WSO2 Identity Server

Security Target

Date: 15/12/2025

Created by 

Change History

Version	Date	Author	Comment
1.0	26/11/2024	WSO2	First draft
1.1	22/08/2024	WSO2	Changes due to OR
1.2	01/09/2025	WSO2	Changes based on evaluation feedback
1.3	18/09/2025	WSO2	Changes based on evaluation feedback
1.4	25/09/2025	WSO2	Changes based on evaluation feedback
1.5	16/10/2025	WSO2	Changes based on evaluation feedback
1.6	22/10/2025	WSO2	Changes based on evaluation feedback
1.7	15/12/2025	WSO2	Changes based on evaluation feedback

Table of contents

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: WSO2 Identity Server ST

Version: v1.7

Author: WSO2

Evaluation Lab: Applus+

Date of publication: 15/12/2025

1.2 TOE REFERENCE

TOE Name: WSO2 Identity Server

TOE Developer: WSO2

TOE Version: 7.0.0, update level 126

1.3 TOE OVERVIEW

1.3.1 INTRODUCTION

The Target of Evaluation (TOE) is WSO2 Identity Server (WSO2 IS), version 7.0.0, update level 126. Referred to as TOE from this point forward. The TOE is a powerful, modern identity and access management solution for on-premises or cloud environments. It enables organizations to deliver exceptional, trusted digital experiences to all types of users.

The TOE can handle authentication requests from integrated service providers and redirect them to the appropriate authentication services remotely or locally. The WSO2 Identity Server ensures easy integration with various applications to facilitate single sign-on (SSO), social login, identity federation, API security, strong authentication, account management, and privacy compliance.

1.3.2 TOE TYPE

The TOE is a software application used in enterprise environments to manage identities, access, and authorization through different apps.

1.3.3 TOE USAGE & MAJOR SECURITY FEATURES

The main focus of the TOE is the establishment of unique, unambiguous identities which enables the issuance and management of credentials and authorization attributes of enterprise user accounts. The notion of identity refers to the unique identifier assigned to an individual with whom credential and attribute data can be associated.

The TOE is expected to be deployed on a system and provide an interface to one or more subject data repositories. One or more Assignment Managers will be given the authority to use the TOE to manipulate this data as needed. Subject data is used by other Enterprise Security Management (ESM) components as necessary to carry out their duties. The TOE can generate audit trails, which can be stored locally and transmitted to an external entity for further processing and retention.

An individual must be enrolled to be identified as a user within the ESM system. Enrollment refers to the act of assigning a unique identifier to a subject, generating and issuing credentials, defining attributes for a user, and propagating that data to any repositories that use it. The TOE can securely transmit this data to other ESM components.

The TOE exhibits the following behavior:

- Provisioning of subjects (enrolls new subjects to an organizational repository, associate and disassociate subjects with organizationally defined attributes)
- Issue and maintain credentials associated with user identities
- Publish and change credential status (such as active, suspended, or terminated)
- Establish appropriate trusted channels between itself and compatible ESM products
- Generate an audit trail of configuration changes and subject identification and authentication activities
- Store audit trail data and transmit it to a trusted external entity securely
- Securely transmit identity and credential attribute data via a trusted channel

1.3.4 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

The WSO2 Identity Server is a Java application that requires JDK 17.0.2. For detailed information, please refer to “Environment Compatibility” section in the WSO2 Identity Server Documentation (PDF).

The TOE is compatible with most common DBMSs. The embedded H2 database is suitable for development and testing. For enterprise production environments, an industry-standard RDBMS such

as Oracle, PostgreSQL, MySQL, MSSQL, or MariaDB is recommended. For detailed information, please refer to "Tested DBMSs" in "Environment Compatibility" section in WSO2 Identity Server Documentation PDF

The TOE supports any of the following user stores:

- RDBMS
- An LDAP
- Active Directory

To fully utilize the product's console, a web browser with JavaScript enabled is required.

For external provisioning, the Identity Provider shall be compatible with the SCIM2 protocol. For inbound provisioning, a connection with an application or REST API is necessary.

The developer provides sample applications that can be used to test this functionality. These applications require Node.js and NPM.

To encrypt the critical parameters of configuration files, utilize the Cipher Tool with Secure Vault, which is included in the WSO2 Identity Server product.

To securely maintain the TOE over time, the WSO2 Update Tool may be used as part of the operational environment. While not part of the TOE itself, the Update Tool is the authorized mechanism for delivering security updates and patches. It ensures that updates are applied safely by validating their integrity using cryptographic hashes, downloading updates over secure channels, and creating a backup of the TOE before applying changes. For a complete list of security updates and advisories applied to the evaluated TOE version, see "Appendix A: Security Updates Applied".

1.4 TOE DESCRIPTION

1.4.1 INTRODUCTION

The TOE can connect to different applications and control the way users log in. When applications are connected, the TOE can customize the login flow and manage the user attributes shared with them. The TOE also supports a variety of external identity providers, which it can connect to and use to authenticate or manage users.

1.4.2 TOE LOGICAL SCOPE

The TOE is the main point of cohesion in an enterprise environment. It manages user accounts, credentials, and attributes used within the enterprise environment. The TOE also logs and controls users' actions through different applications.

Figure 1, “TOE Environment,” presents the components that are in the TOE’s scope. That is, TOE includes Identity and Credential management with control of repositories that keep identity and credential data, as well as relevant attributes.

The TOE can manage user accounts and their attributes and transmit these data by provisioning them to external entities.

Furthermore, the TOE permits the recording of different events as audit logs in a local and external database, thus registering all users’ actions related to enterprise identification and authentication.

