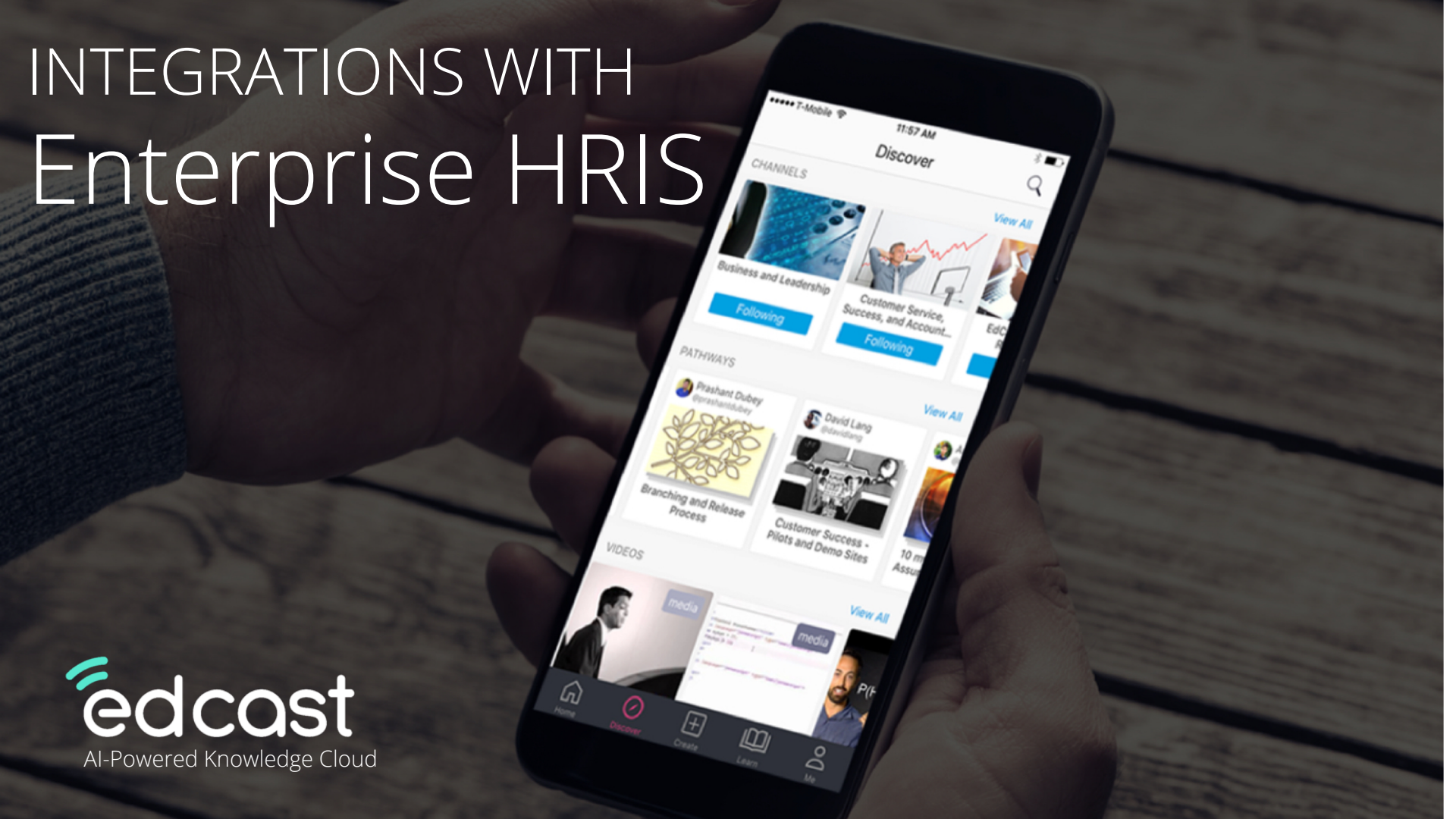
INTEGRATIONS WITH Enterprise HRIS



edcast

AI-Powered Knowledge Cloud

Enterprise HRIS Integration

- Typically, HRIS Integrations with EdCast comprise of these three aspects:
  - Employee Profile Modelling
    - Setting up a Typical User Profile on LXP
  - Employee Data Synchronization
    - Groups, Users, Managers, Custom Attributes etc
  - SSO Integration
    - SAML, OAuth, OpenID Connect

