

One Identity Manager On Demand Foundation Service Package

Description

Establish and implement a strong Identity Manager foundation in as little as six weeks with the Identity Manager SaaS Foundation Services Package. Offered through One Identity Services (OIS), you get expert, guided assistance every step of the way to implement your Identity Manager solution quickly, effectively, and efficiently.

The Identity Manager SaaS Foundation Services Package establishes core functionality to deliver an immediate value to your organization. Once implemented, the OIS team helps build your internal skillset while implementing best practices so that you can keep your systems running optimally.

The service offering will assist Customer with the installation, configuration, and testing of the One Identity Manager software, in the following phases:

- **Discover:** verify prerequisites in order to determine specific program requirements
- **Design:** create design document and work with customer to setup all appropriate access and accounts
- **Development:** Configure software and components to Customer environment
- **Deployment:** verify functionality of software and perform code migration
- **Delivery:** documentation and final knowledge transfer to review the systems in place

Each phase will result in the creation of the Project Deliverables listed below.

Outcomes

The One Identity Manager SaaS Foundations Package is designed to provide automated provisioning from an authoritative source with lifecycle management of identities to a Target System. Authoritative Source can be integrated using one of the following methods (limited to one (1) instance):

- CSV, ODBC, LDAP, or Starling (native) HR Connector

Target System considered for this offer is limited to one (1) of the following system with a maximum of one (1) domain/tenant:

- Active Directory, LDAP, or Azure Active Directory

Approach and Activities

A One Identity Services consultant will work with the necessary customer stakeholders and subject matter experts to analyze and document the performance of your Identity Manager 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 2 hour.
Discovery Workshop	Conduct a maximum of one (1) discovery workshop last no more than 8 hours to include the following: <ul style="list-style-type: none"> • Review of business and technical requirements in alignment with the assumptions below • Review of environment requirements including, Network and Servers for Development, Test and Production • Overview of Identity Manager capabilities • Overview of support portal for Customer • Overview of training packages available • Document requirements and use cases limited to Join, Move, and Leave

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	<p>Conduct a maximum of one (1) design workshop last no more than 8 hours to include the following:</p> <ul style="list-style-type: none"> • Review Target System implementation • Design System Requirements and Architecture (Server, service accounts rights, Change Control) •
Design Document	<p>The design document consists of but not limited to:</p> <ul style="list-style-type: none"> • Project Scope Definition • Solution Overview • Architecture Design <ul style="list-style-type: none"> ○ Communication Design ○ Components Placement Architecture ○ Service Accounts and Permissions • Use Cases and Requirements • Data Flow and Mappings

Development Phase

One Identity will provide assistance to the customer with configuring at least one Authoritative Source and one Domain/Tenant in accordance with the design architecture identified in the Design Document created during the design phase. In addition to the Project Deliverables listed below, the Development Phase will also include a maximum of five (5) Days of user acceptance testing (UAT) support and two (2) Days support during the production rollout.

Project Deliverables Development Phase	Description
Configure Identity Manager in Pre-prod environment	Configuration of a single Authoritative Source using .CSV, ODBC, LDAP, or Starling out-of-the-box HR connector

	<p>Configuration of Target System in a single domain or tenant using the OOTB connector</p> <p>Configuration of Use Cases for Join, Move, and Leave</p> <p>Configuration of IT Shop with customer branding only</p>
Unit Test and Code Migration Preparation	<p>System Integration Test</p> <p>Perform code migration</p>
User Acceptance Test	<p>Maximum of five (5) days of user acceptance testing (UAT) support included</p>
Configure Identity Manager in Production	<p>Import of configuration and configuration of environment specific parameters in conformance with the specifications in the Design Document.</p>
Creation of Production Documentation	<p>One Identity will create documentation detailing the installation in the production environment</p>

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	<p>Conduct a maximum of one (1) knowledge transfer session lasting no more than 8 hours to include the following:</p> <ul style="list-style-type: none"> • 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 Identity in its delivery of the Services. Customer agrees to the following prerequisites and responsibilities:

- Customer must have less than 10,000 Managed Identities
- The Services will address only one (1) authoritative source
- The Services will address only one (1) Active Directory, LDAP domain, or Azure Active Directory Tenant
- AD, LDAP, and AAD Directories contains a single attribute to correlate with the authoritative source
- 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
- Customization of WebPortal, Approval or Attestation workflows, Fulfillment workflow, Roles, SOD and Compliance policies

SKU

OSF-VOL-CO	ONE IDENTITY MANAGER ON DEMAND FOUNDATION SERVICE PACKAGE	Pre-Paid
------------	---	----------