One Identity Manager v8.1.5

Security Target

Version 1.0

16 December 2021

Prepared for:

One Identity LLC
4 Polaris Way
Aliso Viejo, CA 92656
United States

Prepared by:

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, Maryland 21046

Contents

List of Tables

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is One Identity Manager v8.1.5 provided by One Identity.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 0)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)

1.1 Security Target, TOE and CC Identification

ST Title – One Identity Manager v8.1.5

ST Version – Version 1.0

ST Date – 16 December 2021

TOE Identification – One Identity Manager v8.1.5

TOE Developer – One Identity

Evaluation Sponsor – One Identity

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013, [ESMICM] and including the following optional SFRs: FMT_MTD.1.
- The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

  TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs
  TD0066: Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
  TD0055: Move FTA_TAB.1 to Selection-Based Requirement (not included in ST: Operational Environment component authenticates the administrator)

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Release 4, September 2012
  - Part 2 Extended

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example, FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- The [ESMICM] uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Acronyms

Acronym	Definition
2FA	Two Factor Authentication
AAA	Authentication, Authorization and Accounting
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CM	Configuration Management
ESMICM	Protection Profile for Enterprise Security Management Identity and Credential Management
FIPS	Federal Information Processing Standard
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
LDAP	Lightweight Directory Access Protocol

Acronym	Definition
OAUTH2	Open Authorization
PP	Protection Profile
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
REST	REpresentational State Transfer
SAP	Systems, Applications and Products (Data Management Software)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

1.3.2 Terminology

This section identifies TOE-specific terminology.

Administrator	A TOE user that also has permissions to manage some or all of the TOE's functionality. The ST defines the One Identity Manager administrator as an administrator with full permissions to manage the TSF. However, administrators with a subset of these permissions may also be created based on the permissions granted by the associated application role.
Application Role	A user identity attribute that grants a TOE user administrative privileges on the TOE, making them an administrator. Application roles derive their privileges through association with permissions groups.
Business Role	A user identity attribute that associates the user with an arbitrarily-defined job title. This data may be propagated to other repositories where the user is defined, or it could be used to automatically configure access to environmental resources based on the expected responsibilities that are conferred on the role (e.g. a user with an 'auditor' role may have greater access needs than a user with an 'engineer' role).
Connectors	TOE components that allow the TOE to securely connect with external systems.
Designer	An administrative tool included with the fat client used to perform initial configuration of One Identity Manager. Specifically, the Designer is used to establish the evaluated configuration by enabling security-relevant auditing.

Enterprise User	An enterprise user is a company employee whose accounts are managed by the TOE. All administrators, TOE Users and employees are enterprise users.
External Systems	The organizational repositories (sometimes called Target Systems) that can either be the authoritative source of enterprise user attributes or that can contain user attributes managed by the TOE or both. The external systems are also classified as Enterprise Security Management products.
Fat Client	A One Identity Manager Windows application installed on an administrative workstation primarily used for initial configuration activities. The fat client includes the Designer, Synchronization Editor, and Manager administrative tools.
Organization Data	User identity attribute data that relates to the user's position within an organization. Includes department, cost center, and (geographic) location.
Manager	An administrative tool included with the fat client that is used to manage application roles and password policies. The Manager interacts with the TOE via invocation of the Web Service over HTTPS.
Password Reset Portal	A tool that TOE users can use to reset their own user password. Part of the Web UI.
Permissions Group	Authorizations to manipulate data in the database. Permissions Groups are associated with Application Roles to determine the administrative privileges of users that are assigned those roles.
Synchronization Editor	An administrative tool included with the fat client that is used to perform initial configuration of One Identity Manager. Specifically, the Synchronization Editor is used to define the connectivity and data mapping between the TOE and external systems.
System Role	A grouping of permissions to interact with external systems. Can be assigned directly to a user as an identity attribute or can be inherited through assignment to a business role or organization data.
Target Systems	A term synonymous with External Systems.
TOE User	An enterprise user that can log on to the One Identity Manager in order to reset their own password or to perform delegated administration.
Web Portal	An administrative tool that is used to perform security-relevant management activities of user identity and credential data, password policies, and administrative roles and privileges. Users may also modify their own personal data using this interface. Part of the Web UI.

2 TOE Description

The One Identity Manager v8.1.5 TOE provides centralized provisioning and management of enterprise user accounts based on defined 'identities' and therefore is an Identity and Credential Management product as defined in the [ESMICM].

2.1 TOE Overview

The One Identity Manager v8.1.5 TOE provides centralized provisioning and management of user accounts based on defined 'identities'. The TOE provides identity and credential management functions by serving as the authoritative source for various user attributes while also designating various external systems to be authoritative sources for other attributes. The end result is that user data can be automatically and accurately propagated to multiple organizational locations so that external systems can subsequently make use of this data. For example, One Identity Manager may interface with an organization's HR system (e.g. PeopleSoft) such that when a new user is created by the HR system, One Identity Manager will automatically generate external system accounts for that new user (e.g. create a new AD entry for them based on the default information and/or information supplied by the HR system). One Identity Manager can also be used to manually create user accounts and as an interface for TOE users to perform self-service management of their own password credentials, which are then pushed out to the organizational repositories (external systems) where that password data resides. The external systems that the TOE supports are equivalent to the connectors identified in Section 2.2.1. For example the TOE includes an Active Directory Connector and therefore Active Directory external systems are supported. The TOE provides the ability to manage credential data by providing an interface to change a user's "master password", which is then propagated to any external systems that the TOE is configured to synchronize password data with. The TOE also acts as a central point for password policy enforcement by defining password policies that these passwords must comply with. Note that the administrator must ensure that external systems do not enforce stricter password policies than the TOE or else password synchronization may fail due to contradictory policies.

The TOE provides the One Identity Manager administrator role and TOE user role. Users with the One Identity Manager administrator role have full permissions to create new users, permissions and roles and manage identities. This user has full administrative capabilities to manage the TOE including creating custom role and permissions and associating users with them.

Users with the One Identity Manager administrator role can create new Administrative roles with different levels of permissions and then assign these roles to TOE users for delegated administration. However, a TOE user doesn't have to have admin permissions, they can be just an organizational user who uses the TOE solely to reset their own password.

One Identity Manager supplies employees in a company with company resources, for example, permissions or applications, according to their function. The company structures are represented in hierarchical role form in the One Identity Manager. Employees can obtain their company resources through these roles when they are assigned to roles as members.

In One Identity Manager the following roles (also referred to as role classes) are defined for mapping company structures:

- Organization data (departments, cost centers and locations)

Departments, cost centers and locations are each mapped to their own hierarchy under the heading "Organizations". This is due to their special significance for daily work schedules in many companies. The

TOE can be used to associate accounts and permissions on external systems based on organization data so that all users with this identity attribute are treated uniformly.

- Business roles

Business roles map company structures with similar functionality that exist in addition to departments, cost centers, and locations. This might be project groups, for example. The TOE can be used to associate accounts and permissions on external systems based on business roles so that all users with this identity attribute are treated uniformly.