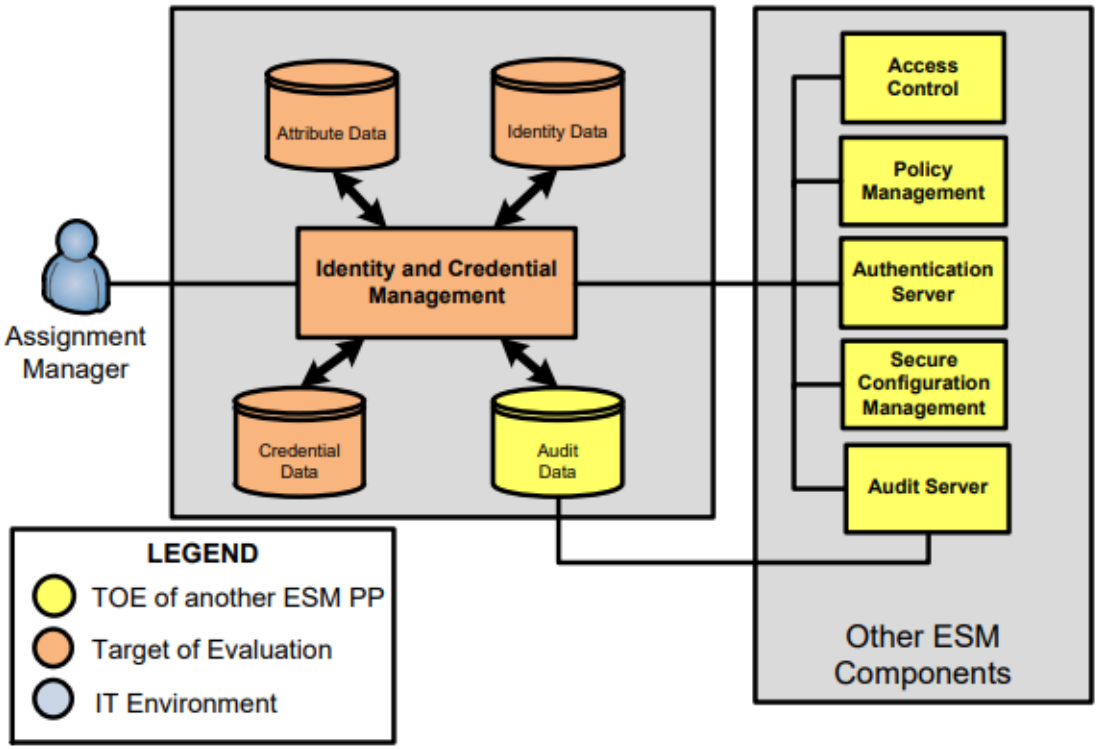

Figure 1 TOE Environment

1.4.3 TOE PHYSICAL SCOPE

WSO2 Identity Server 7.0.0 is a software-only TOE, and therefore, its physical boundary is its software. The TOE does not include the hardware or operating system of the system on which it is installed. It also does not include the third-party software that is required for the TOE to run (indicated in Non-TOE software/hardware).

The software bundle is available at the developer’s GitHub delivered as a zip file, the SHA256 hash is the following:

Item	SHA256 Hash Value
wso2is-7.0.0.zip	47df36faee3ff8f851d3d2064952968b bdd0b077f8b7367ddd872047e948c2c9

Table 1 Software SHA256

The TOE physical scope additionally includes the preparative and operational guidance to install and operate the TOE in a secure manner.

TOE Item	Format	Delivery Method	Hash
WSO2 Identity Server 7.0.0	Zip file	GitHub Download	47df36faee3ff8f851d3d2064952968b bdd0b077f8b7367ddd872047e948c2c9
[AGD-PRE]	PDF	Web Download	56AD97E3939F91FB727A6E325373DE6C08FCAAE0FC78A5F2665954D269272816
[AGD-OPE]	PDF	Web Download	0F80711B7554A2CAF5408B6CF79B7F6B8CCB104138ED7469737256150CE197D1
[API-Calls]	PDF	Web Download	A41673EB187D634FE408B382EF9568701E4A8CA23EA852ACCA626BDD5E785778
[WSO2-DOCS]	PDF	Web Download	7F4273D15DBD799092A67E6E619A6259F7F2A0D5EBA5C12E35F7F34628F7EDC9

Table 2 Physical scope of the TOE

2 CONFORMANCE CLAIMS

This Security Target and the TOE described are in accordance with the requirements of Common Criteria [CC:2022].

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC2022R1P2] extended.
- Conformance with [CC2022R1P3] conformant.

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of November 2022, version 1 revision 1 with an evaluation assurance level of EAL1 + ASE_SPD.1 + ASE_OBJ.2.

This Security Target claims conformance with the following protection profiles:

- Protection profile Enterprise Security Management Identity and Credential Management v2.1 with strict conformance [PP-ESM-I-CM].

Although the [PP-ESM-I-CM] is compliant with CCMB-2012-09-001, Version 3.1 Revision 4 September 2012, this ST is in accordance with the CC:2022. This is due to the following transition periods rules, stated in [CC2022-TRANSITION-POLICY]:

> "1. CC v3.1 R5 is the last revision of version 3.1 and may optionally be used for evaluations of Products and Protection Profiles starting no later than the 30th of June 2024.
>
> 2. Security Targets conformant to CC:2022 and based on Protection Profiles certified according to CC v3.1 will be accepted up to the 31st of December 2027.
>
> 3. After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date."

As stated in the first rule, evaluations starting after 30th of June 2024 shall not use CC v3.1 R5. Therefore, the Security Target is stating compliance with CC:2022 while claiming compliance with a certified PP with CC v3.1. This fact should be accepted according to rule 2. This version change does not affect either the scope of the evaluation or the security functional requirements. Table 3 SFRs affected by the CC version change is provided to indicate the changes between the two versions of the Common Criteria.

In addition to the above, although the [PP-ESM-I-CM] does not claim conformance with either the security assurance requirement (SARs) ASE_SPD.1 or ASE_OBJ.2 this ST does include them because the needed information for be compliant with both SARs is present in the PP.

SFR	Change
FAU_GEN.1.2	CC2022 adds the PP-module and functional package concepts but SFR both versions are equivalent.
FAU_STG_EXT.1	The extended component has been substituted with CC:2022 requirements FAU_STG.1 and FAU_STG.2. Both SFRs complete the FAU_STG_EXT.1 requirements.
FTA_TAB.1	The CC2022 version of FTA_TAB.1 includes a selection and assignment that does not change the purpose of the requirement.
FTP_TRP.1.3	With the CC:2022 version of the SFR the refinement of the PP is not needed.

Table 3 SFRs affected by the CC version change

2.1 CONFORMANCE CLAIMS RATIONALE

2.1.1 TOE TYPE CONSISTENCY

The TOE Type is consistent with the Protection profile Enterprise Security Management Identity and Credential Management v2.1 as the TOE is a Java application that provides features to manage identities and credentials in an enterprise environment. The TOE enforces secret keeping policies and access control. Also, TOE is able to maintain security attributes and associations with the subject's accounts. The TOE is able to create trusted channels for the transmission of identity and credentials with external entities. In addition, TOE is able to generate audit data, store it, and transmit it to a remote log server.

2.1.2 SECURITY PROBLEM DEFINITION CONSISTENCY

2.1.2.1ASSUMPTIONS CONSISTENCY

PP_ESM_ICM with strict conformance.

The following assumptions have been selected. Optional assumptions are discussed below:

A.CRYPTO: The TOE does not implement cryptographic primitives, so these are taken from the environment.

A.ROBUST: The TOE does not fulfill a feature expected by FIA_SOS.1, so features related to brute-force hardening of the TOE are delegated to the environment.

A.SYSTIME: The TOE is a software product that does not implement a time source. It is received from the Operational Environment as a reliable source.

