One Identity Manager On-Demand Bronze Plus Enablement Package

Overview

The Identity Manager On-Demand Bronze Plus enablement package is the base implementation and configuration package of our One Identity Manager On-Demand solution. While the entire base license software solution is installed and all base level features are available, many of these features will require configuration with Customer specific information and parameters.

The Bronze Plus enablement package includes setup and configuration by One Identity Professional Services for a predefined set of features and use cases.

The basic Bronze Plus package includes the In-Scope services listed below.

Additional functionality is available for purchase with the One Identity Manager Silver and Gold Packages.

In-Scope Services

The Bronze Plus enablement package includes the following:

- Initial configuration of One Identity Manager in the One Identity Manager On-Demand Dev/Test environment
- Basic birthright provisioning and deprovisioning of user accounts and entitlements for managed target systems based on information from one authoritative data source such as an HR system, subject to the conditions below:
- Authoritative Data Sources for people information include single file or table data source containing employee adds, changes, or delete (or disable) transactions
- Valid data sources include CSV file, Database table or view, Workday HR, SuccessFactors HR, or Dayforce
- Managed Target systems include the following:
    - Active Directory (maximum 1 domain) includes the creation, update and deletion (or disable) of Accounts, and Active Directory Group Memberships
    - Azure Active Directory (maximum 1 domain) includes the ability to update and delete (or disable) accounts and group memberships (this feature requires the Customer previously configuring Azure AD Connect for the creation of accounts. After the initial account is created by Azure AD Connect, One Identity Manager will connect to sync accounts, groups and group memberships from Azure AD to One Identity Manager, which will allow One Identity Manager to perform account and group membership changes to Azure and M365
    - M365 (1 instance) includes the ability to manage licenses and group memberships after the account is created by Azure AD Connect
- Configuration of policies and rules for controlling the following:
    - Configuration of Account and E-mail address structure and rules
    - Active Directory Organizational Unit assignments
    - Birthright rules for Account creation and update rules in target systems based on active persons in the authoritative data source

    - Account deprovisioning rules based on person inactive status from authoritative data source
    - Birthright Active Directory and Azure Active Directory Group membership assignments
    - Creation of Department, Cost Center or Locality records (if exists in Authoritative source file)
    - Linking person identity records to person's Manager (if Manager present in Authoritative source)
- One Identity Manager History Database will be installed and configured with Customer archiving rules
- During Customer testing of the Identity Manager Bronze Plus package in the One Identity Dev/Test Environment, provide up to 24 hours of technical support and remediation of configuration changes to Customers during their User Acceptance Testing of the Use Cases created during in the Bronze Configuration Package
- Prepare the Identity Manager On-Demand Production Environment based on configurations made in the Development Test Environment
- Configure any on-site Job Servers required to support the Identity Manager On Demand Production environment
- Configure Production specific settings in One Identity Manager
- Assist with initial load of data from Authoritative and Target in-scope applications configured with basic Bronze services package
- Provide up to 6 hours of knowledge transfer for product handover and additional product knowledge
- Provide Administration Manual with Customer specific configuration settings
- Provide Implementation Documentation with Customer specific configuration settings

To support the deployment, the One Identity Professional Services will perform the following:

Discovery

- Project Kickoff
- Conduct Workshop and Discovery meetings (up to 16 hours)
- Document In-scope Configuration Requirements on One Identity standard templates
- Develop One Identity Deployment schedule
- Review and approve In-scope Configuration Requirements

Design

- Conduct Use Case definition workshop (up to 8 hours)
- Document Use Cases on One Identity standard templates
- Build out integration connection matrix diagram
- Review and approve design phase documents

Configuration in One Identity On-Demand Dev/Test Environment

- Confirm environment readiness
- Determine and request service accounts needed to access Customer environment
- Setup one on-prem Job Server in Customer's environment

- Setup initial configuration parameters
- Setup SMTP mail server configuration to access Customer's email environment
- Configure Sync Editor to sync data from supported HR Connector (inbound only)
- Configure AD connector (maximum 1 domain) for standard Joiners, Movers and Leavers use cases and reconciliation
- Configure M365 Syncback Connector (maximum 1) and license management
- Configure M365 Joiners, Movers and Leavers use cases for Azure AD group memberships (up to 10 max)
  Perform up to 8 hours of Unit Testing
- Confirm configuration conforms to Functional Requirements and Use Case documents

User Acceptance Testing

- Perform initial sync and data imports of authoritative data source and target systems, and verify readiness to begin testing
- Start User Acceptance testing and provide up to 24 hours of Customer support for Customer testing assistance configuration remediations required based on requirements and use cases documented
- Validate In-scope Configurations Requirements and Use Cases are configured
- Review and signoff testing is complete

Production Standup and Cutover

- Import configurations from One Identity Manager On-Demand Test environment to One Identity Manager On-Demand Production environment
- Configure one Production Environment Job Server in Customer's environment
- Configure environment to access Customer's Production environment data
- Configure Web Servers
- Perform initial synchronization of data from Customer's authoritative data source and target systems
- Determine readiness/go-live and provide up to 16 hours of post go-live support