- Application roles

Application roles are used to grant One Identity Manager object access rights to One Identity Manager users, making them administrators of the TOE for the functions defined by the assigned roles. For more detailed information, see the One Identity Manager Application Roles Administration Guide.

One Identity provides several methods of assigning company resources: Direct Assignment; Indirect Assignment; Assigning through Dynamic Role.

- Direct assignment of company resources results from the assignment of a company resource to an employee, device or a work desk, for example.
- In the case of indirect assignment of company resources, employees, devices and work desks are arranged in departments, cost centers, locations, business roles or application roles. The total of assigned company resources for an employee, device or work desk is calculated from the position within the hierarchies, the direction of inheritance (top-down or bottom-up) and the company resources assigned to these roles. In the Indirect assignment methods, a difference between primary and secondary assignment is taken into account. Secondary assignments are made by classifying an employee, a device or a work desk within a role hierarchy. Secondary assignment is the default method for assigning and inheriting company resources through roles. Secondary assignments are specified on the role classes (department, location, cost center, business roles, application role) and indicate whether a secondary assignment of company resources to employees, device and work desk is possible. Primary assignments are made by referencing a department, cost center or location through a foreign key to the employee, device and work desk objects. A foreign key is a field (or collection of fields) in one table that refers to the foreign key in another table. Input fields are used for roles on the employee, device and work desk master data forms. Primary assignment inheritance can be enabled through configuration parameters. Assignment through dynamic roles is a special case of indirect assignment.
- Dynamic roles can be used to specify role memberships dynamically. Employees, devices and work desks are not permanently assigned to a role, just when they fulfill certain conditions. A check is performed regularly to assess which employees, devices or work desks fulfill these conditions. This means the role memberships change dynamically.
- One Identity also provides the ability to define custom roles and permissions.

One Identity Manager offers different methods for supplying user accounts to employees. One Identity Manager supports the following methods for linking employees and their user accounts.

- Employees can automatically obtain their user accounts through One Identity Manager account definitions.

- When user accounts are inserted in the One Identity Manager, they can be automatically assigned to an existing employee or a new employee can be created if necessary.
- Employee and user account data in the One Identity Manager can be manually entered and assigned to each other.

Typically, the user accounts are initially read into One Identity Manager from a target system or systems through synchronization. One Identity Manager consolidates user account data from all of the various target systems in the TOE. Either the TOE or the external system can be defined as the 'definitive' source of user data. For example, a user's employee ID may be defined in AD and the TOE will keep track of that data but can't be used to change it. Whereas a user's unique ID may be defined in One Identity Manager and the TOE can make changes to this data and push it out to external systems (e.g. Active Directory).

The TOE can create or modify user accounts on external systems based on user identity attributes. In other words the TOE 'manages' identity data in the sense that it can do something to treat the managed users differently based on what their identity attributes say about them. The external systems are sources of the object attribute data required of an ESM access control system. The TOE does not define object attributes and this ST does not include the optional ESM_ATD.1: Object Attribute Definition SFR.

Administrators use the fat client to configure the TOE and the web UI and web service to manage the TOE and create and approve user requests for user entitlement or to add a user to an account or a role with entitlements. All communication with users is through a secure HTTPS channel.

The TOE relies on FIPS 140-2 validated cryptographic modules in the operational environment for cryptographic functions. The cryptographic functions are used for all SSH and TLS connections with trusted external IT entities, and for HTTPS connections with users accessing the TOE.

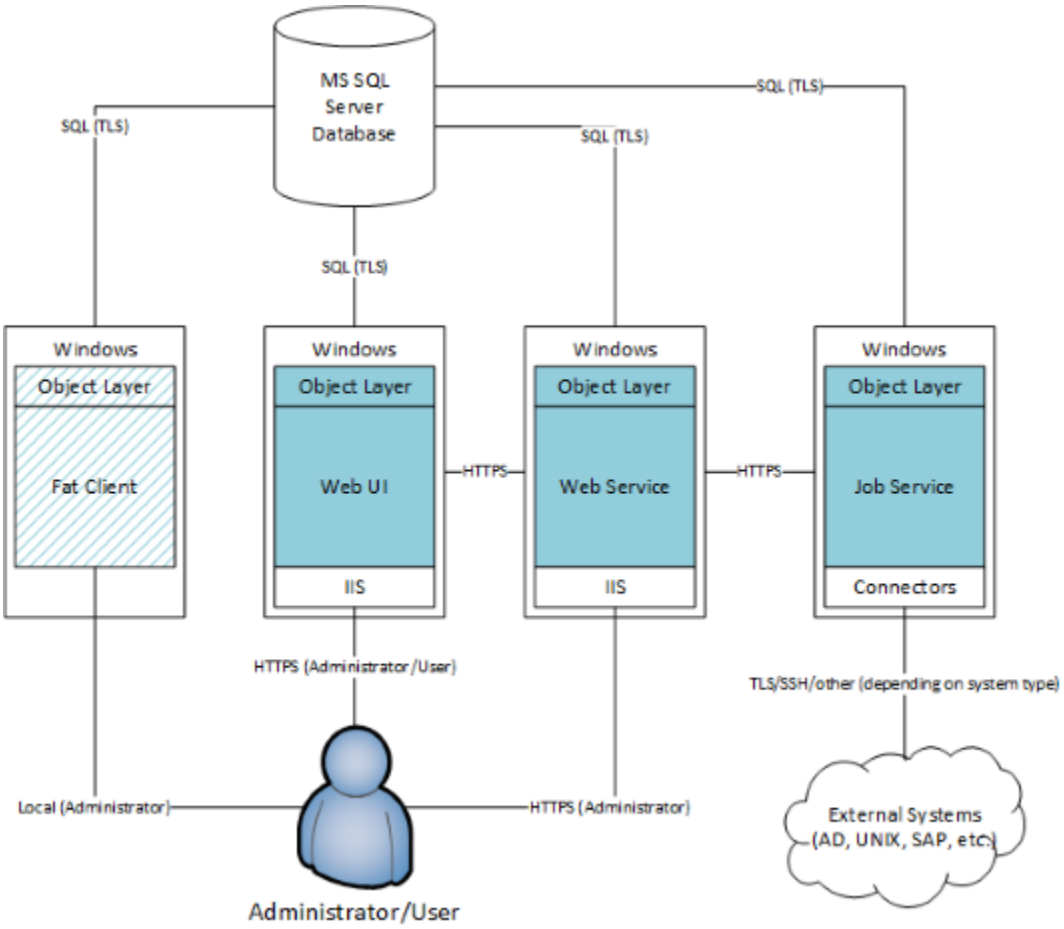
2.2 TOE Architecture

The One Identity Manager v8.1.5 TOE consists of several components: fat client, web UI, web service, job service (and its connectors) that interface with a centralized Microsoft SQL Server database through a shared object layer interface. The object layer interface is responsible for all database I/O operations and interfacing with external systems. The One Identity Manager Service (Job Service) performs data synchronization and provisioning between the database and any connected target systems and executes actions at the database and file level. The Job Service retrieves process steps from the JobQueue and executes them. The Job Service Application is the only method of interfacing with other organizational systems (e.g. HR system, AD, SAP) and the protected communication is through the use of connectors. The fat client provides the Designer and Synchronization Editor tools that are used for the initial setup of One Identity Manager. The fat client also includes the Manager application, but this interacts with the TOE via the web service. The Web UI and web services component provide interfaces for managing employee data. The Web UI is the graphical front-end that handles administrative management tasks, and where a TOE user can use the Password Reset Portal to change their password. The Web service is a REST API that provides the same functions as the Web UI as well as the interfaces that Manager uses to manage administrative role assignment and password policies.