PP	Assumptions
PP_ESM_ICM	A.CRYPTO, A.ESM, A.FEDERATE, A.ROBUST, A.SYSTIME, A.MANAGE, A.ENROLLMENT

Table 4 Assumptions Consistency

2.1.3 SECURITY OBJECTIVES CONSISTENCY

2.1.3.1OPERATIONAL ENVIRONMENT SECURITY OBJECTIVES CONSISTENCY

PP_ESM_ICM with strict conformance.

Security Objectives modified or deleted from this PP.

No security objectives for the environment modified from this PP

2.1.4 SECURITY REQUIREMENTS CONSISTENCY

2.1.4.1SARS CONSISTENCY

PP_ESM_ICM with strict conformance.

More SAR's has been added or augmented compared with the original PP. This means an improvement in the evaluations assurance and therefore it is justified.

PP	SARs
Added in this ST	ASE_SPD.1, ASE_OBJ.2

Table 5 SARs Consistency

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- The alleged known threats that will be countered by the TOE
- The organizational security policies that the TOE has to adhere to
- The TOE usage assumptions in the suggested operational environment.

3.1 ASSETS

TOE DATA: Relevant data transmitted or stored in the TOE or between the TOE and the environment.

TOE IDENTITY: TOE attributes that identify the TOE within the operational environment.

EXTERNAL IDENTITY: External entity attributes that identify an external entity from the other.

ACTIONS: Any interaction between a user and the TOE.

AUDIT DATA: Data generated by the TOE that records a history of actions finished or attempted by any subject within the TOE.

CREDENTIAL DATA: A piece of information that assures that a user is who they claim to be or that allows someone to see the information.

TOE's MANAGEMENT FUNCTIONS: Functions that modify environment behavior that needs administrator permissions.

3.2 THREATS TO SECURITY

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers, and the adverse action that materializes the threat.

T.ADMIN_ERROR: An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.

T.EAVES: A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

T.FALSIFY: A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.

T.FORGE: A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.

T. INSUFFATR: An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

T.MASK: A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.

T.RAWCRED: A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.

T.UNAUTH: A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.

T.WEAKIA: A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials

3.3 ORGANIZATIONAL SECURITY POLICIES

The organizational Security policies are defined as follows.

P.BANNER: The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

3.4 ASSUMPTIONS

The assumptions when using the TOE are the following:

A.CRYPTO: The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.

A.ENROLLMENT: There will be a defined enrollment process that confirms user identity before the assignment of credentials.

A.ESM: The TOE will be able to establish connectivity to other ESM products in order to share security data.

A.FEDERATE: Third-party entities that exchange attribute data with the TOE are assumed to be trusted.

A.MANAGE: There will be one or more competent individuals assigned to install, configure, and operate the TOE.

A.ROBUST: The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.

A.SYSTIME: The TOE will receive reliable time data from the Operational Environment.

4 SECURITY OBJECTIVES

The security objectives are high-level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and assumptions. These consist of:

- The security objectives for the operational environment.
- The security objectives for the TOE.

4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives for the TOE must determine (to the desired extent) the TOE's responsibility in countering the threats and in enforcing the Organizational Security Policies(OSP). Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE.

O.ACCESSID: The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.

O.AUDIT: The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.

O.AUTH: The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.

O.BANNER: The TOE will display an advisory warning regarding use of the TOE.

O.EAVES: The TOE will either leverage a third-party cryptographic suite or contain the ability to use cryptographic algorithms to secure the communication channels to and from itself.

O.EXPORT: The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.

O.IDENT: The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.

O.INTEGRITY: The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.

O.MANAGE: The TOE will provide Assignment Managers with the capability to manage the TSF.

O.PROTCOMMS: The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

O.PROTCRED: The TOE will be able to protect stored credentials.

O.SELFID: The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing the OSPs and upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment, to aspects of OSPs to be enforced by the environment and to assumptions to be uphold by the environment.

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.

Application Note: This functionality can be provided by a part of the non-TOE software product.

OE.SYSTIME: The Operational Environment will provide reliable time data to the TOE.

4.3 SECURITY OBJECTIVES RATIONALE

The following table provides a mapping of security objectives, tracing each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective,

and each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective. This illustrates that the security objectives counter all threats, the security objectives enforce all OSPs, and the security objectives for the operational environment uphold all assumptions.

	O.ACCESSID	O.AUDIT	O.AUTH	O.BANNER	O.EAVES	O.EXPORT	O.IDENT	O.INTEGRITY	O.MANAGE	O.PROTCOMMS	O.PROTCRED	O.SELFID	OE.ROBUST	OE.ADMIN	OE.CRYPTO	OE.ENROLLMENT	OE.FEDERATE	OE.INSTALL	OE.MANAGEMEN	OE.PERSON	OE.SYSTIME
T.ADMIN_ERROR									X					X				X		X	
T.EAVES					X	X				X					X						
T.FALSIFY								X		X		X			X						
T.FORGE	X									X					X		X				
T. INSUFFATR							X														
T.MASK		X																			X
T.RAWCRED											X										
T.UNAUTH			X						X	X					X						
T.WEAKIA													X								
P.BANNER				X																	
A.CRYPTO															X						

	O.ACCESSID	O.AUDIT	O.AUTH	O.BANNER	O.EAVES	O.EXPORT	O.IDENT	O.INTEGRITY	O.MANAGE	O.PROTCOMMS	O.PROTCRED	O.SELFID	OE.ROBUST	OE.ADMIN	OE.CRYPTO	OE.ENROLLMENT	OE.FEDERATE	OE.INSTALL	OE.MANAGEMEN	OE.PERSON	OE.SYSTIME
A.ENROLLMENT																X					
A.ESM																			X		
A.FEDERATE																	X				
A.MANAGE														X				X		X	
A.ROBUST													X								
A.SYSTIME																					X

Table 6 Security Objectives vs Security Problem Definition

Figure 2 Mapping of Security Problem Definition to Security Objectives

4.3.1 THREATS

4.3.1.1T.ADMIN_ERROR

O.MANAGE - The TOE will provide Authentication Managers with the capability to manage the TSF.

FMT_MOF.1

FMT_SMF.1

By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior.

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.

This objective requires the TOE to have designated administrators for its operation. This provides some assurance that the TOE will be managed and configured consistently.

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.

This objective reduces the threat of administrative error by ensuring that the TOE is installed in a manner that is consistent with the evaluated configuration.

OE.PERSON - Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.

This objective reduces the threat of administrative error by ensuring that administrators have been properly vetted and trained prior to having access to the TOE.

4.3.1.2T.EAVES

O.PROTCOMMS - The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

FPT_SKP_EXT.1

FTP_ITC.1

FTP_TRP.1

FAU_STG.2

Implementation of trusted channels and paths ensures that communications are protected from eavesdropping.

O.EAVES - The TOE will either leverage a third-party cryptographic suite or contain the ability to use cryptographic algorithms to secure the communication channels to and from itself.

FTP_ITC.1

FTP_TRP.1

Establishing trusted channels and paths for external communications will provide the TOE with reasonable assurance that transmitted data will not be disclosed to or modified by an unauthorized party.

