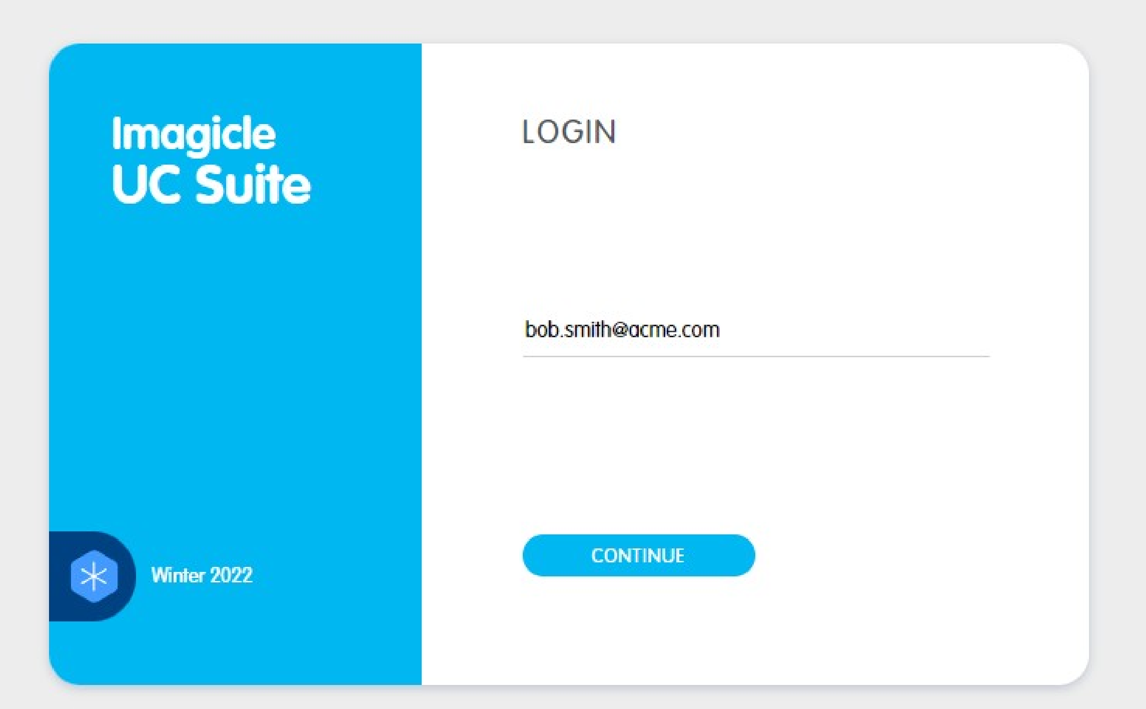
- customer's IdP must support either SAML or OpenID Connect. As of now, these are the only Imagicle supported standards for SSO
- Imagicle UC Suite 2022.Winter.1 or newer
- Imagicle UC Suite must be cloud connected or a Cloud Suite (UCCS). This is required to be able to retrieve from the Imagicle Cloud the SSO configuration for the customer's domain
- Imagicle UC Suite must reach the domain *.amazoncognito.com and *.amazonaws.com via HTTPS protocol. This is required for the login process
- Imagicle UC Suite must reach the corporate IdP, that can be either cloud or on-prem
- Imagicle UC Suite must be reachable from users via HTTPS protocol
- Imagicle UC Suite must have, at least, one FQDN
- only if Attendant Console is used
  - ♦ Imagicle Attendant Console 2022.Winter.1 or newer
  - ♦ Imagicle Attendant Console must reach the domain *.amazoncognito.com and *.amazonaws.com via HTTPS protocol. This is required to validate the token provided by Attendant Console
- only if Cisco Jabber gadgets are accessed outside corporate network (MRA is not supported)
  - ♦ gadgets must be configured as not internal, so "internal" parameter set to false (refer to this section for further information)

- Imagicle UC Suite must be reachable from Internet (only the HTTPS port, e.g., 443)