From an architectural standpoint, the identity data maintained by One Identity Management resides in a central database (in the operational environment). All communications between the TOE and the database use TLS.

The following figure depicts the TOE components within the operational environment.

Figure 1 TOE in Operational Environment



TOE components are highlighted in blue / shaded blue. The fat client application is shaded to indicate that it is primarily used for initial configuration activities. The web UI, web service, and job service (with connectors) can each be installed on their own platform or on the same platform in a distributed architecture.

2.2.1 Physical Boundaries

The One Identity Manager v8.1.5 TOE consists of fat client, web UI, web service, job service, and connectors. The TOE provides connectors and any required templates for the following types of external systems:

Connectors and prepared templates:

- Active Directory
- UNIX/Linux
- Exchange 2010, 2013, 2016
- SharePoint 2010, 2013, 2016
- Azure AD
- Exchange Online

- SharePoint Online
- Google G-Suite
- LDAP (including AS/400, RACF, ACF2, Top Secret)

The Operational Environment consists of:

- Database Server
  - SQL Server 2017 (64-bit) with the current cumulative update
- Minimum System Requirements - Administrative Workstations (Fat client)
  - Windows 10 (32-bit or 64-bit) minimum version 1511
  - Microsoft .NET Framework Version 4.7.2 or later
- Minimum system requirements for the Job Service (admin guides refer to as Server Service)
  - Windows Server 2016
  - Microsoft .NET Framework Version 4.7.2 or later
- Minimum system requirements for the Web Service and Web UI
  - Windows Server 2016
  - Microsoft .NET Framework Version 4.7.2 or later
- Microsoft Internet Information Services 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2
- web browser:
  - Internet Explorer 11 or later
  - Firefox (Latest Release)
  - Chrome (Latest Release)
  - Microsoft Edge (Latest Release)
- SSH Client,
- one or more supported external systems (see connectors above),
- Active Directory authentication server.

The TOE relies on the Windows FIPS-compliant cryptographic libraries bcryptprimitives.dll (CMVP2937) and cng.sys (CMVP2936) for trusted channel and trusted path connections. Random seeding for deterministic random bit functions used for key generation is obtained through the Windows bcryptgenrandom function and its underlying OS operations that provide its non-deterministic entropy data. The TOE uses SSHBlackbox that in turn uses the same underlying Windows FIPS-compliant cryptographic libraries for SSH functionality. SSHBlackbox is provided with the One Identity Manager TOE but is itself a third-party product.

The TOE interacts with the external systems to transmit and receive identity and credential data for user authentication and provisioning.

The TOE has the following minimum system requirements:

TOE Component	Processor	Memory	Hard drive storage
Job Service	8 physical cores 2.5 GHz+	16 GB RAM	40GB
Web UI	4 physical cores 1.65 GHz+	4 GB RAM	40GB
Web Service	8 physical cores 2.5 GHz+	8 GB RAM	40GB
Fat Client	4 physical cores 2.5 GHz+	4 GB+ RAM	1GB

2.2.2 Excluded from the Evaluated Configuration

The evaluation excludes the following Operational Environment software and security functionality that is supported by One Identity Manager but is not included or tested in the evaluated configuration:

- LDAP Enterprise User Stores
- User authentication methods: Internal One Identity Manager authentication, LDAP Server, OpenID Connect, OAUTH2, and 2-factor authentication
- Connectors: SCIMv2, databases (ADO.NET, OLEDB, ODBC), structured files (CSV, tab separated, etc.), IBM Notes, SAP R/3 and S/4Hana, PowerShell, Oracle E-Business Suite
- Configuration of the Password Reset Portal such that a user can log in to the Password Reset Portal using user accounts other than the central user account (i.e. target system user account).

2.2.3 Logical Boundaries

This section summarizes the security functions provided by One Identity Manager:

- Enterprise security management
- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels

2.2.3.1 Enterprise Security Management

The TOE provides the ability to identify and authenticate administrators using Active Directory. The TOE provides the capability to define and manage enterprise user security attributes and provision modifications in the target systems. The TOE provides the capability to define and securely transmit identity and credential data for use with other ESM products. The TOE provides a password restriction policy mechanism to ensure secure passwords are defined.

2.2.3.2 Security Audit

The TOE generates logs for the security relevant events specified in ESMICM PP. The TOE writes the logs to the central Microsoft SQL Server database using a TLS channel.

2.2.3.3 Identification and Authentication

The TOE associates roles, entitlements, and other user attributes with enterprise users and relies on the operational environment for user authentication. The TOE enforces binding of users to subjects by defining users as 'employee' objects inside the TOE. These objects are then mapped to accounts on external systems such that changes to user data on the TOE is propagated to these external systems through synchronization. The TOE also enforces binding between administrators and subjects during initial authentication such that an administrator's privileges to manage the TSF are assigned when they log in and any changes to their privileges only take effect on subsequent logins.

2.2.3.4 Security Management

The TOE provides the following management functions identified in the ESMICMPP:

- Management of administrator authentication data
- Definition and management of user identity and credential data
- Configuration of password policy for credential data
- Management of user credential status (e.g. suspended)
- Enrollment of users
- Configuration of transmission of identity and credential data to external entities, including enabling of trusted communications where necessary
- Configuration and assignment of administrative roles

The TOE also provides the ability for users to perform self-service management of their own password credential data. The TOE restricts access to the management functions to users with applicable roles and entitlements. By default, the TOE includes a One Identity Manager administrator role with full privileges to manage the TSF, but additional administrative roles can be defined and associated with users to grant a subset of these privileges.

2.2.3.5Protection of the TSF

Credentials/keys used by the TOE are stored in the operational environment. The TOE does not offer any interfaces to view the credentials/keys.

2.2.3.6 Trusted Path/Channels

The TOE provides trusted communication channels using TLS for communication with authentication servers, the audit server and for transfer of policy (identity and credential) data. SSH is used for transfer of policy data between the TOE and UNIX systems. HTTPS is used to protect communication channels between distributed TOE components.

The TOE provides trusted communication paths using Web UI/Web Service for remote administrators, which is enforced by IIS.