O.EXPORT - The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.

ESM_ICT.1

OE.CRYPTO - The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed.

4.3.1.3T.FALSIFY

O.INTEGRITY - The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.

FTP_ITC.1 If the TSF is able to transmit data in such a way that its integrity can be validated, the risk of it being altered in transit by a malicious agent is reduced.

O.PROTCOMMS - The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

FPT_SKP_EXT.1

FTP_ITC.1

FTP_TRP.1

FAU_STG.2

Implementation of a trusted channel between the TOE and other ESM products ensures that the TOE will securely assert its identity when transmitting data over this channel.

O.SELFID - The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

ESM_EID.2

FTP_ITC.1

By establishing a trusted channel and providing a means for the TSF to validate its own identity to other ESM components, the source of transmitted data can be trusted and the risk of spoofing the TOE is diminished.

OE.CRYPTO - The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed.

4.3.1.4T.FORGE

O.ACCESSID - The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.

FTP_ITC.1

By establishing a trusted channel that provides identification of end points, the TSF is able to assert that any data it may be transmitting will only be going to valid ESM components.

O.PROTCOMMS - The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

FPT_SKP_EXT.1

FTP_ITC.1

FTP_TRP.1

Implementation of a trusted channel between the TOE and other ESM products ensures that the TOE will have a means to verify the identity of external entities that access it.

OE.CRYPTO - The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed.

OE.FEDERATE - Data the TOE exchanges with trusted external entities is trusted.

In the case where the TOE uses external attribute authorities to provide or validate certain attribute data it maintains, the authenticity of these entities must be trusted in order for the data they produce to be trusted.

4.3.1.5T. INSUFFATR

O.IDENT - The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.

ESM_ICD.1

The Identity and Credential Management product must provide the ability to define subject (and optionally object) attributes. These attributes must be sufficient to support use by other ESM products and must be sufficient to support policies defined by Policy Management components. This will ensure that strong policies are created that are capable of using the full set of access control functions of compatible products.

4.3.1.6T.MASK

O.AUDIT - The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.

FAU_GEN.1

FAU_STG.1

If security relevant events are logged and backed up, an attacker will have difficulty performing actions for which they are not accountable. This allows an appropriate authority to be able to review the recorded data and acquire information about attacks on the TOE.

OE.SYSTIME - The TOE will receive reliable time data from the Operational Environment.

This objective helps ensure the accuracy of audit data by providing an accurate record of the timing and sequence of activities that were performed against the TOE.

4.3.1.7T.RAWCRED

O.PROTCRED - The TOE will be able to protect stored credentials.

FPT_APW_EXT.1

The Identity and Credential Management Product must protect stored credentials such that they cannot be accessed in their raw, repayable form.

4.3.1.8T.UNAUTH

O.AUTH - The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.

ESM_EAU.2

ESM_EID.2

FIA_USB.1

FMT_SMR.1

FTP_TRP.1

If the TOE requires all TSF-mediated activities to be performed following authentication via a trusted path and a user is bound to a defined role during authentication, an attacker will be unable to perform unauthenticated actions against the TSF.

O.MANAGE - The TOE will provide Authentication Managers with the capability to manage the TSF.

FMT_MOF.1

FMT_SMF.1

By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior.

O.PROTCOMMS - The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

FTP_ITC.1

FTP_TRP.1

By implementing cryptographic protocols, the TOE is able to prevent the manipulation of data in transit that could lead to unauthorized administration.

OE.CRYPTO - The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed.

4.3.1.9T.WEAKIA

OE.ROBUST - The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.

This objective helps ensure that administrative access to the TOE is robust by externally defining strength of secrets, authentication failure, and session denial functionality that is enforced by the TSF.

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threats	Security Objectives
T.ADMIN_ERROR	O.MANAGE OE.ADMIN OE.INSTALL OE.PERSON
T.EAVES	O.PROTCOMMS O.EAVES O.EXPORT OE.CRYPTO
T.FALSIFY	O.INTEGRITY O.PROTCOMMS O.SELFID OE.CRYPTO
T.FORGE	O.ACCESSID O.PROTCOMMS OE.CRYPTO OE.FEDERATE
T. INSUFFATR	O.IDENT
T.MASK	O.AUDIT OE.SYSTIME
T.RAWCRED	O.PROTCRED

Threats	Security Objectives
T.UNAUTH	O.AUTH O.MANAGE O.PROTCOMMS OE.CRYPTO
T.WEAKIA	OE.ROBUST

Table 7 Threats vs Security Objectives

4.3.2 ORGANIZATIONAL SECURITY POLICIES

4.3.2.1P.BANNER

O.BANNER - The TOE will display an advisory warning regarding use of the TOE.

FTA_TAB.1

The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.

The following table maps the organizational security policies of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

OSPs	Security Objectives
P.BANNER	O.BANNER

Table 8 OSPs vs Security Objectives

4.3.3 ASSUMPTIONS

4.3.3.1A.CRYPTO

OE.CRYPTO - The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.

It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE. If the TOE

provides its own cryptographic primitives, then this becomes an objective for the TOE rather than for the environment.

4.3.3.2A.ENROLLMENT

OE.ENROLLMENT - The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.

NIST SP 800-63 stresses the importance of having a process that confirms an individual's identity before assigning that individual credential. This process is assumed to provide that confirmation.

4.3.3.3A.ESM

OE.MANAGEMENT - The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.

In order for the TOE to establish a connection to other ESM products, these products must already be deployed in the Operational Environment. In particular, an Authentication Server component needs to be in place to consume the identity data provided by the TOE or else the TOE does not provide a benefit to the environment in which it is deployed.

4.3.3.4A.FEDERATE

OE.FEDERATE - – Data the TOE exchanges with trusted external entities is trusted.

If the TOE uses third-party entities (for example, another instance of the same product that is deployed in a different organization) for attribute exchange or validation, such as in a federation, it is necessary to assume that these entities are trusted. They are likely to reside in different networks so an administrator for the TOE will not be able to take direct action to ensure their security.

4.3.3.5A.SYSTIME

OE.SYSTIME - The Operational Environment will provide reliable time data to the TOE.

The TSF is expected to use reliable time data in the creation of its audit records. If the TOE is a software-based product, then it is expected that the TSF will receive this time data from a source within the Operational Environment, such as a system clock or NTP server.

4.3.3.6A.MANAGE

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.

Assigning specific individuals to manage the TSF provides assurance that management activities are being carried out appropriately.

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.

Assigning specific individuals to install the TOE provides assurance that it has been installed in a manner that is consistent with the evaluated configuration.

OE.PERSON - Personnel working as TOE administrators shall be carefully selected and trained for the proper operation of the TOE.

Ensuring that administrative personnel have been vetted and trained helps reduce the risk that they will perform malicious or careless activity.

