One Identity Manager 8.1.5

Common Criteria Supplemental Admin Guidance

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Common Criteria Supplemental Admin Guidance
Updated - 14 December 2021, 14:20
Version - 8.1.5

Contents

1

Introduction

With One Identity Manager you can mitigate risk, secure data, meet uptime requirements and satisfy compliance by giving your users access to data and applications they need and nothing more. Now, identity and access management (IAM) can be driven by business needs, not IT capabilities. With One Identity Manager you can unify information security policies and meet governance needs — today and into the future.

About this guide

This guide is intended for administrators responsible for installing, configuring, and/or operating One Identity Manager.

Guidance provided in this document allows you to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the Common Criteria evaluation.

You are expected to be familiar with the security target for One Identity Manager and the general Common Criteria terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the security target document and provides instructions for how to perform the security functions that are defined by these SFRs.

Configuration prerequisites

You must meet the following prerequisites.

Enabling FIPS mode

You do not need to make any settings in One Identity Manager itself for using One Identity Manager native components or One Identity Manager in conjunction with SecureBlackbox as part of the Unix connector for synchronizing and provisioning to Unix system.

One Identity Manager as well as the SecureBlackBox component use the cryptographic settings of the underlying Windows operating system.

For steps to enable FIPS-compliant cryptographic setting on the Windows operating system, refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation.

Basic steps for enabling FIPS mode on Microsoft Windowsoperating systems as stated in the referenced article are:

1. Run `gpedit.msc`.
2. Navigate to **Computer Configuration** | **Windows Settings** | **Security Settings** | **Local Policies** | **Security Options**
3. Set the value of **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** to **Enabled**.

DISCLAIMER: The use of other cryptographic engines was neither evaluated nor tested during the Common Criteria evaluation of One Identity Manager.

Information on permission groups

The attached Microsoft Excel spreadsheet `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx` contains all information about default permission groups and the permissions they grant to user and account data in One Identity Manager.

The columns on the worksheets have the following meaning:

- **CanSee**: Anybody with that permissions can see the data.
- **CanInsert**: Anybody with that permissions can create new record.

- **CanEdit**: Anybody with that permissions can edit the data.
- **CanDelete**: Anybody with that permissions can delete a record.

For more information, refer to the *One Identity Manager Authorization and Authentication Guide* chapters *One Identity Manager Application roles*, *Granting One Identity Manager schema permissions* and *Managing permissions to program features*.

NOTE: If you have problems opening the attached Microsoft Excel spreadsheet `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`, you may perform the following actions:

- Upgrade your PDF reader software to a version that supports attachments.
- If you are a customer of One Identity, you can use the configuration user interface **Designer** to see the same information as provided with the spreadsheet. Follow the steps as described in the *One Identity Manager Authorization and Authentication Guide* chapter *Displaying permissions for tables* (https://support.oneidentity.com/de-de/technical-documents/identity-manager/8.1.5/authorization-and-authentication-guide/13#TOPIC-1250052).
- Contact the One Identity support team (https://support.oneidentity.com).

4

Reliance on enterprise authentication (ESM_EAU.2)

To perform any management functions, users must authenticate against One Identity Manager, regardless of the management interface being used. One Identity Manager supports different types of authentication modules, which are described in more detail in the *One Identity Manager Authorization and Authentication Guide* in chapter *One Identity Manager Authentication modules*.

In order to rely on Active Directory as enterprise authentication only, as described in the Security Target, you need to select one of the following authentication methods in the login screen of One Identity Manager as those are the authentication methods using Active Directory credentials for the login to One Identity Manager:

- Active Directory user account (role-based)
- Active Directory user account (manual input/role-based)
- Active Directory user account
- Active Directory user account (manual input)
- User account
- User account (role-based)

NOTE: As stated in the *One Identity Manager Authorization and Authentication Guide*, the main differences between those authentication modules are:

- The authentication modules starting with **Active Directory...** require the Active Directory to be synchronized with One Identity Manager and the authentication module will lookup that information for identifying the logged in identity.
- The authentication module **User account (role-based)** will lookup a reference to the currently logged in Active Directory user in the **Person** table that stores the identities within One Identity Manager.
- The authentication module **User account** will lookup a reference to the currently logged in **Active Directory** user in the **DialogUser** table that stores the One Identity Manager internal user accounts.