2.3 TOE Documentation

There are numerous documents that provide information and guidance for the deployment and management of the TOE. The following guides are used in the evaluated configuration:

- One Identity Manager 8.1.5 Common Criteria Supplemental Admin Guidance
- One Identity Manager 8.1.5 Installation Guide

- One Identity Manager 8.1.5 Configuration Guide
- One Identity Manager 8.1.5 User Guide for One Identity Manager Tools User Interface
- One Identity Manager 8.1.5 Web Portal User Guide
- One Identity Manager 8.1.5 Web Application Configuration Guide
- One Identity Manager 8.1.5 System Roles Administration Guide
- One Identity Manager 8.1.5 Target System Base Module Administration Guide
- One Identity Manager 8.1.5 Administration Guide for Connecting to Active Directory
- One Identity Manager 8.1.5 Business Roles Administration Guide
- One Identity Manager 8.1.5 Authorization and Authentication Guide
- One Identity Manager 8.1.5 Identity Management Base Module Administration Guide
- One Identity Manager 8.1.5 Operational Guide
- One Identity Manager 8.1.5 REST API Reference Guide
- One Identity Manager 8.1.5 Target System Synchronization Reference Guide
- One Identity Manager 8.1.5 LDAP Connector for CA ACF2 Reference Guide
- One Identity Manager 8.1.5 LDAP Connector for CA Top Secret Reference Guide
- One Identity Manager 8.1.5 LDAP Connector for IBM AS/400 Reference Guide
- One Identity Manager 8.1.5 LDAP Connector for IBM RACF Reference Guide
- One Identity Manager 8.1.5 Administration Guide for Connecting to Azure Active Directory
- One Identity Manager 8.1.5 Administration Guide for Connecting to Exchange Online
- One Identity Manager 8.1.5 Administration Guide for Connecting to G Suite
- One Identity Manager 8.1.5 Administration Guide for Connecting to Microsoft Exchange
- One Identity Manager 8.1.5 Administration Guide for Connecting to SharePoint
- One Identity Manager 8.1.5 Administration Guide for Connecting to SharePoint Online
- One Identity Manager 8.1.5 Administration Guide for Connecting Unix-Based Target Systems
- One Identity Manager 8.1.5 Administration Guide for Connecting to LDAP

3 Security Problem Definition

The Security Problem Definition (composed of organizational policies, threat statements, and assumption) has been drawn verbatim from the Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013 (ESMICM). The [ESMICM] offers additional information about the identified threats, but that has not been reproduced here and the [ESMICM] should be consulted if there is interest in that material.

In general, the [ESMICM] has presented a Security Problem Definition appropriate for enterprise security identity and credential management products, and as such is applicable to the One Identity Manager TOE.

4 Security Objectives

As with the Security Problem Definition, the Security Objectives have been drawn verbatim from the [ESMICM] and includes the optional objectives: OE.CRYPTO, OE.ROBUST, and OE.SYSTIME. O.BANNER is excluded per TD0055. The [ESMICM] offers additional information about the identified security objectives, but that has not been reproduced here and the [ESMICM] should be consulted if there is interest in that material.

In general, the [ESMICM] has presented a Security Objectives statement appropriate for enterprise security identity and credential management products, and as such are applicable to One Identity Manager.

4.1 Security Objectives for the Operational Environment

Table 1: Security Objectives Descriptions

Objective	Description
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.

5 IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013, [ESMICM]. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [ESMICM] made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in [ESMICM].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [ESMICM]. The [ESMICM] defines the following extended SFRs and since they are not redefined in this ST, the [ESMICM] should be consulted for more information in regard to those CC extensions.

- ESM_EAU.2: Reliance on Enterprise Authentication
- ESM_EID.2: Reliance on Enterprise Identification
- ESM_ICD.1: Identity and Credential Definition
- ESM_ICT.1: Identity and Credential Transmission
- FAU_STG_EXT.1: External Audit Trail Storage
- FPT_APW_EXT.1: Protection of Stored Credentials
- FPT_SKP_EXT.1: Protection of Secret Parameters

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Table 2: TOE Security Functional Components

Requirement Class	Requirement Component
ESM: Enterprise Security Management	ESM_EAU.2: Reliance on Enterprise Authentication
	ESM_EID.2: Reliance on Enterprise Identification
	ESM_ICD.1: Identity and Credential Definition
	ESM_ICT.1: Identity and Credential Transmission
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_STG_EXT.1: External Audit Trail Storage
FIA: Identification and Authentication	FIA_USB.1: User-Subject Binding
FMT: Security management	FMT_MOF.1: Management of Functions Behavior
	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions

Requirement Class	Requirement Component
	FMT_SMR.1: Security Management Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Stored Credentials
	FPT_SKP_EXT.1: Protection of Secret Key Parameters
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

5.2.1 Enterprise Security Management (ESM)

5.2.1.1 Reliance on Enterprise Authentication (ESM_EAU.2)

ESM_EAU.2.1 The TSF shall rely on [*[**Active Directory**]*] for subject authentication.

ESM_EAU.2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

5.2.1.2 Reliance on Enterprise Identification (ESM_EID.2)

ESM_EID.2.1 The TSF shall rely on [*[**Active Directory**]*] for subject identification.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

5.2.1.3 Identity and Credential Definition (ESM_ICD.1)

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, **[name, employee ID, password, business role, system role, application role, organization data]**.

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

1. For password-based credentials, the following rules apply:

a. Passwords shall be able to be composed of a subset of the following character sets: **[English character set]** that include the following values **[26 uppercase letters, 26 lowercase letters, 10 numbers, and the following 10 special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"**]; and
b. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and
c. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
d. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

2. For non-password-based credentials, the following rules apply:

a. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

5.2.1.4 Identity and Credential Transmission (ESM_ICT.1)

ESM_ICT.1.1 The TSF shall transmit [***identity and credential data***] to compatible and authorized Enterprise Security Management products under the following circumstances: [***immediately following creation or modification of data, at a periodic interval*****].**

Application Note: *The periodic interval is defined when the connection to the external system is first defined.*

5.2.2 Security Audit (FAU)

5.2.2.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1) Start-up and shutdown of the audit functions;
2) All auditable events identified in Table 3 for the not specified level of audit; and
3) [**none**].

Table 3: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)

Requirement	Auditable Events	Additional Audit Record Contents
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

1) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no other audit relevant information**].

5.2.2.2 External Audit Trail Storage (FAU_STG_EXT.1)

Modified by TD066: Clarification of FAU_STG_EXT.1 Requirement in ESM PPs

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [**SQL Database**].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

1) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and
2) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 User-Subject Binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**all user security attributes**].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [

- **Successful user authentication to the TOE associates that user's application role to the subject to determine the extent to which TOE administration is permitted.**

- **Explicit mapping of user attributes associates identity and credential attributes with a user account based on values for those attributes that are directly assigned to the account by an administrator.**
- **Implicit mapping of user attributes associates identity and credential attributes with a user account based on administrator-defined criteria, such that an explicit change to one attribute may automatically change a different attribute].**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**changes to user attributes take place upon the next logon**].