4.3.3.7A.ROBUST

OE.ROBUST – The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.

The ESM deployment as a whole is expected to provide a login frustration mechanism that reduces the risk of a brute force authentication attack being used successfully against the TSF and defines allowable conditions for authentication (e.g., day, time, location). It is expected that if the TSF does not provide this mechanism, then it will receive this capability from elsewhere in the ESM deployment.

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Assumptions	Security Objectives
A.CRYPTO	OE.CRYPTO
A.ENROLLMENT	OE.ENROLLMENT
A.ESM	OE.MANAGEMENT
A.FEDERATE	OE.FEDERATE
A.MANAGE	OE.ADMIN OE.INSTALL OE.PERSON

Assumptions	Security Objectives
A.ROBUST	OE.ROBUST
A.SYSTIME	OE.SYSTIME

Table 9 Assumptions vs Security Objectives for the Operational Environment

5 EXTENDED COMPONENTS DEFINITION

The PP provides a definition for the extended components required [PP-ESM-I-CM]. This section lists the references to the extended components definitions compliance by the ST.

- ESM_EAU.2 component at Section 5.1.2 from [PP-ESM-I-CM]
- ESM_EID.2 component at Section 5.1.3 from [PP-ESM-I-CM]
- ESM_ICD.1 component at Section 5.1.4 from [PP-ESM-I-CM]
- ESM_ICT.1 component at Section 5.1.5 from [PP-ESM-I-CM]
- FAU_STG_EXT.1 component at Section 5.2 from [PP-ESM-I-CM] is covered by FAU_STG.1 and FAU_STG.2 from [CC:2022]
- FPT_APW_EXT.1 component at Section 5.4.1 from [PP-ESM-I-CM]
- FPT_SKP_EXT.1 component at Section 5.4.2 from [PP-ESM-I-CM]

6 SECURITY REQUIREMENTS

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration, and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word "assignment" is maintained, and the resolution is presented in ***boldface, italic, and blue color.***
- Selections. They appear between square brackets. The word "selection" is maintained, and the resolution is presented in ***boldface, italic, and blue color.***
- Iterations. It includes "/" and an "identifier" following the requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.
- Refinements: the text where the refinement has been done is shown ***in bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

The refinements already performed in PP_ESM_ICM are not identified (e.g., highlighted) here; rather the refined requirements have been copied from PP_ESM_ICM and any residual operations have been completed herein.

6.1 SECURITY FUNCTIONAL REQUIREMENTS

6.1.1 ESM: ENTERPRISE SECURITY MANAGEMENT

6.1.1.1ESM_EAU.2: RELIANCE ON ENTERPRISE AUTHENTICATION

ESM_EAU.2.1 The TSF shall rely on ***[selection: [assignment: LDAP, Active Directory]]*** for subject authentication.

ESM_EAU2.2 The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.2 ESM_EID.2: RELIANCE ON ENTERPRISE IDENTIFICATION

ESM_EID.2.1 The TSF shall rely on ***[selection: [assignment: LDAP, 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.

6.1.1.3ESM_ICD.1: IDENTITY AND CREDENTIAL DEFINITION

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, ***[assignment: user ID, user name, first name, last name, password, email]***.

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:

a) For password-based credentials, the following rules apply:
    1. Passwords shall be able to be composed of a subset of the following character sets: ***[assignment: English character set, numbers, special characters]*** that include the following values ***[assignment: a-z, A-Z, 0-9, "!", "@", "#", "$", "%", "^", "&", "*", "-", "_"]***; and
    2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

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

Application Note: In the statement of ESM_IDC.1.8 above, the term "administrator" refers to both *Admin* and *Administrator* roles, as defined in FMT_SMR.1.

6.1.1.4ESM_ICT.1 IDENTITY AND CREDENTIAL TRANSMISSION

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

6.1.2 FAU: SECURITY AUDIT

6.1.2.1FAU_GEN.1: AUDIT DATA GENERATION

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

a) Start-up and shutdown of the audit functions;

b) All auditable events ***identified in Table 10 TOE Auditable Events*** for the ***[selection: not specified]*** level of audit;

c) ***[assignment: no other auditable events]***.

Component	Event	Additional Information
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)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted

Component	Event	Additional Information
FAU_STG.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

Table 10 TOE Auditable Events

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, ***[assignment: no other audit relevant information]***.

6.1.2.2 FAU_STG.1 SECURITY AUDIT DATA STORAGE

FAU_STG.1.1 The TSF shall be able to store the generated audit data on the ***[assignment: TOE itself, transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC].***

6.1.2.3 FAU_STG.2 PROTECTED AUDIT DATA STORAGE

FAU_STG.2.1 The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to ***[selection, choose one of: prevent, detect]*** unauthorized modifications to the stored audit data in the audit trail.

6.1.3 FIA: IDENTIFICATION AND AUTHENTICATION

6.1.3.1FIA_USB.1: USER-SUBJECT BINDING

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: ***[assignment: user's assigned role that regulates permissions to access objects]***.

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: ***[assignment: all users are assigned to role "Everyone"]***.

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: ***[assignment: any change is reflected immediately]***.

6.1.4 FMT: SECURITY MANAGEMENT

6.1.4.1FMT_MOF.1: MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR

FMT_MOF.1.1 The TSF shall restrict the ability to ***[selection: determine the behavior of, disable, enable, modify the behavior of]*** the functions ***[assignment: specified in Table 11 Manage Functions per Role]*** to ***[assignment: specified roles]***.

Role	Management Functions
Admin, Administrator*	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF) **** Administrator role is not allowed to manage authentication data of Admin role***
Admin, Administrator*	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.) **** Identity and credential data for Admin role is defined upon TOE installation and can later be modified by Admin role only (not accessible to Administrators)***
Admin, Administrator*	Management of credential status **** Management of credential status for Admin role is under the exclusive control of said Admin role (not accessible to Administrators)***
Admin, Administrator	Enrollment of users
Admin, Administrator	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed
Admin, Administrator	Configuration of auditable events
Admin	Configuration of external audit storage location
Admin, Administrator	Management of the threshold for unsuccessful authentication attempts

Role	Management Functions
Admin, Administrator	Management of actions to be taken in the event of an authentication failure
Admin, Administrator	Management of the metric used to verify secrets
Admin, Administrator*	Definition of default subject security attributes, modification of subject security attributes **** Security attributes for Admin role are under the exclusive control of said Admin role (not accessible to Administrators)***
Admin, Administrator*	Management of sets of users that can interact with security functions **** The set of users with access to security functions reserved to the Admin role is fixed (i.e.: to the individual user initially associated to the Admin role during TOE installation)***
Admin, Administrator*	Management of the users that belong to a particular role **** The set of users belonging to the Admin role is fixed (i.e.: to the individual user initially associated to the Admin role during TOE installation)***
Admin, Administrator	Configuration of the inactivity period for session termination
Admin	Maintenance of the banner

Table 11 Manage Functions per Role

6.1.4.2FMT_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[assignment: specified in Table 12 TOE Management Functions]***.

