

Identity Manager on Demand Bronze Plus package

IMOD accelerated deployment service offering description.

ABA-VOL-FF

Provides a scalable operational baseline for business readiness in a short time.

Overview

The **Identity Manager on Demand (IMOD) Bronze Plus package** provides the essential foundation for successful deployment. While the solution grants immediate access to all core features, the Bronze Plus enablement ensures these tools are precisely calibrated to your organization's unique parameters.

Through this package, One Identity Professional Services handles the end-to-end configuration of a predefined suite of high-impact use cases. This ensures your team can hit the ground running with a production-ready environment, while offering a seamless upgrade path to Silver or Gold tiers as your identity governance needs evolve.

The packaged PSO service leverages One Identity's proven methodology (D5), focusing on efficiency, standardization, and rapid knowledge transfer to customer resources.

It delivers a **scalable operational foundation** that includes **core architectural components, baseline functionality, and standard documentation**.

Service delivery is executed remotely and follows a phased approach of the D5 consisting of **Discovery, Design, Develop, Deploy, and Deliver** stages, emphasizing short time-to-value.

Objectives

- **Accelerated time-to-value:** A phased D5 (Discovery, Design, Develop, Deploy, Deliver) delivery model drives a faster path to a production-ready IMOD environment.
- **Production ready from day one:** One Identity Professional Services configures a predefined set of high-impact, standardized use cases end-to-end so your team can operate immediately after go-live.
- **Fit-to-your-organization calibration:** Core IMOD capabilities are not just enabled—they are tuned to your organization's unique parameters to reduce rework and misconfiguration risk.
- **Standardized, repeatable delivery:** Packaged services leverage a proven methodology and predefined scope to improve predictability, reduce variability, and simplify stakeholder alignment.
- **Reduced consulting effort and delivery risk:** Standard use-case implementation and baseline architecture minimize custom work, accelerate decision-making, and lower overall project risk.
- **Scalable operational foundation:** Establishes core architectural components, baseline functionality, and standard documentation to support growth and operational maturity over time.
- **Efficient remote execution:** Delivered remotely to streamline scheduling, reduce travel overhead, and improve speed of execution across distributed teams.
- **Rapid knowledge transfer:** Designed for efficient enablement and knowledge handoff to customer resources, improving self-sufficiency post-deployment.
- **Clear upgrade path:** Provides a seamless transition to Silver/Gold tiers as identity governance requirements expand, preserving prior investment and enabling incremental value.
- **Immediate access to core features—properly implemented:** Customers get access to all core IMOD features while ensuring the foundational configuration is correctly established for long-term success.
- **Audit & Compliance:** Ensure firm alignment with audit and compliance needs.

Scope and Deliverables

The implementation follows a phased delivery approach and includes the essential activities required to expand IMOD functionalities, integrations, and configurations.

Package entitlements (e.g., number of use cases, integrations, authoritative sources) are limited to the quantitative thresholds defined in the Package Scope Table below:

Package Scope Table (Bronze Package):

Category	Deliverable / Item	Bronze Plus Package (IMOD – One Identity Manager)
Environment	IMOD Dev/Test Environment	Initial configuration of One Identity Manager in the IMOD Dev/Test environment.
	IMOD Production Environment	Prepare the IMOD Production environment based on the validated Dev/Test configuration; configure production-specific settings.
	On-premises Job Servers	Install and configure the Job Servers to support Dev/Test and Production environments on-premises.
Identity Source (Authoritative)	Authoritative Data Source (HR)	One (1) authoritative source for people information. Source provides employee add/change/delete (or disable) transactions. Supported source types: Single file or table source: CSV file, Database table/view, Workday HR, SuccessFactors HR, or Dayforce.
Target Systems (Managed)	Active Directory	Active Directory (up to 1 domain): create/update/delete (or disable) accounts and manage AD group memberships (Joiners/movers/leavers).
	Azure Active Directory	Azure AD (up to 1 tenant/domain): update/delete (or disable) accounts and manage group memberships after initial account creation by Azure AD Connect (customer prerequisite). OIM syncs accounts/groups/memberships into OIM to enable changes to Azure and M365.
	Microsoft 365	M365 (1 instance): manage licenses and group memberships after account is created by Azure AD Connect.
Use Cases	Use Cases Creation	Design and configure three use cases based on discovery outcomes: Joiners, Movers, and Leavers (J/M/L).
	Birthright Provisioning	Basic birthright provisioning of user accounts and entitlements for managed target systems based on the authoritative source.
	Deprovisioning	Basic deprovisioning rules based on a person becoming inactive in the authoritative source (disable/delete per target-system capability and policy).
Policies & Rules	Naming & Email Rules	Configure account structure and e-mail address structure/rules.
	AD Placement	Configure Active Directory Organizational Unit (OU) assignment rules.
	Birthright Rules	Configure account creation/update rules for target systems based on “active persons” in the authoritative source.
	Group Membership Birthright	Configure birthright AD and Azure AD group membership assignment rules.
	Org Data (if present)	Configure creation of Department, Cost Center, or Locality records if present in the authoritative source.