5.2.4 Security Management (FMT)

5.2.4.1 Management of Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of, disable, enable, modify the behavior of***] the functions: [**list of functions in Table 4**] to [**role, permission, entitlement in** Error! Reference source not found.**].**

Requirement	Management Activities	Role/Entitlement	Operation
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	One Identity Manager administrator A TOE user with the *change/set password* permission and the Entitlement(s) for the particular external system and resource. See Application Note. All users can change their own passwords.	Determine/modify the behavior of
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	See ESM_EAU.2	Determine/modify the behavior of
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	One Identity Manager administrator A TOE user with the *change data* permission and the Entitlement(s) for the particular external	Determine/Modify/ Enable, Disable the behavior of: Full control over establishment, removal etc... of enterprise users (maintained in the

Requirement	Management Activities	Role/Entitlement	Operation
		system and resource. See Application Note.	TOE and/or modified in external system) and their credentials including the ability to activate (or define a user), assign users to roles, and revoke roles, accounts, and entitlements.
		One Identity Manager administrators TOE users with permissions to *change/set password policy*: "insert" (create), "update" (change) or "delete"	Enable, Disable, Modify the behavior of the password management function
ESM_ICD.1	Management of credential status	One Identity Manager administrator TOE users with permissions to manage identities	Modify the behavior of
ESM_ICD.1	Enrollment of users into repository	One Identity Manager administrator TOE user with permissions to manage identities	Determine the behavior of
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data is performed	One Identity Manager administrator	Determine/modify the behavior of Enable/Disable
FAU_STG_EXT.1	Configuration of external audit storage location	Performed during installation and set-up. The One Identity Manager administrator must configure the TLS secure channel.	Enable, disable.
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	See ESM_ICD.1	
FMT_MOF.1	Management of sets of users that can interact with security functions	One Identity Manager administrator	Determine/modify the behavior of

Requirement	Management Activities	Role/Entitlement	Operation
FMT_SMR.1	Management of the users that belong to a particular role	One Identity Manager administrator	Determine/modify the behavior of
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	One Identity Manager administrator TOE user with permissions to start synchronization editor and to create/edit schedule	Enable/Disable
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	N/A- no configuration is necessary.	Enable/Disable

Table 4 TOE Management Functions

Application Note: *The required entitlement needed will depend on the external system account being managed. For example, in order to manage a user account in an external UNIX system, the entitlement required would be the account definitions entitlement for the specific target system (UNIX).*

5.2.4.2 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify]*** the [**password authentication data**] to [**TOE users**].

5.2.4.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**list of functions in Table 4**].

5.2.4.4 Security Management Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**One Identity Manager administrator, TOE users, administrator-assigned application roles**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Protection of Stored Credentials (FPT_APW_EXT.1)

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

5.2.5.2Protection of Secret Key Parameters (FPT_SKP_EXT.1)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.6 Trusted Path/Channels (FTP)

5.2.6.1 Trusted Channel (FTP_ITC.1)

Modified by TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs.

FTP_ITC.1.1 The TSF shall be capable of using **[*SSH, TLS, HTTPS*]** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **[*audit server, authentication server*, *transfer of data between distributed TOE components*, *[transfer of policy data, database]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [*[**audit data, user authentication, transfer of data between distributed TOE components**]*].

5.2.6.2 Trusted Path (FTP_TRP.1)

Modified by TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs.

FTP_TRP.1.1 The TSF shall be capable of using **[HTTPS]** to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and **[*no other types of integrity or confidentiality violations]*.**

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication and execution of management functions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the [ESMICM].

Table 5: Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Consequently, the assurance activities specified in the [ESMICM] apply to the TOE evaluation.

6 TOE Summary Specification

This chapter describes the security functions:

- Enterprise security management
- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels

6.1 Enterprise Security Management

The TOE provides automated methods to read user accounts and permissions from target systems into the One Identity Manager database and to link this data to employees. The TOE provides the capability to define and manage user accounts and their permissions and provision modifications in the target systems. Employees are supplied with the necessary permissions in the connected target systems according to their function in the company. Regular synchronization keeps data consistent between target systems and the One Identity Manager database.

In this ST, target systems are also referred to as external systems. The external systems are synonymous with the terms “authorized ESM Products” and "other Enterprise Security Management products" as used in the ESMICM PP. See Sections 2.2.1 and 6.1.3 for the list of supported external systems.

6.1.1 ESM_EAU.2 / ESM_EID.2

The TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject. The TOE uses an external Active Directory authentication server in the operational environment for user and administrator authentication. Username and password-based credentials are used for subject authentication. The TSF accepts the validity of an identity asserted by these authentication servers.

6.1.2 ESM_ICD.1

The TOE keeps track of users in a central SQL Server database as “identities”. During initial configuration Administrators define the relationships of how that identity data is populated using scripts. So for example, an administrator can configure it so that when a new user gets created in PeopleSoft, the TOE will take that data and create a new ‘identity’ and assign them their first name, last name, etc. Then another script could be configured to take that same data and create an AD account with it. The TOE keeps track of this data in the local SQL Server database.

The TOE maintains the following security-relevant identity data:

- Name
- Employee ID
- System role
- Business role

- Application role
- Organization data (department, cost center, location)

The product may also maintain other user identity data, but it does not have security relevance with respect to the TSF. This includes data such as physical address and contact information.

The TOE maintains the following security-relevant credential data:

- Credential lifetime
- Credential status (enabled, suspended, temporarily revoked, permanently revoked)
- Password

Note that while the TSF is responsible for maintenance of the password, password data is not stored persistently by the TOE. It is only stored in memory long enough to be transmitted to the environmental data store(s) in which it resides.

The TOE's role within an organization's architecture is to maintain user identity and credential data in a single location so that changes to this data can be replicated to different organizational systems all at once, and so that changes to a user's ability to access organizational resources across multiple systems can be initiated automatically when their associated attributes change.

User identity data maintained by the TSF can be mapped to corresponding attributes in organizational systems. For example, the administrator may configure the TOE to associate the 'name' value with an Active Directory User class object so that a change to a user's name updates the corresponding data in Active Directory. Credential changes work the same way. The TOE's user password attribute may be mapped to corresponding password attributes on a variety of different environmental entities. When a user's password is changed, the TSF will use its configured synchronization mappings to push the updated password to the relevant user records on the configured entities.

For each attribute, an administrator may configure whether the 'authoritative' source of the attribute is the TOE or an external system. The TOE will periodically communicate with the external entities it is configured to synchronize with (see ESM_ICT.1 below) and will resolve data conflicts by ensuring that the value associated with the authoritative source is applied at both ends of the connection. This allows administrators to retain the use of legacy systems for managing certain user attributes if desired.