Employee Profile Modeling

Employee Profile Modeling - Mandatory Attributes

- The LXP can work with the most minimal amount of employee information - only the following attributes are mandatory
  - Email
  - First Name
  - Last Name
- A consistent user account can be created using these mandatory attributes

Employee Profile Modeling - Custom Attributes

- LXP User Account can be enriched to pass some additional information from the customer's HR record such as:
  - Employee ID
  - Business Unit
  - Functional Manager
- Custom attributes can be populated using any of our integration modes from the HR record of the Employee

Employee Data Synchronization

HRIS – Modes of Employee Data Synchronization

- For all HRIS Integrations EdCast synchronizes the user's data from the customer's HR system into the LXP
  - It is a unidirectional Integration
- There are four modes of Integration
  - Mode #1 - Pre-Built connectors – Workday, SuccessFactors etc
  - Mode #2 - SFTP based integration
  - Mode #3 - Push Integration - Customer pushes data through EdCast APIs
  - Mode #4 - Pull Integration - EdCast pulls data from the HRIS APIs

Data Integration – Mode #1 – Pre-Built Connectors

- Workday
- SuccessFactors

WorkDay Connector

- Supports adding/updating users
- Supports adding/updating custom attributes
- Supports synchronizing user states
- Fetches all the user data on day one and then fetches the delta from second day onwards
- WorkDay connector runs once in every 24 hours

WorkDay Connector - Things to note

- Doesn’t support fetching profile images
- Doesn’t support fetching and mapping the manager details

Workday Connector - Configuration Parameters

Name	Description	Sample Value
API Endpoint	API Endpoint of Workday	http://acme.sumtotal.host
API Version	API version used to fetch users data from workday current 32.1	32.1
Username	Username to access Workday API's	admin
Encoded Password	Base64 Encoded password to access workday API's	asdasfdsadas===
Tenant	Name of tenant given by workday	acme_corp
Global Unique ID	Unique ID that represents the user (only if SSO is enabled)	acme_id

WorkDay Integration Process (Internal)

1. Customer IT administrator share the WorkDay configuration parameters(From slide#7) with EdCast customer support team

2. EdCast support team will configure WorkDay job in https://hrms-prod.edcast.io
    - Create HRMS Source with customer provided values

WorkDay HRMS Source (Internal)

Name	Description	Sample Value
Name	Name of the WorkDay Source	Workday Acme SB

source_config	Configuration parameters for the WorkDay connector	{
		"api_version": "v32.1",
		"username": "ISU_Edcast_01",
		"encoded_password": "RWRjYXN0MDEhd2Q=",
		"tenant": "acme",
		"workday_end_point": "https://wd5-services1.myworkday.com/ccx/service/acme/Human_Resources"
		}

optional_config	Optional configuration parameters for the WorkDay connector	{
		"sso_enabled": "true",
		"external_identifier_key": "acme_id",
		"contingent_workers_enabled": true
		}

WorkDay HRMS Source (Internal)

Name	Description	Sample Value
Field Mapping	Map the EdCast LXP schema to customer's WorkDay schema	{ "first_name": { "external_key": "worker_data_data_first_name" }, "last_name": { "external_key": "worker_data_last_name" }}
Organization	Organization of the customer deployment	1908
is_enabled	The option enables the WorkDay connector	Yes

SuccessFactors Connector

- Supports adding/updating users
- Supports adding/updating custom attributes
- Supports synchronizing user states
- Fetches all the user data on day one and then fetches the delta from second day onwards
- SuccessFactors connector runs once in every 24 hours

SuccessFactors Connector - Things to note

- Doesn’t support fetching profile images
- Doesn’t support fetching and mapping the manager details

SuccessFactors Connector - Configuration Parameters

Name	Description	Sample Value
Host URL	Host URL used to fetch users data from SuccessFactor API	http://acme.sumtotal.host
Client ID	Client ID given by SuccessFactor	32.1
User ID	User ID given by SuccessFactor	admin
Company ID	Company ID_id given by SuccessFactor	asdasfdsadas===
Private Key	Private Key given by SuccessFactor	acme_corp
Global Unique ID	Unique ID that represents the user (only if SSO is enabled)	acme_id