One Identity Manager can be configured to allow/disallow specific authentication methods for the product as a whole, or it can be configured to allow/disallow different methods for individual management interfaces.

For more information, refer to the *One Identity Manager Authorization and Authentication Guide* chapters *Enabling authentication modules* and *Disabling or enabling authentication modules for applications*.

By default, the Web Portal uses the following authentication modules:

- **Active Directory user account (role-based)**: Primary authentication module using windows identity-based single sign-on
- **Employee (role-based)**: Alternative authentication module used as fallback if the single sign-on authentication fails

The **Employee (role-based)** authentication method MUST be disabled for the product to be in its evaluated configuration.

In order to rely only on Active Directory as enterprise authentication for the Web Portal, reconfigure the alternative authentication module to be either set to **Active Directory user account (manual input/role-based)** or **None**. For more information, refer to the *One Identity Manager Installation Guide* chapters *Configuring the Web Portal* and *Authentication data for the web application*.

Other authentication methods for the Web Portal MUST be disabled for the product to be in its evaluated configuration.

5

Identity and credential definition (ESM_ICD.1)

User data is mainly stored in the **Person** table. The configuration of enterprise user data is described in the *One Identity Manager Identity Management Base Module Administration Guide* in chapter *Employee administration*.

Users can be created using Manager (see the *One Identity Manager Identity Management Base Module Administration Guide* chapter *Entering employee master data*) and the Web Portal (see the *One Identity Manager Web Portal User Guide* chapter *Adding employees*). User data can also be created from external systems by means of synchronization and using the automatic employee assignment.

For the automatic employee assignment, you first have to link the users of the connected target system to the employees in One Identity Manager as described in the *One Identity Manager Administration Guide for Connecting to Active Directory* in chapter *Linking user accounts to employees*. For more information regarding automatic employee assignment, refer to the *One Identity Manager Administration Guide for Connecting to Active Directory* chapter *Automatic assignment of employees to Active Directory user accounts*.

The status of user credentials can be viewed and edited using Manager and the Web Portal. For more information, refer to the following manuals:

- Manager: *One Identity Manager Identity Management Base Module Administration Guide* chapter *Entering employee master data*.
- Web Portal: *One Identity Manager Web Portal User Guide* chapter *Editing employee data*

The password of a user a can be reset using:

- Manager by changing the password in the user's master data (see *One Identity Manager Identity Management Base Module Administration Guide* chapters *Entering employee master data* and *Miscellaneous employee master data*)
- the Password Reset Portal by logging in to the Password Reset Portal using a passcode and changing the password (see *One Identity Manager Web Portal User Guide* chapter *Change password*)

Defining password policies is described in the *One Identity Manager Identity Management Base Module Administration Guide* in chapter *Password policies for employees*.

Identity and credential transmission (ESM_ICT.1)

This chapter describes how to set up a connection to specific external systems/endpoints.

NOTE: If the setup of a trusted channel for a system/endpoint is not mentioned here, the underlying API uses a secure channel by default.

Active Directory

Enable SSL and configure the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to Active Directory* in chapter *Creating a synchronization project for initial synchronization of an Active Directory domain*.

Unix/Linux

The connector always uses SSH to connect to the Unix host. Configure the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to Unix Based Target Systems* in chapter *Creating a synchronization project for initial synchronization of a Unix host*.

Exchange 2010, 2013, 2016

Enable **Use SSL** and configure the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to Microsoft Exchange* in chapter *Creating a synchronization project for initial synchronization of a Microsoft Exchange environment*.