New users may be created manually on the TOE, or enrolled from external sources using synchronization. For example, the TOE may be synchronized with the organization's HR system such that new users are created on that system and then imported into the TOE through a mapping between TOE user attributes and attributes on the HR system. When a new user is created, the TSF automatically assigns that user a unique employee ID value. This value can then be used as a primary key across all environmental systems to associate all of that user's various system and application accounts with their centrally-defined identity.

In addition to replicating user identity data between different organizational systems, administrators may use the TOE to define conditional rules such that a change to one user attribute causes different changes to be made on external systems (also referred to as "resources"). For example, the organization may have a resource that only users with a certain role, department, or geographic location may access. The TSF may be configured in such a way that changing a user's role or organization data attribute to a specific value will automatically trigger a synchronization event that creates a new account on that resource for that user. Likewise, it may be configured to remove the account if the user's role or organization data attribute is changed to no longer be that value. This is typically configured based on changes to a user's

system role or business role attributes. The logical access granted to resources is dependent on the type of external entity it is, and may include the following:

- Target System account definitions (e.g. Unix system account)
- Active Directory groups
- SharePoint groups
- Azure Active Directory groups
- Azure Active Directory administrator roles
- Azure Active Directory subscriptions
- Disabled Azure Active Directory service plans
- Azure Active Directory Module
- Unix Groups

Business roles are typically assigned to employees so they can obtain their company resources. System roles make it easier to assign company resources that are frequently required or that are always assigned together. For example, new employees in an auditor role may be provided, by default, with certain system entitlements for both Active Directory and for SharePoint. In order to avoid a lot of separate assignments, it is possible for the TOE administrator to group these company resources into a system role. System roles may be assigned directly to individual users, or they may be assigned indirectly through the same types of triggers as are defined above (e.g. assigning a user a given business role or organization data attribute may automatically trigger the assignment of one or more attached system roles).

Changes to credential data may have a similar effect. For example, the TOE may be configured so that if a user's credential status has been set to be suspended or revoked, the TSF may synchronize with the configured external entities to disable or delete all relevant external accounts for that user.

Users also have an entitlement attribute, which is also known as an application role. This attribute determines the extent to which a user may manage the TSF. By default, a user has an unprivileged application role, which allows them to log in to the TOE to perform self-service of their own credential data (see FMT_MTD.1).

The TOE provides the ability to query the status of an enterprise user's credentials. This allows an administrator to determine whether a user is active or if they have been suspended, temporarily disabled, or permanently disabled, as well as when their credential is set to expire. An administrator may manually configure the expiration period of a user's credential on a per-user basis. For example, if the organization establishes a 90-day lifetime for credentials but a given user has a known departure date that is sooner than 90 days, the administrator may specify a "last working day" value for them that supersedes the credential lifetime policy for that user. Once that day has been reached, the credential is automatically set into a permanently disabled status. The TOE also includes a 'security incident' option that allows an administrator to immediately suspend or revoke a user's credential, which then deactivates all accounts that are mapped to their identity.

The TOE provides the capability to ensure defined enterprise user credentials satisfy specified minimum strength rules, via Password Policies. Predefined password policies are supplied with the default installation and can be customized. Password policies can be created or modified by One Identity Manager administrators and TOE users with administrator permissions. Password Policies define and enforce the following:

- Password strength — Minimum password length and alphanumeric character requirements and restrictions (as specified in ESM_ICD.1.8 parts a-c).
- Password history — The number of passwords that have been previously reset that cannot be used in a password reset (as specified in ESM_ICD.1.8 part d).

6.1.3 ESM_ICT.1

The TOE transmits subject identity and credential data to other compatible and authorized ESM external systems:

- Active Directory
- UNIX/Linux
- Exchange 2010, 2013, 2016
- SharePoint 2010, 2013, 2016
- Azure AD
- Exchange Online
- SharePoint Online
- Google G-Suite
- LDAP (including AS/400, RACF, ACF2, Top Secret)

The types of data transmitted to these external systems and the secure channel used to carry this data is shown in the table below:

Table 6: External Systems, attributes, and secure channel

	Attributes Transmitted		
External System / ESM product	**Identity Data**	**Credential Data**	**Secure Channel**
Active Directory	X	X	LDAPS (TLS)
Unix/Linux	X	X	SSH
Exchange 2010, 2013, 2016	X		HTTPS
SharePoint 2010, 2013, 2016	X		HTTPS
Azure AD	X	X	HTTPS
Exchange Online	X		HTTPS
SharePoint Online	X		HTTPS
Google G-Suite	X	X	HTTPS
Mainframe (AS/400, RACF, ACF2, Top Secret)	X	X	LDAPS (TLS)

LDAP	X	X	LDAPS (TLS)

All outbound transmissions are done immediately following creation or modification of data. Inbound communications of data is periodic, and depends on initial configuration of time period for each external system. The Synchronization Editor provides interfaces to configure the interval for consumption (e.g. daily, hourly, etc.). When the TOE receives data from an external system, it will reconcile all changes by updating any modified attributes where the external system is the authoritative source for that attribute and discarding any modifications of attributes that the TOE is the authoritative source for.

6.2 Security Audit

The TOE generates logs for security relevant events including the events specified in ESMICM PP. The TOE sends the logs to an external (to the TOE) SQL database for storage. The database and reliable timestamps are provided by the operational environment.

6.2.1 FAU_GEN.1

The TOE generates log records for security relevant events as they occur. The events that can cause an audit record to be logged include the following auditable events defined in **Table 3Error! Reference source not found.**:

- Startup and shutdown of the audit functions
- All use of the authentication mechanism
- Creation or modification of identity and credential data
- Enrollment or modification of subject
- All attempts to transmit information
- Establishment and disestablishment of communications with audit server
- All modifications of TSF function behavior
- Use of the management functions
- All use of trusted channel functions
- All attempted uses of the trusted path functions

Startup/shutdown of the audit function occurs when the product is started/stopped. Additionally, the establishment and disestablishment of communications with audit server occurs when the product is started/stopped. Establishing/disestablishing connectivity with the audit server is also logged in the form of logging changes to whether certain events are configured to be audited.

Use of the authentication mechanism is logged in the DialogJournal table in the SQL Server database as “Login failed” and “Login succeeded” events. As this is the only use of the trusted path function, logging for this behavior is synonymous with logging trusted path usage.

All manipulation of administrator, user, or configuration data that would occur as a result of executing the TOE’s management functions is logged in the DialogWatchOperation table in the SQL Server database. Within this table, the OperationType field identifies whether the data in question was created, modified, or removed, and the DisplayValue field identifies the data.