	Manager Relationship	Configure linking of a person to their manager if manager information is present in the authoritative source.
Data & History	History Database	Configure the One Identity Manager History Database, including customer archiving rules.
Data Load	Initial Load Assistance	Assist with initial load of data from the authoritative source and in-scope target applications configured under Bronze services.
Validation & Testing	UAT Support	During customer UAT in IMOD Dev/Test, provide up to 24 hours of UAT support and remediation of configuration changes for the implemented use cases to the customer team.
Documentation	Use Cases and Requirements Documentation	Provide a Use-cases and requirements document based on the discovery meetings to support the use cases in the scope (Joiners, movers, and leavers).
	Administration Manual	Provide a standard Administration Manual.
	Implementation Documentation	Provide Implementation Documentation including customer-specific configuration settings.
Knowledge Transfer	Handover & Product Knowledge	Provide up to 8 hours of knowledge transfer for handover and product administration knowledge transfer.
Scope Limits & Dependencies	Quantitative Limits	1 authoritative source; AD max 1 domain; Azure AD max 1 tenant/domain; M365 1 instance; UAT Cycle support 1 cycle up to 40 hours.
	Key Dependency	Azure AD / M365 account creation requires customer to have Azure AD Connect configured (OIM performs updates/changes after initial creation).
	Key Dependency	The Customer must have the business processes and requirements for the three Joiner/Mover/Leaver (JML) use cases documented and finalized before the Discovery phase begins.
	Key Dependency	The Customer is responsible for creating the Test Plan to guide and execute the User Acceptance Testing (UAT). It must be ready by the end of the Development phase.

These limits apply across all project phases and represent the maximum number of configuration items included in the IMOD Bronze Package. Any work beyond these limits requires mutual agreement and will be managed through formal change control. Phase completion and change control are governed by the provisions defined in the General Terms section at the end of this Service Description.

1. Phase – Discovery

The Discovery Phase establishes the foundation for the IMOD implementation by validating customer objectives, confirming requirements and initial scope, assessing the target environment, and capturing the implementation inputs (use cases and integration requirements).

Activities

- Conduct the project kickoff meeting.

- Facilitate an IMOD workshop and conduct discovery sessions with business and technical stakeholders (up to 20 hours).
- Document in-scope configuration requirements using One Identity (OI) standard templates.
- Review and adjust the IMOD deployment project plan.

Deliverables

- IMOD workshop (up to 4 hours).
- Discovery meetings (up to 20 hours).
- Updated Project Plan based on the discovery meetings.

2. Phase - Design

The Design Phase translates the confirmed use-case details into a Use Case and Requirements Document, defining how IMOD will be implemented within the agreed scope.

Activities

- Create the Use Cases and Requirements Document covering the three in-scope use cases and their requirements.
- Conduct the Use Case Review Workshop (up to 4 hours).
- Update the document based on workshop outcomes.
- Submit the document to the customer for review and approval.
- Incorporate customer feedback and finalize the document.
- Accept the Use Cases and Requirements Document (Customer).

Deliverables

- Use Cases and Requirements review Workshop.
- Use Cases and Requirements document.

3. Phase – Development

The Develop Phase configures the IMOD solution in the DEV/TEST environment based on the Use Case and Requirements Document approved in the Design phase.

Activities

- Confirm DEV/TEST environment readiness.

- Configure one on-premises Job Server in the customer's environment.
- Configure initial system parameters.
- Configure SMTP settings to enable email delivery via the customer's mail environment.
- Configure the Sync Editor to enable inbound synchronization from a supported HR connector.
- Configure the Active Directory connector (up to one domain) to support standard Joiners/Movers/Leavers (JML) use cases and reconciliation.
- Configure the Microsoft 365 sync-back connector (up to one) and license management.
- Configure Microsoft 365 (Join, Move, Leave) use cases for Azure AD group membership provisioning (up to 10 groups).
- Perform unit testing to confirm the configuration aligns with the approved Use Case and Requirements documents.

Deliverables

- DEV/TEST environment is operational and available.
- IMOD is configured in accordance with the approved Use Cases and Requirements document.

4. Phase – Deployment

The Deployment phase supports customer validation of the package configuration in the DEV/TEST environment and formal UAT remediation.

Activities

- Execute customer-led validation of the Bronze capabilities in DEV/TEST. (Customer)
- Provide clarification and guidance on in-scope configuration during customer validation.
- Document agreed outcomes and obtain completion acknowledgement for the package scope.