Requirement	Management Activities
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities
ESM_EID.2	Management of identity data for both interactive users and authorized IT entities
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)

Requirement	Management Activities
ESM_ICD.1	Management of credential status
ESM_ICD.1	Enrollment of users into the repository
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data is performed
FAU_STG.1	Configuration of external audit storage location
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF.1	Management of sets of users that can interact with security functions
FMT_SMR.1	Management of the users that belong to a particular role
FTA_TAB.1	Maintenance of the banner

Table 12 TOE Management Functions

6.1.4.3FMT_SMR.1: SECURITY ROLES

FMT_SMR.1.1 The TSF shall maintain the roles ***[assignment: Admin, Administrator]***.

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

Application Note: TOE able to manage other types of roles, but these are the roles with management permissions on the TSF.

Application Note: The term *Administrative Entity* is used to refer collectively to both *Admin* and *Administrator* roles. This means that any statements about *Administrative Entity* are applicable to both *Admin* and *Administrator* roles.

6.1.5 FTA: TOE ACCESS

6.1.5.1FTA_TAB.1: DEFAULT TOE ACCESS BANNERS

FTA_TAB.1.1 Before establishing a user session, the ***[selection: TSF]*** shall display a~~n~~ ***[assignment: configurable advisory warning message regarding unauthorized use of the TOE]*** ~~***message***~~.

6.1.6 FTP: TRUSTED PATH/CHANNELS

6.1.6.1FTP_ITC.1: INTER-TSF TRUSTED CHANNEL

FTP_ITC.1.1 The TSF shall ***use [assignment: TLS, HTTPS] to*** provide a ***trusted*** communication channel between itself and ***authorized IT entities ~~another trusted IT product~~*** that is logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification **and ~~or~~** disclosure.

FTP_ITC.1.2 The TSF shall permit ***[selection: Management Console, MyAccount portal, API]*** 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***, ***[assignment: authentication using external authentication servers, provisioning to external entities, transfer of audit data]***.

6.1.6.2FTP_TRP.1: TRUSTED PATH

FTP_TRP.1.1 The TSF shall ***use [selection: TLS, HTTPS] to*** provide a communication path between itself and ***[selection: remote]*** users that is logically distinct from other communication **channels ~~paths~~** and provides assured identification of its end points and protection of the communicated data from ***[selection: modification, disclosure]***.

FTP_TRP.1.2 The TSF shall permit ***[selection: remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[selection: initial user authentication, [assignment: execution of management functions]]***.

Application note: The cipher suites TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, as well as the digital signature mechanism RSA PKCS#1 v1.5, are supported by the TOE but are legacy until December 31, 2031 with European Union Agency for Cybersecurity (ENISA) Agreed Cryptographic Mechanisms, Version 2.0 [ACM].

6.1.7 FPT: PROTECTION OF THE TSF

6.1.7.1FPT_APW_EXT.1 PROTECTION OF STORED CREDENTIALS

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.

6.1.7.2FPT_SKP_EXT.1 PROTECTION OF SECRET KEY PARAMETERS

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

6.2 SECURITY ASSURANCE REQUIREMENTS

The development and evaluation of the TOE shall be done in accordance with the following security assurance requirements: **EAL1 + ASE_SPD.1 + ASE_OBJ.2**

The following table shows the assurance requirements by referencing the individual components in [CC2022R1P3]

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_REQ.1: Stated security requirements ASE_TSS.1: TOE summary specification ASE_SPD.1: Security problem definition ASE_OBJ.2: Security objectives
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE ALC_CMS.1: TOE CM coverage
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 13 Security Assurance Requirements

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 NECESSITY AND SUFFICIENCY ANALYSIS

Information of the rationale of security functional requirements and TOE security objective in Threats.

SFR / TOE Security Objective	O.ACCESSID	O.AUDIT	O.AUTH	O.BANNER	O.EXPORT	O.IDENT	O.INTEGRITY	O.MANAGE	O.PROTCOM	O.PROTCRED	O.SELFID
ESM_EAU.2			X								
ESM_EID.2			X								X
ESM_ICD.1						X					
ESM_ICT.1					X						
FAU_GEN.1		X									
FAU_STG.1		X									
FAU_STG.2									X		
FIA_USB.1			X								
FMT_MOF.1								X			
FMT_SMF.1								X			
FMT_SMR.1			X								
FPT_APW_EXT.1										X	
FPT_SKP_EXT.1									X		
FTA_TAB.1				X							

SFR / TOE Security Objective	O.ACCESSID	O.AUDIT	O.AUTH	O.BANNER	O.EXPORT	O.IDENT	O.INTEGRITY	O.MANAGE	O.PROTCOM	O.PROTCRED	O.SELFID
FTP_ITC.1	X						X		X		X
FTP_TRP.1			X						X		

Table 14 SFRs / TOE Security Objectives coverage

6.3.2 SECURITY REQUIREMENT SUFFICIENCY

6.3.3 SFR DEPENDENCY RATIONALE

6.3.3.1TABLE OF SFR DEPENDENCIES

The following table lists the dependencies for each requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
ESM_EAU.2	ESM_EID.2	ESM_EID.2	None
ESM_EID.2	None	None	None
ESM_ICD.1	None	None	None
ESM_ICT.1	ESM_ICD.1	ESM_ICD.1	None
FAU_GEN.1	FPT_STM.1	None	FPT_STM.1
FAU_STG.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1	None
FAU_STG.2	FAU_GEN.1	FAU_GEN.1	None
FIA_USB.1	FIA_ATD.1	None	FIA_ATD.1

SFR	Required	Fulfilled	Missing
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	None	FIA_UID.1
FPT_APW_EXT.1	None	None	None
FPT_SKP_EXT.1	None	None	None
FTA_TAB.1	None	None	None
FTP_ITC.1	None	None	None
FTP_TRP.1	None	None	None

Table 15 SFR Dependencies

6.3.3.2JUSTIFICATION FOR MISSING DEPENDENCIES

FAU_GEN.1 dependency on FPT_STM.1

This SFR is an unfulfilled dependency on FAU_GEN.1. It has not been included because the TOE is not necessarily expected to include its own system clock. The host operating system is the source for system time. OE.SYSTIME satisfies this dependency.

FIA_USB.1 dependency on FIA_ATD.1

This SFR is an unfulfilled dependency on FIA_USB.1. It has not been included because ESM_ICD.1 is expected to satisfy the dependency in the same manner.

FMT_SMR.1 dependency on FIA_UID.1

This SFR is an unfulfilled dependency on FMT_SMR.1. ESM_EID.2 satisfies this dependency by providing equivalent functionality.