- Creation or modification of identity and credential data – if a new user is created, the DisplayValue will just show the name/ID of the user. If an existing user attribute is modified, the DisplayValue will show both the name/ID of the user and the modified attribute.
- Enrollment or modification of subject – same as "creation or modification of identity and credential data."
- Establishment and disestablishment of communications with audit server – if an auditable event is enabled/disabled, the OperationType field will show a U for modification and the DisplayValue field will show the event that was affected by the change (e.g. "Common\Journal\LoginAudit"). This event is then tied to the DialogWatchProperty SQL table via a shared key, which includes the ContentShort field that flags whether the modification was to enable or disable logging for the event.
- All modifications of TSF function behavior – the DisplayValue will show different information, depending on the function behavior being modified:
    - Creating or modifying users or any data associated with them will be logged as shown in "creation or modification of identity and credential data" above.
    - Creating or updating an application role will show the name of the role.
    - Assigning a user to an application role will show the name of the role and the username/ID of the user.
    - Configuring communications with an external entity will identify the type and name of the target system (e.g. "Active Directory Domain (DC=IAM,DC=CORP) - Active Directory Service (Root DN dc=IAM,dc=corp, Server iams01.iam.corp)")
- Use of the management functions – same as "all modifications of TSF function behavior" and "creation or modification of identity and credential data"

When using the TOE to review this data, the TSF will automatically associate the data in the DialogWatchOperation and DialogWatchProperty SQL tables. If this data is exported beyond the SQL Server database, the primary key of the DialogWatchOperation table is the UID_DialogWatchOperation field, which is the foreign key for the DIalogWatchProperty table.

Transmission of identity and credential data is logged in the DPRJournal, DPRJournalObject, and DPRJournalMessage tables. Specifically, the DPRJournal.UID_DPRProjectionConfig field identifies the external system data is being transmitted to/from and the type of transmission that is performed (e.g. "initial synchronization" for the first time connectivity is established with that system). The DPRJournalObject.ObjectDisplay field identifies the data that is transmitted as part of this operation. This also serves as a log for use of the trusted channel functions since synchronization operations require use of the trusted channel.

When using the TOE to review this data, the TSF will automatically associate the data in the DPRJournal, DPRJournalObject, and DPRJournalMessage SQL tables. If this data is exported beyond the SQL Server database, the primary key of the DPRJournal table is the UID_DPRJournal field, which is the foreign key for both the DPRJournalObject and DPRJournalMessage fields.

The logged audit records identify the date and time, the nature or type of the triggering event, an indication of the outcome of the event, and the identity of the user responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in **Table 3**.

6.2.2 FAU_STG_EXT.1

The TOE stores audit records in the operational environment in the Microsoft SQL Server 2017 database. The audit records can be accessed through the Web UI.

Audit records sent to the database are transmitted over a TLS trusted channel. There is no concern with unavailability because if the database is unavailable, changes to the TSF or its data cannot be made. Therefore, there is no possibility a change is made but not logged.

The storage of generated audit data is in the operational environment and therefore the TOE relies on the environment to protect the stored audit records from unauthorized deletion; and to prevent unauthorized modifications to the stored audit records in the audit trail.

6.3 Identification and Authentication

The TOE associates roles, entitlements, and other user attributes with enterprise users. The TOE relies on the operational environment to authenticate users.

6.3.1 FIA_USB.1

The TOE provides user-subject binding in two situations. The first situation is binding of the administrator and TOE user to their assigned privileges in the object layer during initial authentication. If a user or administrator's privileges are changed while they are logged in, the change won't take effect until their next session. This applies both to their role (i.e. what functions they can perform) and scoping (i.e. what objects they can perform their allowed functions against). For the web service interface, the binding is made through generated tokens. The specific interfaces that can be accessed is derived from role and entitlement membership or by direct assignment to account.

The second situation is binding of user 'identities' defined by the product to accounts on external systems. This is done through implicit or explicit mapping. For example, you can create a workflow that automatically creates a new AD account for a user (using scripts for example) if the product ingests a new user from the HR system. The new user would be created as an 'identity' (the subject) and its various accounts on external systems would be directly mapped to it. Rules can also exist to change some aspects of that identity if a specific change is detected on a specific external system.

The "user" is the person (an enterprise user) in the organization who is authorized to perform activities in the organization, and the "subject" is the 'identity' that is defined for them in the TOE. The 'binding' is the notion that the subject attributes are used to go out and change the configurations of accounts that the user actually uses, which affects what they can do on the organizational systems. The "initial association" between user security attributes and subjects is the notion that you can script things to say that when a new identity is created, this will automatically trigger certain other accounts to be created based on the identity attributes that were filled out.

Enterprise users (including those that have administrative privileges) are associated with all user security attributes during user subject binding.

6.4 Security Management

The TOE provides the management functions identified in the ESMICM PP; maintains roles and restricts access to the functions. The management functions are restricted to the One Identity Manager administrator and to TOE users with delegated administrative permissions.

6.4.1 FMT_MOF.1

The TOE restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the management functions as defined in **Table 4**.

In order to manage enterprise user authentication data for another user, one must have been assigned the change/set password permission and the entitlement(s) for the particular external system and resource. All users can change their own passwords. A user with the change/data permission can manage the identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.). Enrollment of users and management of credential status can be performed by users with permissions to manage identities. Other permissions include those to start synchronization editor and to create/edit schedule that control actions requiring the trusted channel. These management functions can also be performed by the One Identity Manager administrator.

6.4.2 FMT_MTD.1

The TOE provides a self-service option that allows users to change their own password attribute data. This is performed using the Password Reset Portal on the Web UI.

The TOE uses Active Directory for user/administration authentication, so authentication data needed to access the TSF is stored there. Since the TOE uses TLS to communicate with the external Active Directory, this is used to protect any authentication data in transit (e.g. challenge/response and propagation of updated credential data initiated through a password change on the TOE).

Depending on how the TOE is configured, the password attribute data may be transmitted to other external systems as well. In this case, protection of the credential data is the responsibility of the system that the data is transmitted to. Table 6 identifies the trusted channel that may be used to secure this data while it is in transit to the target system.

6.4.3 FMT_SMF.1

The TOE provides the management functions identified in **Table 4.**

The “Configuration of circumstances in which transmission of identity and credential data is performed” function is performed during initial configuration of the TOE in Synchronization Editor, both in terms of establishing the connection to the external systems and configuring the communications interval.

The “Management of sets of users that can interact with security functions” function is performed using Manager, as is management of password policies (a subset of “Definition of identity and credential data that can be associated with users”).

6.4.4 FMT_SMR.1

The TOE maintains the roles of One Identity Manager administrator and TOE user. Users with the One Identity Manager administrator role have full permissions to create new users, permissions and roles and manage identities. This user has full administrative capabilities to manage the TOE including creating custom role and permissions and associating users with them.

Users with the One Identity Manager administrator role can create new roles with different levels of permissions and then assign these roles to TOE users for delegated administration. However, a TOE user doesn’t have to have admin permissions, they can be just an organizational user who uses the TOE solely to reset their own password.