SharePoint 2010, 2013, 2016

Configure the connection to the SharePoint farm and the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to SharePoint* in chapter *Creating a synchronization project for initial synchronization of a SharePoint farm*.

Azure Active Directory

Configure the connection to the Azure Active Directory client and the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to Azure Active Directory* in chapter *Creating a synchronization project for initial synchronization of an Azure Active Directory tenant*.

Exchange Online

Configure the connection to the Exchange Online environment and the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to Exchange Online* in chapter *Creating a synchronization project for initial synchronization of an Exchange Online environment*.

SharePoint Online

Configure the connection to the SharePoint Online tenant and the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to SharePoint Online* in chapter *Preparing a remote connection server for access to the SharePoint Online tenant*.

Google G-Suite

Configure the connection to G Suite and the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to G Suite* in chapter *Creating a synchronization project for initial synchronization of G Suite*.

LDAP

Enable SSL/TLS in the additional settings and configure the schedule to synchronize regularly as described in the *One Identity Manager Administration Guide for Connecting to LDAP* in chapter *Creating a synchronization project for initial synchronization of a LDAP domain*.

Mainframe CA ACF2

The connector accesses the target system via LDAP. To ensure a secure channel is used, configure the connection to use SSL as described in *One Identity Manager LDAP Connector for CA ACF2 Reference Guide* in chapter *Initializing and configuring the LDAP connector for CA ACF2*.

The connector does not come with pre-defined mappings for identity or credential data. Therefore, One Identity Manager is not responsible for the transmitted data. You may create a mapping as described in the *One Identity Manager LDAP Connector for CA ACF2 Reference Guide* in chapter *User mapping information*.

Mainframe IBM RACF

The connector accesses the target system via LDAP. To ensure a secure channel is used, configure the connection to use SSL as described in the *One Identity Manager LDAP*

Connector for IBM RACF Reference Guide in chapter *How to initialize and configure the RACF LDAP connector*.

The connector does not come with pre-defined mappings for identity or credential data. Therefore, One Identity Manager is not responsible for the transmitted data. You may create a mapping as described in *One Identity Manager LDAP Connector for IBM RACF Reference Guide* in the following chapters:

- *User mapping information*
- *Group mapping information*
- *Data set profile mapping information*

Mainframe IBM AS/400

Enable SSL and configure the connection accordingly as described in the *One Identity Manager LDAP Connector for IBM AS/400 Reference Guide* in chapter *How to initialize and configure the AS/400 LDAP connector*.

The connector does not come with pre-defined mappings for identity or credential data. Therefore, One Identity Manager is not responsible for the transmitted data. You may create a mapping as described in *One Identity Manager LDAP Connector for IBM AS/400 Reference Guide* in the following chapters:

- *User mapping information*
- *Group mapping information*

Mainframe CA Top Secret

Enable SSL and configure the connection accordingly as described in the *One Identity Manager LDAP Connector for CA Top Secret Reference Guide* in chapter *How to initialize and configure the AS/400 LDAP connector*.

The connector does not come with pre-defined mappings for identity or credential data. Therefore, One Identity Manager is not responsible for the transmitted data. You may create a mapping as described in the *One Identity Manager LDAP Connector for CA Top Secret Reference Guide* in the following chapters:

- *User mapping information*
- *Group mapping information*
- *Profile mapping information*

Not evaluated connectors

The following connectors provided by One Identity Manager have not been included within the evaluation:

- Generic connectors:
    - SCIMv2
    - ADO.NET, OLEDB, ODBC

    - Structured files (CSV, tab-separated, etc.)
    - PowerShell
- Connectors incl. a connected systems module
    - IBM Notes
    - SAP R/3 and SAP S/4HANA
    - Oracle E-Business Suite

Note that regardless of not being part of the evaluation all connectors will support secured communications if the target systems support such communication channels.

Audit data generation (FAU_GEN.1)

NOTE: Audit functions are running whenever One Identity Manager is running. The audit function does not start up and shut down separately from One Identity Manager.