SuccessFactors Integration Process (Internal)

1. Customer IT administrator share the SuccessFactors configuration parameters(From slide#7) with EdCast customer support team

2. EdCast support team will configure SuccessFactors job in https://hrms-prod.edcast.io
    - Create HRMS Source with customer provided values

SuccessFactors HRMS Source (Internal)

Name	Description	Sample Value
Name	Name of the SuccessFactors Source	SuccessFactors Acme SB
source_config	Configuration parameters for the SuccessFactors connector	{ "host_url": "https://api4.successfactors.com", "client_id": "NGUyZjasdasVjZDQzZjYzNWNjMmRmOTZhNDBiZmZiZA", "user_id": "SFAPI_EDCAST", "company_id": "acmeP", "private_key": "" }
optional_config	Optional configuration parameters for the SuccessFactors connector	{ "sso_enabled": "true", "external_identifier_key": "acme_id"}

SuccessFactors HRMS Source (Internal)

Name	Description	Sample Value
Field Mapping	Map the EdCast LXP schema to customer's SuccessFactors schema	{ "first_name": { "external_key": "worker_data_data_first_name" }, "last_name": { "external_key": "worker_data_last_name" }}
Organization	Organization of the customer deployment	1908
is_enabled	The option enables the SuccessFactors connector	Yes

Employee Data Sync – Mode #2 – SFTP Based

- Customer uploads CSV file to EdCast SFTP folder
  - CSV files need to be encrypted using EdCast Public Key (using PGP encryption)
  - Sample CSV file : https://s3.amazonaws.com/ed-general/bulk_import_sample.csv
  - File with all records on initial launch followed by new or changed (delta) records daily
- Customer is in control of the users that will be added on to the LXP
- EdCast platform processes these files on a daily basis

Employee Data Sync – Mode #3 – Push Integration

- https://documenter.getpostman.com/view/1465156/RW8FERBE?version=latest
- Customer uses Developer API to create/update users/groups
- Customer is in control of the users that will be added on to the LXP
- Real time create/update

Employee Data Sync – Mode #4 – Pull Integrations

- Customer to provide 2 API's
  - API which provides list of all users along with their attributes
    - First Name, Last Name, Email are mandatory
  - API which provides the delta of users (added/deleted) for a given time range