Deliverables

- Package features configured according to the Requirements and Use-case documents and attestation campaigns ready for the UAT in IMOD DEV/TEST environment.
- Support the customer UAT by providing clarification and adjusting any item not in compliance with the Use-case and requirements document.
- Formal customer acceptance.

5. Phase – Delivery

The Deployment phase validates that the configured solution aligns with the approved Use Case and Requirements document by supporting the customer User Acceptance Testing (UAT) and remediating any items that are not compliant with the document.

Activities

- Check the PRODUCTION environment readiness and set up the environment.

- Prepare and move the Transport files from DEV/TEST to the PRODUCTION environment.
- Configure the Production environment and realize the Synchronization (HR and Target systems)
- Execute the **Go-live**.
- Provide postproduction support for the customer (up to 3 days)
- Execute the knowledge transfer Workshop.
- Provide final project acceptance (customer).

Deliverables

- Production environment configured and with the development approved in UAT installed and connected to the HR system and target systems.
- Support the post go-live operation (up to 3 days).
- Administration workshop (up to 16 hours).

Key Benefits

- Give new customers a solid baseline setup so they can adopt IMOD without a lot of upfront effort.
- Use IMOD's out-of-the-box features to deliver value quickly with minimal implementation work.
- Provide tiered packages (Bronze to start, then scale up with Silver and then to Gold).
- Make it clear what's included and what customers should expect from the implementation.
- Let customers start with Bronze and upgrade later to unlock more advanced features in Silver and Gold packages.

Prerequisites and Assumptions

Customer will agree to cooperate with One Identity in the performance of the Services and to meet the following prerequisites and responsibilities:

1. General Terms

- The Customer will designate a single point of contact to coordinate activities and ensure timely completion of required tasks.
- The Customer will provide appropriate technical resource(s) as needed to support One Identity in completing the activities and deliverables described above.
- Services will be delivered remotely during standard business hours (8:00 a.m.–5:00 p.m., Customer local time), Monday through Friday, excluding holidays.
- Unless otherwise agreed in writing, the Services are governed by the terms of the Transaction Services Agreement ("TSA") available at <https://www.oneidentity.com/legal/service-agreements.aspx> as in effect on the date the Customer orders this Service Description. Capitalized terms not defined herein have the meanings set forth in the TSA.

2. Delivery Scope, Phases, and Quantitative Limits

- This Service Description defines the scope, phases, and deliverables for the Services, including quantitative limits (e.g., “up to an”).
- Each phase is deemed complete with Customer acceptance of the deliverables specified for that phase.
- All activities are delivered remotely by design.
- The Customer will develop and provide a UAT Test Plan to be followed during the UAT cycle.
- A cloud-hosted deployment architecture is included within the scope.

3. Design-iterations, UAT-cycles, Reviews, Runbook

- Per package design, one (1) design iteration and one (1) UAT cycle are included in scope; any additional iterations or cycles require mutual written agreement prior to execution.
- The **UAT cycle** is planned to be completed within five (5) consecutive business days. The Customer must confirm that this timeline is feasible. If additional time is required, UAT is on the project’s critical path; therefore, each additional business day will extend the overall project end date by the same amount and must be mutually agreed between Customer and One Identity.
- The OI Team will support the Customer during one (1) UAT cycle, not to exceed forty (40) hours. Any additional UAT support requires an approved change request.
- The **customer business processes** (such as use-cases and business requirements) within the scope of this project to be implemented in the solution must be already defined and established within the company.
- The One Identity team requires **direct remote access** to the DEV/TEST environment (e.g., via VPN or equivalent) to ensure timely project progress.
- **Reviews of the system landscape, user volumes, and connectivity** are based solely on information provided by the Customer during Discovery and exclude modeling of future growth or seasonal/peak scenarios.
- **Runbook content** is limited to core administrative procedures and excludes detailed standard operating procedures (SOPs), training materials, and custom operations manuals.

If any prerequisite or assumption underlying this package is materially inaccurate, or if Customer does not meet these requirements, continuation of the engagement will require mutual agreement on revised scope, timeline, and/or fees.

4. Out-of-Scope Items

- Custom development of new functionality beyond existing out-of-the-box capabilities.
- Configuration or troubleshooting of systems, applications, or tools other than One Identity Manager (IMOD), including Customer-managed infrastructure components outside the IMOD scope.
- Business process design/definition (all in-scope processes must be defined prior to the start of Discovery phase).
- Development of a UAT Test Plan (Customer responsibility).
- Design, execution, or analysis of stress, load, or performance testing.
- Direct execution of tasks in the Production environment; Production activities will be performed by the Customer under One Identity supervision/guidance, as applicable.

- Implementation-related training and formal knowledge transfer beyond the agreed deliverables (e.g., training materials or structured enablement sessions).
-

SKU

ABA-VOL-FF	ONE IDENTITY MANAGER ON DEMAND BRONZE PLUS IMPLEMENTATION	Fixed Price
------------	---	-------------