By default, not all auditable events result in the generation of audit records. To enable all required auditing, the following steps must be performed:

- Log One Identity Manager logins and logouts: In Designer, activate the **Common** | **Journal** | **LoginAudit** and **Common** | **Journal** | **LogoffAudit** configuration parameters. For more information, refer to the *One Identity Manager Process Monitoring and Troubleshooting Guide* chapter *Recording logins and logoffs in the system journal*.
- Log data changes: In Designer, activate the **Common** | **ProcessState** | **PropertyLog** and **Common** | **ProcessState** | **PropertyLog** | **AllDefaultPropertiesForModel** configuration parameters. For more information, refer to the *One Identity Manager Configuration Guide* chapter *Logging data changes*.
- Configure target system logging to generate audit data. For more information, refer to the *One Identity Manager Target System Synchronization Reference Guide* chapter *Configuring the synchronization log*.
- Label the following additional columns to be part of the change data logging as described in the *One Identity Manager Configuration Guide* in chapter *Labeling columns for recording changes to data*:

Table	Columns
AERole	• UID_DialogGroup
DialogAuthentifier	• IsEnabled • IsShowInInterface
DialogColumn	• IsToWatch • IsToWatchDelete
DialogColumnGroupRight	• * (ColumnName does not start with "X")
DialogConfigParm	• Enabled

Table	Columns
	• Value
DialogGroup	• * (ColumnName does not start with "X")
DialogGroupHasFeature	• UID_DialogFeature • UID_DialogGroup
DialogGroupInGroup	• UID_DialogGroupChild • UID_DialogGroupParent
DialogGroupInProductLimited	• UID_DialogGroup • UID_DialogProduct
DialogProductHasAuthentifier	• IsInActive • UID_DialogAuthentifier • UID_DialogProduct
DialogSchedule	• * (ColumnName does not start with "X")
DialogTableGroupRight	• * (ColumnName does not start with "X")
DialogUser	• AuthentifierLogins • IsAdmin • IsLockedOut • IsPwdExternalManaged • IsReadOnly • IsServiceAccount • PasswordNeverExpires • UserName
DialogUserInGroup	• UID_DialogGroup • UID_DialogUser
DPRSystemConnection	• WriteJournal • JournalLogFailedObjectChanges • JournalLogObjectChanges • JournalLogPropertyChanges • JournalMessageContexts
JobAutoStart	• * (ColumnName does not start

Table	Columns
	with "X")
Person	• UID_DialogUser

Use of the authentication mechanism (ESM_EAU.2)

Additional audit record contents:

- None

Sample audit records

The SQL table **DialogJournal** records both failed and successful authentication attempts.

Sample for a failed authentication attempt:

- MessageType = I
- Message = Login failed (Module: System user, Properties: User=<user name>, client machine: DABCFP5DF72, Errors: [810015] Login failed for user <user name>
- MessageDate = 2019-11-15 09:23:50.597
- ApplicationName = <name of the process>

Sample for a successful authentication attempt:

- MessageType = I
- Message = Login succeeded for module System user, properties: User=<username>, client machine: DABCFP5DF72, session: <UID>
- MessageDate = 2019-11-15 09:23:50.597
- ApplicationName = <name of the process>

Creation or modification of identity and credential data (ESM_ICD.1)

Additional audit record contents:

- The attribute(s) modified
- The subject created or modified, the attribute(s) modified (if applicable)

Sample audit records

The **DialogWatchOperation** SQL table records one entry for each operation that corresponds to the creation or modification of an identity, as stored in the **Person** table.

Sample:

- UID_DialogWatchOperation = 76051751-688D-49B1-B860-E8FFD5C9D959
- OperationType = U [for modification] or I [for creation]
- OperationDate = 2019-03-22 10:18:14.453
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>Person</T><P>1200cfaf-fedb-4dd7-bfc4-8bb59ff12093</P></Key> [identifies the identity or credential, in this case an identity/Person object]
- DisplayValue = Franke, Tino – TINOF

For each entry in **DialogWatchOperation**, the **DialogWatchProperty** SQL table records one record per attribute modified as part of that operation.