SSO login process

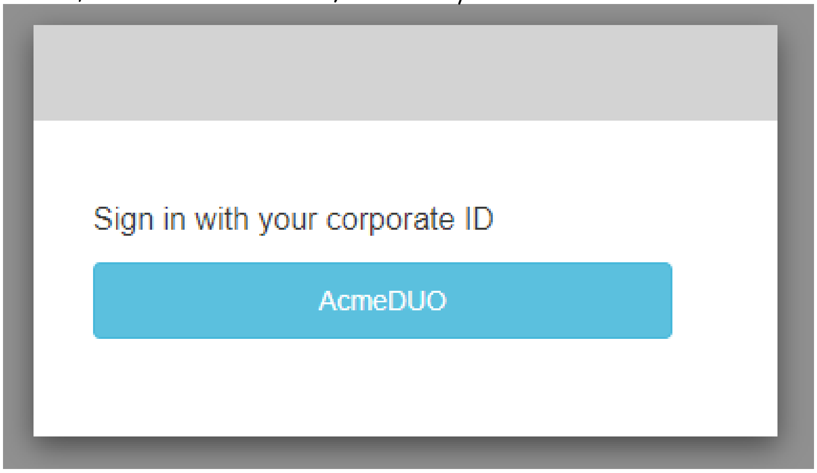
Let's see now how the integration between Imagicle and customer's IdP works in case of a user wants to log into the UCS web portal:

- user connects to the Imagicle UCS web portal (e.g., https://imagicle.acme.com) through a web browser
- once the user is connected, he/she has to enter his/her email address and click on "continue"



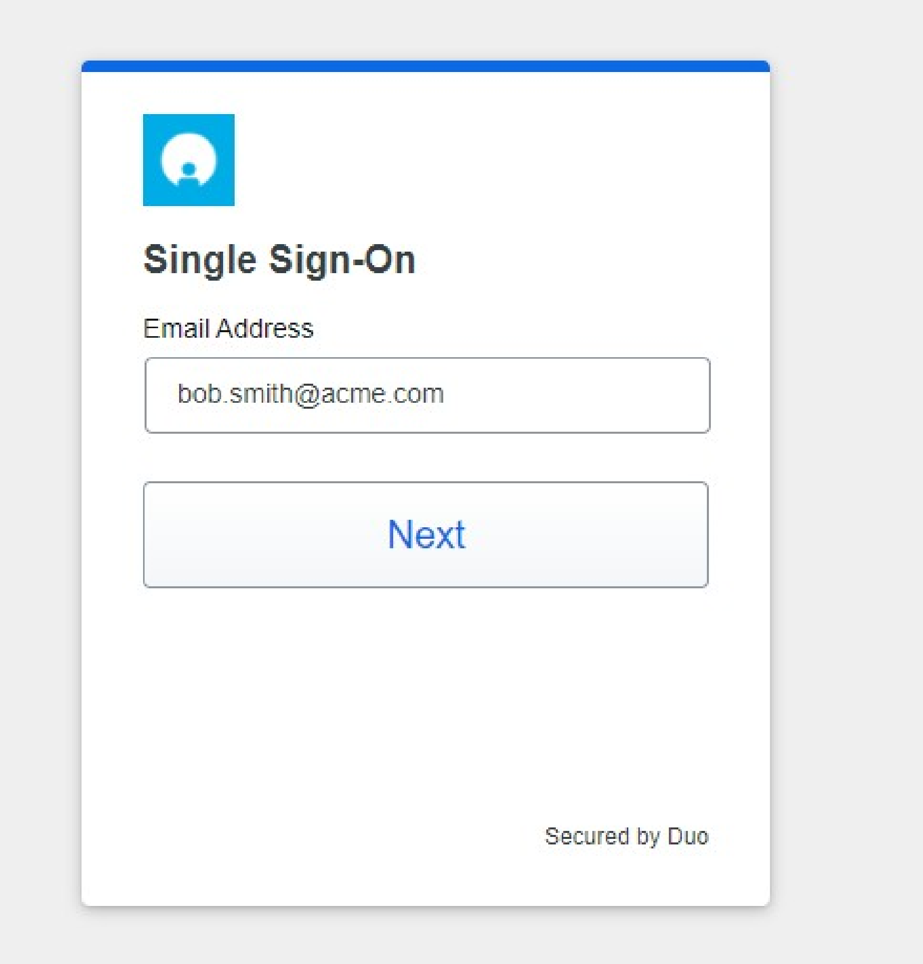
bob.smith@acme.com

- Imagicle UCS, based on user configuration, is able to understand SSO is enabled for this user and manage the login in a different way
- login request is sent to the Imagicle Cloud, where there must be an entry related to the customer's domain (e.g., acme.com). This entry contains the information about the SSO login method for this specific domain
- Imagicle Cloud returns these information to the UCS that in turn returns them to the browser
- at this point, the browser is redirected to a web page where the user can select the IdP (here, most likely, there is only one IdP). In the screenshot below, there is only Cisco DUO