Although the TOE provides pre-defined roles that can be assigned to users, typically administrators of the TOE define their own custom permissions and roles rather than use the predefined ones. Therefore the evaluation focusses on the permissions and entitlements a user must have in order to perform a specific management function. Permissions and entitlements are described in Section 6.1.2. TOE users become administrators through association of Application Roles with their user identities. Application Roles determine the management functions that are authorized. Permission Groups (permissions) define the actions that may be performed and are assigned to Application Roles. Entitlements determine the external targets that the assigned Application Roles can be applied to. For example, an administrator may be assigned an Application Role that allows them to manage user passwords, but if they lack entitlement to interact with Active Directory, an attempted user password change that is pushed to Active Directory will not succeed.

6.5 Protection of the TSF

Credentials/keys used by the TOE are stored in the operational environment. The TOE does not offer any interfaces to view the credentials/keys.

6.5.1 FPT_APW_EXT.1

There is no persistent storage of passwords on the TOE. Administrator and user accounts with passwords are defined on external systems. When a user sets a password on the TOE, the password temporarily exists inside the One Identity Manager until it gets pushed to the relevant external systems. The password is generated or received by the object layer, and then encrypted. Encryption is performed by the Microsoft Windows Cryptographic Primitives Library bcryptprimitives.dll and the private key is stored in the Windows key store in the operational environment. For the purpose of writing a password to the target system there is a very small period of time where the decrypted value must be in memory. However at no time is a password written to a temporary file or swapped out to a region in plain text and therefore no passwords could be discovered by examination of TOE memory through normal methods.

The workflow for password creation is as follows:

1. Password generated/entered in object layer
2. Pull public key from database
3. Encrypt password with public key and send to database
4. Database puts in job queue
5. Job service pulls from queue and decrypts the password with the stored private key
6. From there, the password data is transmitted to the external system.

The database in the workflow process above is a SQL server database shown in Figure 1 and is in the TOE's operational environment.

6.5.2 FPT_SKP_EXT.1

An administrator is unable to read or view any keys (stored or ephemeral) through "normal" interfaces as there are no interfaces to view key data. The TOE stores a private key for password decryption in the Windows key store in the operational environment. Certificates and their associated private keys are stored in the Windows Certificate Store. Windows stores private keys encrypted using RSA. All key management is the responsibility of the environmental cryptographic components that the product relies on.

6.6 Trusted Path/Channels

The TOE provides trusted communication channels using TLS for communication with authentication servers, the audit server and TLS/SSH for transfer of policy data.

The TOE provides trusted communication paths using Web UI/Web Service for remote administrators using HTTPS, which is enforced by IIS.

6.6.1 FTP_ITC.1

The TOE provides trusted communication channels using TLS v1.1, and TLS v1.2 for the following connections:

- External authentication of users and administrators (AD)
- Transfer of policy data (collection and provisioning)
- Transfer of audit records (SQL database)

The mainframe (AS/400, RACF, ACF2, Top Secret), LDAP, and Active Directory connectors use LDAPS, which establishes a TLS connection between the TOE and these types of external systems before any LDAP messages are transferred.

The TOE provides trusted communication channels between the TOE and UNIX-based systems using SSH for transfer of policy data. The TOE uses SSHBlackbox for this connection. SSHBlackbox invokes OS cryptographic libraries for underlying cryptographic functions.

Table 6 lists the environmental trusted channels invoked by the TOE for each type of external system connection.

When the web UI, web service, and job service (with connectors) components are in a distributed architecture, the TOE provides trusted communication channels using HTTPS (HTTP over TLS). TLS v1.1, and TLS v1.2 are supported.

The TOE permits the TSF to initiate communication via the trusted channel.

Microsoft Windows Cryptographic Primitives Library bcryptprimitives.dll (CMVP2937) and cng.sys (CMVP2936) is used for all TLS, SSH, and HTTPS connections.

6.6.2 FTP_TRP.1

The TOE provides trusted communication paths using HTTPS for remote administrators accessing the Web UI. The TOE requires all users to initiate communication via the trusted path for initial user authentication, and execution of management functions.

Microsoft Windows Cryptographic Primitives Library (bcryptprimitives.dll (CMVP2937) and cng.sys (CMVP2936)) is used for the HTTPS connection (i.e. HTTP over TLS).

7 Protection Profile Claims

This ST is conformant to the Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24, 2013 and including the following optional SFRs: FMT_MTD.1.

As explained in Section 0,

Security Problem Definition, the Security Problem Definition of the [ESMICM] has been copied verbatim into this ST.

As explained in Section 4, Security Objectives, the Security Objectives of the [ESMICM] excluding O.BANNER and including the optional objectives: OE.CRYPTO, OE.ROBUST, OE.SYSTIME have been copied verbatim into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the [ESMICM]. The only operations performed on the SFRs drawn from the [ESMICM] are assignment and selection operations.

Table 7. SFR Protection Profile Sources

Requirement Class	Requirement Component	Source
ESM: Enterprise Security Management	ESM_EAU.2: Reliance on Enterprise Authentication	ESMICM
	ESM_EID.2: Reliance on Enterprise Identification	ESMICM
	ESM_ICD.1: Identity and Credential Definition	ESMICM
	ESM_ICT.1: Identity and Credential Transmission	ESMICM
FAU: Security audit	FAU_GEN.1: Audit Data Generation	ESMICM
	FAU_STG_EXT.1: External Audit Trail Storage	ESMICM
FIA: Identification and authentication	FIA_USB.1: User-Subject Binding	ESMICM
FMT: Security management	FMT_MOF.1: Management of Functions Behavior	ESMICM
	FMT_MTD.1: Management of TSF Data	ESMICM
	FMT_SMF.1: Specification of Management Functions	ESMICM
	FMT_SMR.1: Security Management Roles	ESMICM
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Stored Credentials	ESMICM
	FPT_SKP_EXT.1: Protection of Secret Key Parameters	ESMICM
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF Trusted Channel	ESMICM
	FTP_TRP.1: Trusted Path	ESMICM

8 Rationale

This security target includes by reference the [ESMICM] Security Problem Definition, Security Objectives (including the optional objective: OE.CRYPTO, OE.ROBUST, OE.SYSTIME and excluding O.BANNER), and Security Assurance Requirements. The security target makes no additions to the [ESMICM] assumptions. [ESMICM] security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [ESMICM] application notes and assurance activities. Consequently, [ESMICM] rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 8: Security Functions vs. Requirements** Mapping demonstrates the relationship between security requirements and security functions.

Table 8: Security Functions vs. Requirements Mapping

	Enterprise security management	Security audit	Identification and authentication	Security management	Protection of the TSF	Trusted path/channels
ESM_EAU.2	X					
ESM_EID.2	X					
ESM_ICD.1	X					
ESM_ICT.1	X					
FAU_GEN.1		X				
FAU_STG_EXT.1		X				
FIA_USB.1			X			
FMT_MOF.1				X		

	Enterprise security management	Security audit	Identification and authentication	Security management	Protection of the TSF	Trusted path/channels
FMT_MTD.1				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_APW_EXT.1					X	
FPT_SKP_EXT.1					X	
FTP_ITC.1						X
FTP_TRP.1						X