

One Identity Manager On-Demand Gold Plus Enablement Package

Overview

The One Identity Manager On-Demand Gold Plus enablement package builds on top of the automation in the One Identity Manager Bronze and Silver Plus packages and extend the capabilities to integrate with additional applications, perform compliance based real time checking when requesting access to additional systems and perform risk-based analysis, checking and notifications.

Like the Bronze and Silver Plus packages, the Gold Plus package utilizes out-of-the-box functionality and a predefined set of features and use cases to extend the capabilities of One Identity Manager On-Demand.

The Identity Manager On-Demand Gold Plus enablement package includes setup and configuration by One Identity Professional Services for a predefined set of features and use cases.

In-Scope Services

The Gold Plus enablement package includes the following:

- Integration with up to 3 additional applications using one of our standard connectors as listed in the One Identity Manager Release Notes (excludes Epic and SAP R/3) in order to provide full lifecycle management to those systems
- Addition of those applications to the IT Shop Web Portal from which to request additional access to (up to 10 maximum)
- Set up of up to 10 Risk Based Rules and Controls, and up to 5 Segregation of Duties rules and alerts which can be reviewed either on the standard reports and consoles, and optionally be used to control unauthorized or risky access requests
- Provide up to 12 hours of technical support and remediation configuration changes to Customers during their User Acceptance Testing of the Use Cases created during in the Gold Plus package
- Migrate configurations from the Identity Manager On Demand Dev/Test environment to the Identity Manager On-Demand Production Environment
- Perform initial loads of target system data to One Identity Manager
- Update the One Identity Manager Administration Manual with Customer specific configuration settings
- Update the One Identity Manager 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 24 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 16 hours)
- Document Use Cases on One Identity standard templates
- Build out Integration Connection Matrix
- Review and approve design phase documents

Configuration in One Identity On-Demand Dev/Test Environment

- Setup IT Shop Catalogs, Approvals and Requestable Items (up to 10 maximum)
- Setup Segregation of Duties rules (up to 5 maximum)
- Setup Risk Based rules (up to 10 maximum)
- Setup One Identity Manager standard connectors to additional applications (up to 3 maximum)
- Perform up to 8 hours of Unit Testing
- Confirm configuration conforms to Functional Requirements and Use Case documents

User Acceptance Testing

- Perform 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 12 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 Production environment to access Customer's Production environment data
- Perform synchronization of data from Customer's authoritative data source and target systems
- Determine readiness/go-live and provide up to 8 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)
- 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
- Customer has purchased the One Identity Manager On-Demand Bronze and Silver Plus services packages
- Only Out-of-the-box functionality will be used requiring only configuration
- 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 204 Consulting hours, 52 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 25% of the time during 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 5 to 15 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: If needed

- 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 15% during 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

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 Gold 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

ABE-VOL-FF ONE IDENTITY MANAGER GOLD PLUS IMPLEMENTATION ADDON PACKAGE