Sign in with your corporate ID

- once the user selects the corporate IdP he/she wants to use, the browser will do another redirection to the IdP web page. Here, the user can do the login leveraging the corporate credentials and authentication method (e.g., 2FA)

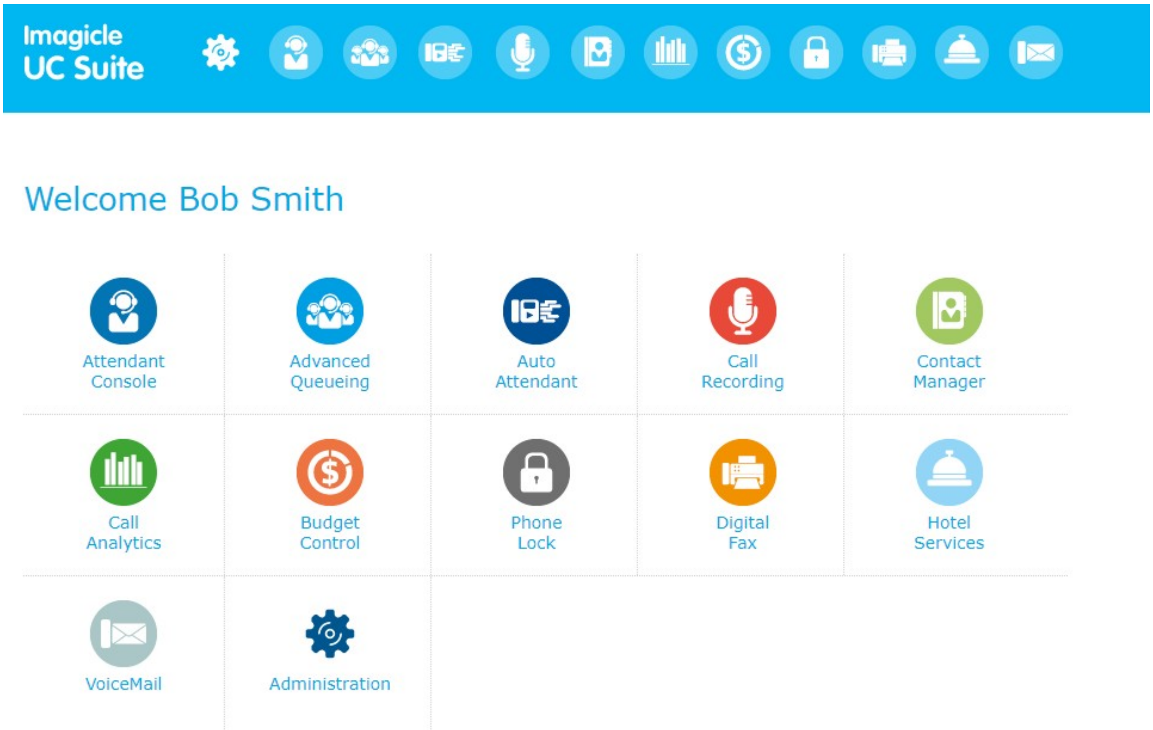


Single Sign-On

Email Address

bob.smith@acme.com

- once the user completed the login procedure on the corporate IdP, the browser is redirected again to the Imagicle Cloud, where there is a check about the IdP response and a new code generation
- this code is sent back to the browser along with the FQDN of the UCS
- browser forwards the code to the UCS that in turn forwards it to the Imagicle Cloud
- Imagicle Cloud replies to the UCS with a token if all the checks are ok
- at this point, the UCS can grant the access to the user



SSO Logout

Starting from 2022.Summer.1, each Imagicle app leveraging SSO supports automatic SSO session logout, at the same time of app/web portal logout.