6.3.4 SAR DEPENDENCY RATIONALE

6.3.4.1TABLE OF SAR DEPENDENCIES

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.1	ASE_ECD.1	ASE_ECD.1	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	None
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1	None
ALC_CMS.1	None	None	None
ADV_FSP.1	None	None	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1	None
AGD_PRE.1	None	None	None
ATE_IND.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	None
AVA_VAN.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	None
ASE_SPD.1	None	None	None

Table 16 SAR dependencies

7 TOE SUMMARY SPECIFICATION

This chapter describes the security functions:

- Enterprise Security Management
- Security Audit
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

7.1 ENTERPRISE SECURITY MANAGEMENT

The TOE requires components that perform centralized identification, authentication, and access control. In order to do this, entity data and transmission of such data to other entities is needed.

For authentication and identification of entities, TOE stores relevant attributes in repositories. The TOE supports different databases as repositories to store attributes, users, roles, and permissions. Users are stored in a repository (user store). Another repository will be used to store roles and permissions. An LDAP or an Active Directory will be used to delegate the authentication to the operational environment.

The Identity Server is capable of defining usernames and passwords, which can then be used on other ESM products. Usernames are forced to be unique therefore users are uniquely identified.

(ESM_EAU.2, ESM_EID.2)

Apart from the username, TOE allows the configuration of multiple attributes as the login identifier and several emails for just one user. Nevertheless, there is only one password per user. The TOE allows to lock accounts. When an account is locked, the user will not be able to access any system with his credential. In addition, accounts state can be enabled with lock reasons. These attributes can be configured at "Attributes and Stores > Attributes" searching for "Account State" and "Locked Reason". Editing them to be displayed at user's profile and to be read-only will serve the Administrative Entity to view the status of the account and therefore the credential status.

In conjunction with the above, the Administrative Entity has to consult the Password Expiring User Identification Rest API to retrieve a list with the accounts that have their password expired. This is done by a GET operation to https://{serverUrl}/t/{tenantDomain}/api/server/v1/password-expired-users.

The Identity Server is capable of updating a user's credentials when another external authorized service requests to do so. By default, when setting passwords, the application supports the English character set, including a-z, A-Z, 0-9, "!", "@", "#", "%", "&", "*", "-" and "_". Forcing a minimum

password length of 15 characters can be achieved through configuration, by using regular expressions. Through the same path, Administrative Entities can set rules for password composition (types of characters and the number of each type). Administrative Entities can also configure the number of password changes that must take place before allowing to reuse one.

Whenever a user creation/update is done by a Service Provider (external entity), credential user data is received by the Inbound Provisioning component. This data is forwarded to the user store where the latest information of the users is stored.

(ESM_ICD.1)

The Identity Server is capable of transmitting identity and credential data to external authorized components through the User Store Manager. This process takes place when users are created/modified through the TOE.

(ESM_ICT.1)

7.2 SECURITY AUDIT

The TOE generates logs for security events, including the events specified in Table 10 TOE Auditable Events.

TOE records audit logs for the following events:

- Application – Logs addition, update or deletion of any application from system.
- Login - Logs an authentication event, login and logout to server or application.
- Session - Logs update, store and termination.
- Identity Provider - Logs addition, updating and deletion of an identity provider to/in the system
- Claim Management – Logs related to claim dialect, local and external claims management.
- Group/Role – Logs addition, update, deletion of a group or role. Also logs the action of retrieval of users of a role.
- User – Logs addition, deletion and update or retrieval of the attributes of a user, retrieve the list of users and roles of a user. Also logs lock and unlock events and events on passwords, such as recover, reset or changes by user or Administrative Entity.
- Remote Log – logs action on the configuration of the remote audit logging server

By default, logs are stored locally, configured in the log4j2.properties file. This storage fulfills half of the requirement that claims that logs shall be protected from unauthorized deletion or modification. Only authorized users who have access to the file system can delete and modify them, but the TOE does not provide any functionality to perform modifications or deletions directly.

Log records include the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

(FAU_GEN.1)

Moreover, Identity Server allows the Admin role to store audit logs on an external server. This is achieved by connecting the TOE with a reachable log storage solution over the network by using a HTTPS protocol (protected by TLS).

If the connection to the remote repository is lost, audit logs are not discarded. Instead, they are persistently stored locally on disk using a queue mechanism to prevent data loss. Once the connection is re-established, the queued logs are automatically transmitted to the remote server. System warnings are generated during connection loss, high disk usage, and upon successful reconnection to keep Administrative Entities informed.

(FAU_STG.1, FAU_STG.2)

7.3 IDENTIFICATION AND AUTHENTICATION

The TOE associates security attributes to users with access to management functionality (these users are known as Administrative Entities). Security attributes are parameters used to take decisions on whether granting access to a resource or not. A TOE user is given Administrator role during initial assignment or via update of user attributes. Administrative Entities are the only ones that can add or delete roles from users. Owner account (the original account created when installing the TOE) cannot be revoked from Admin role.

The TOE associates “user role” and “user store” with these users. Both attributes are always defined when creating a user and, when it is modified both are forced to be set.

(FIA_USB.1)

7.4 SECURITY MANAGEMENT

The TOE provides the management functions identified in the ESMICM PP; maintains roles and restricts access to the functions.

The TOE restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the management functions as defined in Table 11 Manage Functions per Role, only an Administrative Entity can interact with the behavior of management functions identified in Table 12 TOE Management Functions.

(FMT_MOF.1, FMT_SMF.1)

The security roles identified by the TOE are Admin and Administrator. There exists “Everyone” role with no permission associated; this role is associated with all accounts automatically.

(FMT_SMR.1)

7.5 PROTECTION OF THE TSF

Credentials and keys used by the TOE are protected from disclosure. Most credentials are securely stored in user stores. Some credentials, such as the Admin password and keystore password, are stored in configuration files. Sensitive parameters (passwords) are hashed by using the Secure Vault implementation built into the WSO2 Identity Server. The keys generated for the keystore are RSA-3072. The public key of the keystore is used for the encryption of the password at configuration files.

(FPT_APW_EXT.1)

Pre-shared keys, symmetric keys, and private keys are stored in key stores and trust stores, which are repositories protected by a password. The keys used for encryption done in the keystore and in the truststore are RSA-3072.

(FPT_SKP_EXT.1)

7.6 TOE ACCESS

It is possible to configure to display a banner with an advisory warning message regarding the unauthorized management of the Identity Server before establishing an administrative session. Only the Admin role has access to this configuration.

(FTA_TAB.1)

7.7 TRUSTED PATH/CHANNELS

Identity Server provides communication with authorized IT entities through trusted communication channels using TLS and HTTPS. An Administrative Entity can configure the desired cipher suites for each of the established communications.