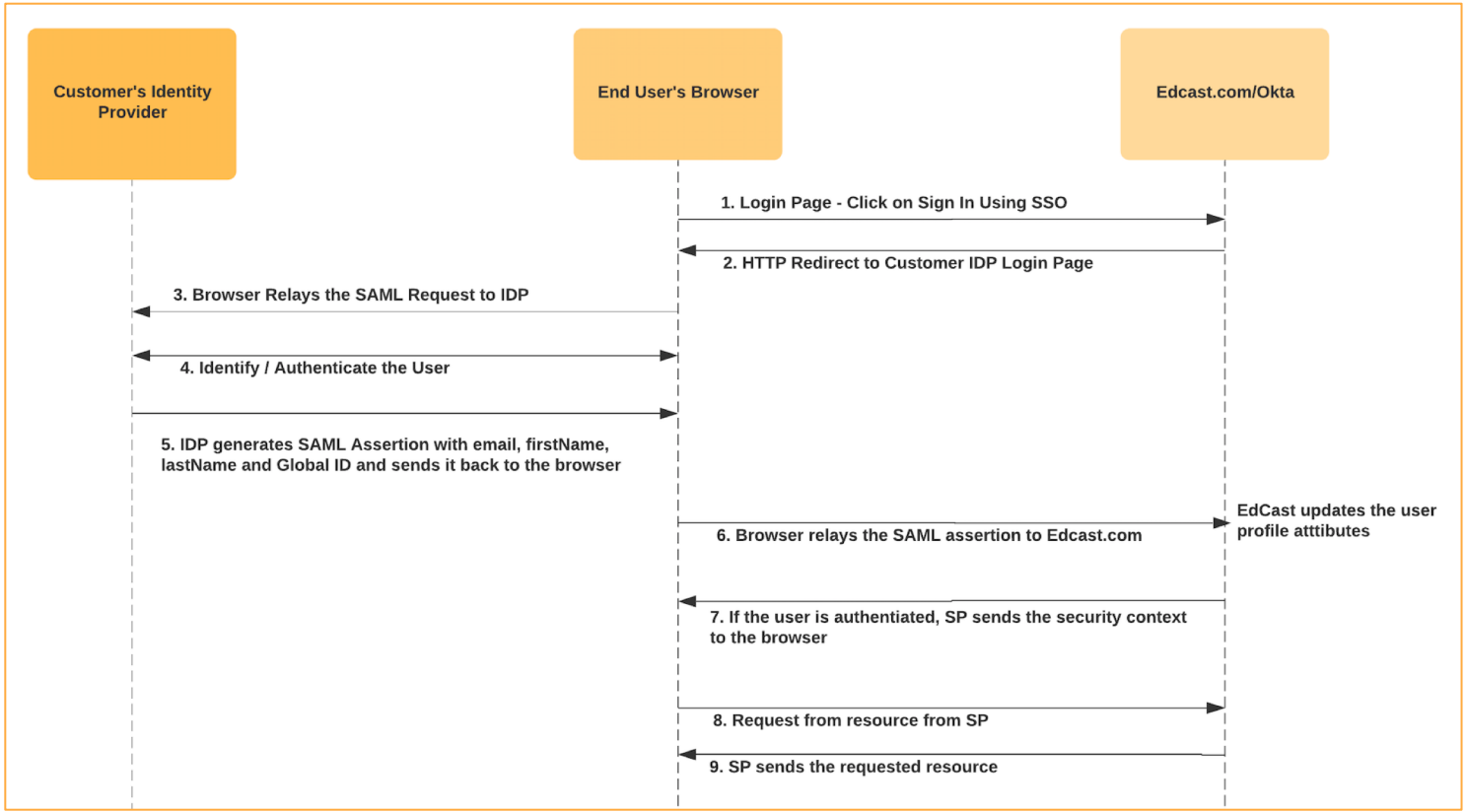
SSO Integration

SSO Integration

- EdCast supports two types of SSO integrations
  - Integration with Customers Identity Provider
  - Integration with Content providers

SSO integration with Customer’s Identity Provider (SP Initiated SSO Flow)

SSO Authentication through SAML (SP Initiated)



SSO Integration Process

1. EdCast Support team creates basic Identity Provider profile for the customer and share below artifacts with customer
    - Service Provider Metadata file
    - ACS URL
    - Entity ID

2. Customer's IT administrator creates the Service Provider profile in their Identity Provider software and share below artifacts with EdCast Support team
    - Identity Provider Metadata file
    - Single Sign On URL

3. Customer's IT administrator also updates their Identity Provider software and send SAML assertion with firstName, lastName, email and globally unique identifier (like employee ID) as subjectNameID

4. EdCast Support team updates the customer's Identity Provider profile with right customer supplied information from step #3