Project Management Support

Throughout the project, One Identity Professional Services will provide up to 48 hours of project management to perform the following:

- Develop, jointly with Customer, an implementation plan indicating both One Identity and Customer tasks to perform, dependencies and responsibilities
- Ensure the right resources attend the right sessions at the right time and manage overall scheduling
- Produce weekly project implementation reports detailing milestones, risks, controls and other implementation elements
- Coordinate and monitor the tasks performed against the project plan
- Monitor and escalate any support tickets needed

Out of Scope:

- Configuration of Use Cases or Functionality outside of the Use Cases or Functionality described above
- Customizations (e.g. development of any scripting or coding that alters the base out-of-the-box functionality offered by One Identity Manager)
- Changes to Administrative or User Interfaces
- Post implementation technical support of configuration changes
- End User training

Prerequisites, Assumptions and Limitations:

- Customer has purchased the necessary licenses for One Identity Manager On-Demand
- Only Out-of-the-box functionality will be used requiring only configuration
- A pre-engagement checklist of prerequisites and requirements to be completed by Customer will be sent to before deployment services commences. Customer must confirm that prerequisites and requirements are met prior to start of engagement. Failure to complete or meet these prerequisites as well as any prerequisites, conditions, limitations, or assumptions listed herein will result in delays which may mean that the above activities cannot be performed.
- Customer will identify a single point of contact to ensure that all engagement tasks are completed within the specified time
- Customer must commit the appropriate technical resource(s) to assist the One Identity expert as required to complete the activities and deliverables
- Customer will provide adequate and appropriate access to servers, systems and data as required
- Customer is responsible for providing and defining the internal processes related to the use cases
- All services will be provided remotely from One Identity locations
- The activities will be performed remotely between 8 a.m.-5 p.m., local time, Monday through Friday, excluding holidays
- This package will not exceed more than 224 Consulting hours, 24 Architect hours, and 48 Project Management hours by the One Identity Professional Services team
- Use Cases and Success Criteria created during Discovery and Design activities will be used to guide User Acceptance Testing and verification readiness to migrate the solution to the Production environment
- All service activities with One Professional Services are expected to be completed with ten (10) business weeks from the jointly planned start date

Customer Skill Requirements and Guidelines

One Identity recommends the availability and participation of the following Customer personnel to ensure the deployment and integration of One Identity Manager is completed successfully and within the expected deployment timeline listed above.

Customer personnel that may need to be involved with this services package include the following:

- Customer Project Manager
- Technical Architect(s)
- Networking Team (IP addresses/networking/firewalls)

- Application owners and SMEs
- Administrators for the One Identity Manager solution
- Power users (involved in testing and verification)

During Deployment, the following Customer resources are recommended to participate:

- Security and Identity Management administrators – Individuals will have an understanding of the security environment within your organization and will provide input for business processes. The individuals typically become the administrators of the identity solution. It is also expected that after deployment these individuals will perform day to day security administration with the One Identity tools deployed.

  Estimated participation is 75 to 100 hours during deployment, then 15 to 20 hours per week after deployment.

- Network Administrators – Individuals with the knowledge, understanding and the ability to provide information about your networking environment, ensure firewalls are open and VPN connectivity is established in order to connect your environment with One Identity Manager On-Demand

  Estimated participation is 15 to 20 hours during deployment.

- Active Directory and Server administrators – Individuals will be knowledgeable from a technical standpoint of the AD environment and servers they run on.

  Estimated participation is from 25 to 50 hours during deployment, and 5o to 10 hours per week after deployment.

- Applications administrators – Individuals will be knowledgeable from a technical standpoint of the application environment and the servers they run on. During User Acceptance Testing, the individuals will help verify Use Cases are working as expected and validate test results.

  Estimated participation is from 10 to 25 hours during deployment, and 5 to 10 hours per week after deployment.

- Identity Management application technical administrators – These individuals will be responsible for the day-to-day application support and maintenance from a technical standpoint. It is expected that they will be working alongside the One Identity deployment team, participating in the deployment and gaining valuable knowledge transfer in preparation of being able to support Identity Manager once deployed in Production.

Estimated participation will be 15 to 30 hours per week during deployment, and 10 to 15 hours per week after deployment.

Success Criteria

- Successful testing of the documented and agreed upon Requirements and Use Cases prepared
- Production environment is configured with in-scope functionality tested and verified during User Acceptance testing
- Upon completion of services for all In-Scope services performed, Customer will be presented with a Completion Acknowledgement form for signature

Payment/Invoicing

The Bronze Plus package will be invoiced to Customer ninety (90) days from the date of purchase, or at the completion of services (whichever occurs first).

SKU

ABA-VOL-FF ONE IDENTITY MANAGER BRONZE PLUS IMPLEMENTATION PACKAGE