

SwipeSense

Single Sign-On Technical Setup

# PURPOSE

The purpose of this document is to assist in detailing the technical requirements needed by a hospital to configure Single Sign-On **(SSO)** Authentication.

The following information is meant to identify stakeholders necessary for configuring the integration, provide an overview of the solution, give steps for SSO implementation, and name SwipeSense resources available for further support.

# STAKEHOLDERS

**Network Identity Access Management/IAM Contact SwipeSense Team**

# OVERVIEW

Single Sign-On is a centralized authentication service. It allows users to leverage previously provided login credentials to access the SwipeSense Application. All user authentications can then be controlled by the hospital IT teams for a safer, more secure experience.

Our solution will connect the client’s Identity Provider **(IdP)** to SwipeSense Admin Portal by integrating with a third-party service called, “WorkOS”. WorkOS requires minimal set up and uses industry-standard encryption at rest & in transit. Once configured, there is no further intervention needed from the client unless there are changes to the IdP that will need to be relayed.

# TECHNICAL SET UP PROCESS

1. **SwipeSense** initiates the set up by creating the organization in WorkOS
   1. A placeholder domain name will be used by **SwipeSense** during the initial stages of setup. The network domain will be added when both parties are ready to bring the SSO solution online.
2. **SwipeSense** will generate a unique ‘Setup Link’ and provide this to the **Network IAM Contact**.
   1. This link has a unique authentication key. If it is being shared internally, the entire link will need to be shared to provide access to the authenticated Set-Up Session.
3. **Network IAM Contact** clicks the link to initiate set-up, chooses their IdP from the provided list and clicks ‘Get Started’ at the bottom of the page.
4. **Network IAM Contact** follows the instructions as laid out by the WorkOS interface.



* 1. Because of the wide range of options available for IdP configuration, the SwipeSense team defers to WorkOS for any steps pertaining to this section of the technical set up process. If there are obstacles that cannot be resolved within the WorkOS interface, please reach out to the SwipeSense team.

1. Once IdP configuration is complete **Network IAM Contact** should contact **SwipeSense**

to let them know that the configuration is active.

1. **SwipeSense** will then review the connection and bring SSO online by adding the network domain to the WorkOS configuration.

# ADDITIONAL NOTES

* It can take up to 24 hours for WorkOS to fully ingest user data necessary to activate single sign-on.
* Please make sure to advise your SwipeSense representative as soon as the connection is activated in WorkOS, so that our team can finalize configuration and minimize any possible downtime for user accounts.
* Only users that have been granted active permissions within the SwipeSense Platform will have the ability to login regardless of domain recognition.

# ACRONYMS, DEFINITIONS & RESOURCES

* **SSO**: Single Sign-On.
* **IdP**: Identity Provider – Used for storing and managing users’ digital identities. Used in conjunction with **SSO** to authenticate users.
* **IAM:** Identity Access Management
* **WorkOS**: An Application Programming Interface **(API)** platform that links Facility Identity Provider’s to SwipeSense Platform and authenticates their user base.
  + <https://workos.com/about>
  + Industry-standard encryption protocols

§ AES-256 at rest

§ HTTPS/TLS in transit