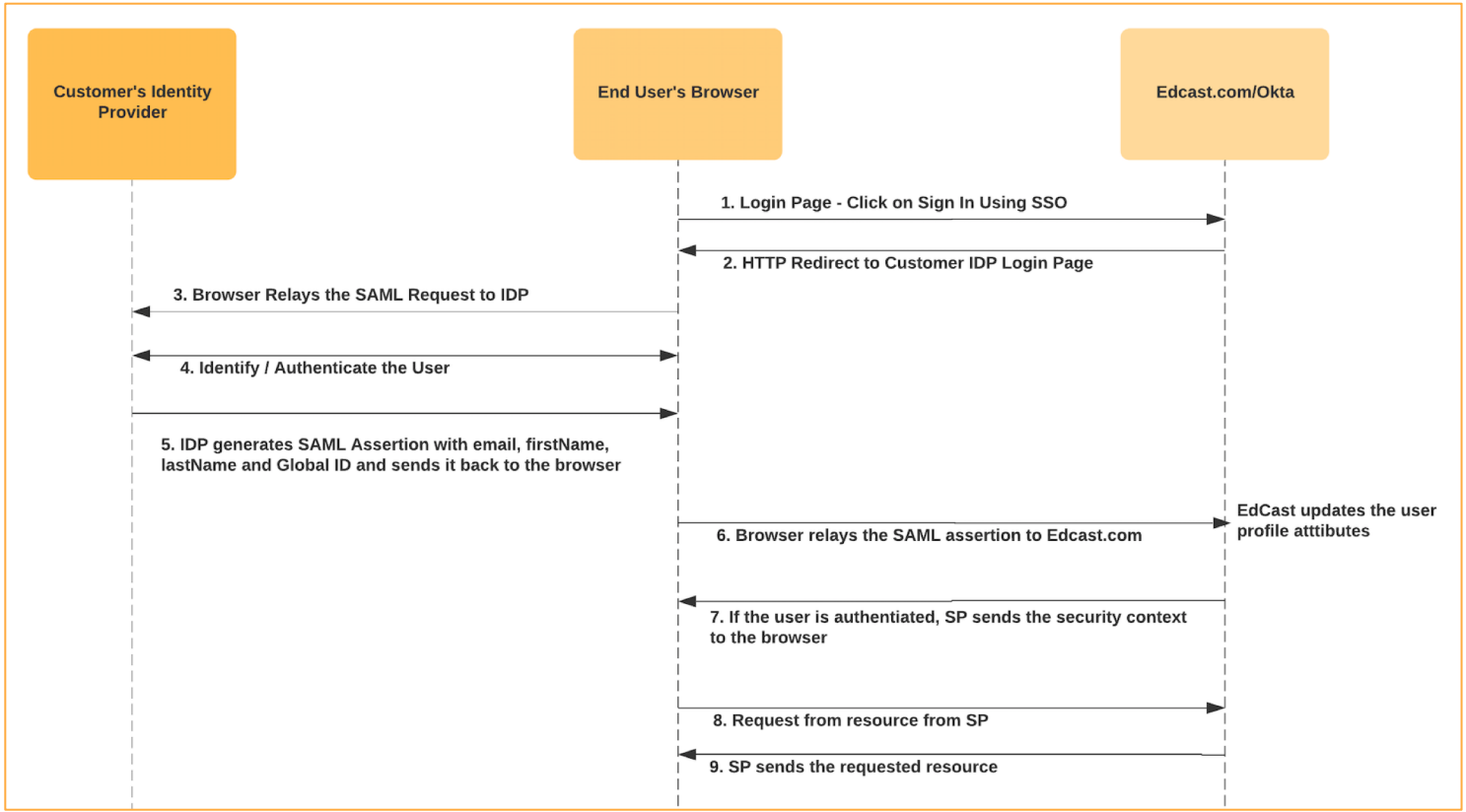
SSO Integration Process (Internal)

1. Note down the IDP Id from the customer's Identity Provider profile
2. EdCast Support team creates OKTA API token for the customer from OKTA Admin Console->Security->API ->Tokens (Make sure to copy the token offline)
3. Enable OKTA for this customer using below steps
    - Go to organization specific settings page in LXP Super Admin Console
    - Go to OKTA tab and Enable OKTA
    - Update OKTA domain (Production - https://edcast.okta.com and SandBox- https://edcast.oktapreview.com)
    - Update the API Token with value from Step#2
    - Enable SAML checkbox and update the IDP value with the value from Step#1
4. Go to Customer's LXP Admin Settings page and enable SAML (Admin->Settings->Login Page Settings-> Okta saml)

For more detailed information, visit https://confluence.edcastcloud.com/display/EP/EP+-+SSO+with+Okta

SSO integration with Content Provider (IDP Initiated SSO Flow)

SSO Authentication through SAML (IDP Initiated)



SSO Integration Process

1. EdCast Support team creates basic SAML 2.0 application for the content provider application (OKTA Admin Console-> Applications->Add Application->Create New App) and share below artifacts with the provider
    - Identity Provider Single Sign-On URL
    - Identity Provider Issuer
    - EdCast public key certificate

2. Content providers IT administrator use the above information and configure their SAML integration and share below artifacts with EdCast Support team
    - Single Sign On URL
    - Service Provider Entity ID (Audience URI)
    - Required Attributes in SAML assertion

3. EdCast Support team updates the content providers application with right customer supplied information from step #3

4. EdCast Support team to assign the customers group to SAML application created in Step#1