The cipher suites used for all communication channels are listed below:

Ciphers Suites	
TLS 1.3	TLS_AES_128_GCM_SHA256
	TLS_AES_256_GCM_SHA384
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Table 17 Allowed Cipher Suites

The TOE establishes several trusted communication channels to protect data in transit between the TOE and external entities. Each trusted channel is implemented using specific third-party libraries,

which rely on the cryptographic mechanisms provided by the Oracle Java JDK 17.0.2, specifically the SunJSSE and SunJCE providers.

The mapping between the trusted channels and the libraries used for their protection is as follows:

HTTPS (port 443)

- Inbound connections are handled by Apache Tomcat 9.0.82, which acts as the HTTPS servlet container for the management console, user portal, and REST/OAuth2/SAML/SCIM/OIDC API endpoints.
- Outbound connections are established via Apache HTTP Client 4.5.13, Apache Oltu OAuth 2.0 Client 1.0.0, and java.net.URLConnection (JRE-provided). These components handle SCIM/REST provisioning, third-party SaaS integrations, OAuth2 and federated login flows, and audit log transmission, among others.
- All HTTPS communications use SunJSSE for the TLS layer, which in turn uses SunJCE for the underlying cryptographic operations.

LDAP over StartTLS (port 389) and LDAPS (port 636)

- Managed through Java JNDI (JRE-provided). Used for secure directory communication with external LDAP servers (e.g., Active Directory, OpenLDAP) for user authentication, provisioning, and attribute retrieval, among others.
- Uses SunJSSE for encrypted communications capabilities, which internally uses SunJCE for all cryptographic implementations.

SMTP with StartTLS (port 587) or SSL/TLS (port 465)

- Implemented using javax.mail 1.4.1 (bundled in Axiom 1.2.11-wso2v16). Used for secure outbound email delivery (MFA, account recovery, and user invitations, among others).
- Uses SunJSSE for encrypted communications capabilities, which internally uses SunJCE for all cryptographic implementations.

JDBC (port 3306)

- Managed using Tomcat JDBC Connection Pool 9.0.65 for secure database communication.
- Encryption capabilities rely on the database driver and the SunJSSE/SunJCE libraries of the JDK 17 when TLS is used.

(FTP_ITC.1)

Communication with remote users takes place through HTTPS. These communications are started by remote users sending a request. Both remote user authentication and management actions can only take place through the Management Console or through the API. These two interfaces are only accessible through HTTPS.

(FTP_TRP.1)

8 ANNEX A: SECURIY UPDATES APPLIED

The following table lists known vulnerabilities and advisories identified for WSO2 Identity Server 7.0.0 and the corresponding updates applied using the WSO2 Update Tool. This provides a clear record of which updates have been applied to maintain the security of the product.

Steps for applying and verifying updates are described in [AGD-PRE] section 2.1.

CVE or Advisory	Update	Advisory
CVE-2024-3511	8	"Security Advisory WSO2-2024-2702/CVE-2024-3511" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-4457	15	"Security Advisory WSO2-2023-3084/CVE-2024-4457" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-4412	15	"Security Advisory WSO2-2023-3098/CVE-2024-4412" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-8008	69	"Security Advisory WSO2-2024-3178/CVE-2024-8008" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-2323	35	"Security Advisory WSO2-2024-3217/CVE-2024-2323" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-5139	64	"Security Advisory WSO2-2024-3382/CVE-2024-5139" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-5617	33	"Security Advisory WSO2-2024-3414/CVE-2024-5617" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-5563	37	"Security Advisory WSO2-2024-3436/CVE-2024-5563" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-7478	67	"Security Advisory WSO2-2024-3606/CVE-2024-7478" section in the WSO2 Identity Server Documentation (PDF)

CVE or Advisory	Update	Advisory
CVE-2025-0326	85	"Security Advisory WSO2-2025-3857/CVE-2025-0326" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-6429	48	"Security Advisory WSO2-2024-3490/CVE-2024-6429" section in the WSO2 Identity Server Documentation (PDF)
CVE-2025-0209	87	"Security Advisory WSO2-2025-3902/CVE-2025-0209" section in the WSO2 Identity Server Documentation (PDF)
CVE-2025-0663	88	"Security Advisory WSO2-2025-3864/CVE-2025-0663" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-7103	64	"SECURITY ADVISORY WSO2-2024-3425/CVE-2024-7103" section the in WSO2 Identity Server Documentation (PDF)
CVE-2024-6914	56	"SECURITY ADVISORY WSO2-2024-3561/CVE-2024-6914" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-7073	59	"SECURITY ADVISORY WSO2-2024-3562/CVE-2024-7073" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-7096	60	"SECURITY ADVISORY WSO2-2024-3573/CVE-2024-7096" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-7097	60	"SECURITY ADVISORY WSO2-2024-3574/CVE-2024-7097" section in the WSO2 Identity Server Documentation (PDF)
WSO2-2023-2972	74	"SECURITY ADVISORY WSO2-2023-2972" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-3509	9	"SECURITY ADVISORY WSO2-2024-2701/CVE-2024-3509" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-1440	30	"SECURITY ADVISORY WSO2-2024-3171/CVE-2024-1440" section in the WSO2 Identity Server Documentation (PDF)
CVE-2024-7487	65	"SECURITY ADVISORY WSO2-2024-3348/CVE-2024-7487" section in the WSO2 Identity Server Documentation (PDF)

CVE or Advisory	Update	Advisory
WSO2-2025-3302	N/A	"Security Advisory WSO2-2025-3302" section in the WSO2 Identity Server Documentation (PDF) Updating the product is not required, since this is not a vulnerability of the product or the default configuration.

9 ACRONYMS

The following table shows the acronyms used in this document.

Acronym	Meaning
PP	Protection Profile
CC	Common Criteria
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFi	TSF Interface
OSP	Organizational Security Policies
EAL	Evaluation Assurance Level
ST	Security Target
IT	Information Technology
ESMICM PP	Enterprise Security Management Identity and Credential Management

Table 18 Abbreviations

10 GLOSSARY OF TERMS

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance

Table 19 Glossary of terms

11 DOCUMENT REFERENCES

The following table shows the acronyms used in this document.

Reference	Document
[CC:2022]	Common Criteria for Information Technology Security Evaluation
[CC2022R1P2]	Common Criteria for Information Technology Security Evaluation, Revision 1, Part 2: Security functional components
[CC2022R1P3]	Common Criteria for Information Technology Security Evaluation, Revision 1, Part 3: Security assurance components
[CEM2022R1]	Common Criteria Evaluation methodology, Revision 1
[PP-ESM-I-CM]	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013
[ACM]	European Union Agency for Cybersecurity (ENISA), Agreed Cryptographic Mechanisms, Version 2.0, April 2025.
[AGD-PRE]	WSO2 Identity Server Preparative Procedures, Version 1.6
[AGD-OPE]	WSO2 Identity Server Operational User Guidance, Version 1.5

Table 20 List of document references