One Identity (OneLogin) Deployment Gold Service

Description

This Service Description describes the implementation tasks to be performed by One Identity's professional services team. This Service Description is governed by the terms set forth in the Service Subscription Agreement ("**Agreement**") currently in effect between One Identity, Inc. ("**One Identity**") and the purchasing subscriber ("**Subscriber**"). Capitalized terms not defined herein have their meaning in the Agreement.

During this engagement ("**Implementation**"), One Identity will work with the Subscriber team to assist with the initial configuration of One Identity Services through a series of joint configuration and training sessions.

The Implementation will assist Customer with the installation, configuration, and testing of the One Identity, in the following phases:

- **Engagement Leadership**: One Identity will provide prescriptive guidance and project planning leadership for the duration of the Implementation
- **Configuration/Rollout**: At the end of the implementation, One Identity will provide the platform configuration documentation as mutually agreed upon with the subscriber.

Outcomes

Directory Deployment Plan: One Identity will provide guidance and configuration support for two (2) directories

Windows Domain Authentication (WDA): One Identity will provide confutation and setup support for one (1) WDA configuration through the capabilities provided by the Active Directory Connector (ADC)

App Configuration/Rollout: One Identity will provide configuration and setup support for no more than five (5) applications within the Subscriber's One Identity environment. This is inclusive

of all applications, including any provisioning capable applications.

User Management/Provisioning: One Identity will provide configuration and setup support for three (3) provisioning capable application

Multifactor Authentication (MFA): One Identity will provide configuration and setup support for one (1) MFA device and associated rules for user assignment of the selected MFA device.

Policies: One Identity will provide configuration and setup support for one (1) security policy

Sandbox/Test Configuration: One Identity will make available configuration and setup support for one (1) sandbox environment, if applicable environment has been purchased

Custom Connectors: One Identity together with the Customer, will create up to two (2) forms based (non SAML) connectors

Approach and Activities

A One Identity Implementation consultant will work with the necessary customer stakeholders and subject matter experts to analyze and document the performance of your One Identity implementation. The activities performed may vary based on the complexity of the customer's environment and technical needs.

Discovery Phase

One Identity will host a planning session with the customer to verify environment readiness and establish the use cases and requirements.

Project Deliverables Discovery Phase	Description
Project Initiation and kick-off meeting	Host in project initiation and kick off meeting lasting no more than 1 hour.
Discovery Workshop	Conduct a maximum of one (1) discovery workshop last no more than 8 hours to include the following: • Review of business and technical requirements in alignment with the assumptions below

	• Review of environment requirements including, Servers for Development, Test and Production • Overview of One Identity capabilities • Overview of support portal for Customer • Overview of training packages available

Design Phase

One Identity will work with the customer to establish the base design architecture

Project Deliverables Design Phase	Description
Configuration Workshop	Conduct a configuration workshop with Target System and Human Resources representatives lasting no more than 8 hours.
Design Workshop	Conduct a maximum of one (1) design workshop last no more than 1 hour to include the following: • Review Target Applications • Review directory source for users

Design Document	The design document consists of but not limited to:
	• Project Scope Definition
	• Solution Overview
	• Architecture Design
	  ○ Communication Design
	  ○ Service Accounts and Permissions
	• Use Cases and Requirements

	• Applications included

Development Phase

One Identity will provide assistance to the customer with configuring two Directory sources and five (5) applications in accordance with the design architecture identified in the Design Document created during the design phase.

Project Deliverables Development Phase	Description
Configure two (2) One Identity directory	Configuration of a single Authoritative Source using .CSV, Active Directory, LDAP, BambooHR, Namely or Google
User Acceptance Test	Perform authentication testing Perform self-service password reset if applicable
Configure Applications in One Identity	One Identity will provide configuration and setup support for no more than five (5) applications within the Subscriber's One Identity environment. This is inclusive of all applications, including any provisioning capable applications.
Creation of Production Documentation	One Identity will create documentation detailing the installation in the production environment

Delivery Phase

One Identity will provide guidance to the customer by performing a knowledge transfer of the installation, components and services implemented into the customer's environment throughout the course of the engagement.

Project Deliverables Delivery Phase	Description
Knowledge Transfer	Conduct a maximum of one (1) knowledge transfer session last no more than 1 hour to include the following: • Review Target System implementation • Review System integrations and Architecture • Review processes, code, schedules, and data flow.

Prerequisites and Assumptions

Customer agrees to cooperate with One Login in its delivery of the Services. Customer agrees to the following prerequisites and responsibilities:

- Subscriber will provide an executive sponsor and a project manager to partner with One Identity to ensure the successful and timely completion of the Implementation
- Customer will provide adequate and appropriate access to servers, systems and data
- All pre-requisites to be completed by the customer are completed before the commencement of the project.
- Appropriate access will be granted or a suitable resource with appropriate permissions will be allocated to the work with the One Identity Services team
- Customer will identify a single point of contact to ensure that all tasks are completed within the specified time.
- Customer must commit the appropriate technical resource(s) as required to provide the consultant with the assistance required to complete the activities and deliverables listed above.
- Customer is responsible for providing and defining the internal processes related to the use cases.
- Customer is responsible for execution and preparation of Test Plan used during UAT phase.
- The activities will be performed remotely between 8 a.m.—5 p.m., local time, Monday through Friday, excluding holidays

Limitations

This offering does not include:

- Configuration of reporting
- Workday and UltiPro (UKG) Directory Integrations are not available as a directory choice in the implementation
- Setup or configuration of Trusted Identity Provider (TIDP) capabilities
- Setup or configuration of Proxy Agent components
- Setup or configuration of vLDAP components
- Setup of configuration of One Identity Desktop components
- Setup or configuration of Self Registration workflow
- Setup or configuration of custom SAML connectors
- Creation of custom reports
- Setup or configuration of API interactions or embedded API functionality
- Selected apps for the implementation services must exist in the current One Identity Application catalog
- Setup or configuration of forms based Custom Connectors are subject to target system capabilities
- Deployments utilizing "External Users" concept
- Configuration or troubleshooting of applications, software or hardware not provided by One Identity
- Setup or configuration of directory provisioning to Active Directory of LDAP
- Setup or configuration of for SharePoint or claims provider (people picker)
- Setup or configuration of any One Identity Access integrations
- Customization of WebPortal, Approval or Attestation workflows, Fulfillment workflow, Roles, SOD and Compliance policies

SKU

PS-GOLD	ONELOGIN DEPLOYMENT GOLD PACK PROFESSIONAL SERVICES	Pre-Paid