Sample:

- UID_DialogWatchOperation = 76051751-688D-49B1-B860-E8FFD5C9D959
- UID_DialogColumn = QER-8F03B89FA2F7451597EAAED8E9B9057B [identifies the attribute **FirstName** of the identity model]
- ContentShort = <attribute value>
- Modifications to credentials for external systems are stored and retrieved in the same way.

Enrollment or modification of subject (ESM_ICD.1)

Additional audit record contents:

- The subject created or modified, the attribute(s) modified

Sample audit records

Refer to Creation or modification of identity and credential data (ESM_ICD.1) on page 14.

Attempts to transmit information (ESM_ICT.1)

Additional audit record contents:

- The destination to which the transmission was attempted

Sample audit records

All attempts to synchronize data with third-party systems are logged in the synchronization log, which is stored in the following SQL tables:

- **DPRJournal**
- **DPRJournalObject**
- **DPRJournalMessage**

DPRJournal contains the main information about a single synchronization process between One Identity Manager and a connected target system. **DPRJournalMessage** collects all messages returned by the connector. **DPRJournalObject** collects all changes to an object. Both **DPRJournalMessage** and **DPRJournalObject** have a reference (foreign key relation) to **DialogJournal**.

Sample message:

- DPRJournal.UID_DPRProjectionConfig = "Exchange Online organization <name> - Initial Synchronization" [Identifier of the external system, and of the type of synchronization performed]
- DPRJournalObject.ObjectDisplay = "<user name>” [Identifier of the object being transmitted]
- DPRJournal.MessageString = "1. Executing synchronization step (UnifiedGroup) Processing steps: 2 Execution time: 13.58s"
- DPRJournal.CreationTime = 2019-10-28 04:02:42.710
- DPRJournal.MessageType = I [for Information]

Additionally, synchronization processes are logged in the **JobHistory** SQL table.

Sample message:

- BasisObjectKey = "<user name>" [Identifier of the object being transmitted]
- ParamIN = Wrapper string which contains the identifier of the value **UID_ DPRProjectionConfig** which identifies the external system
- StartAt = 2019-11-21 09:20:38.347
- EndedAt = 2019-11-21 09:20:46.657

Establishment and disestablishment of communications with audit server (FAU_STG_EXT.1)

Additional audit record contents:

- Identification of audit server

One Identity Manager must be connected to the database for all operations. The database also holds all audit logs. Thus, there is no way for the TOE (target of evaluation) to make an audit record for this action, because disestablishment and establishment of this channel is synonymous with operation of the TOE. To summarize: A connection to the audit server is established when One Identity Manager starts up and that the connection is torn down once One Identity Manager shuts down.

Additionally, One Identity Manager only writes audit records to the database when the events are configured to be enabled. The enabling or disabling of audit records for an event also identifies the establishment or disestablishment of the use of the continuous connection to the database for audit.

Sample audit records

The **DialogWatchOperation** SQL table records one entry for each operation that corresponds to the modification of an audit event as stored in the **DialogConfigParm** table.

Sample for disabling the login audit event

- UID_DialogWatchOperation = 4DC0E48B-6248-4840-8E57-62447DB747BA
- OperationType = U [for modification]
- OperationDate = 2019-03-22 10:18:14.453
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>DialogConfigParm</T><P>QBM-77C0BBF5293F414E8A7BF9F06CF2531D</P></Key> [identifies the audit event; in this case the login event]
- DisplayValue = Common\Journal\LoginAudit

For each entry in **DialogWatchOperation**, the **DialogWatchProperty** SQL table records one record per attribute modified as part of that operation.

Sample:

- UID_DialogWatchOperation = 4DC0E48B-6248-4840-8E57-62447DB747BA
- UID_DialogColumn = QBM-DE26DD4FAB774FC890756D65D73F887F "Enabled" property of the audit event.
- ContentShort = 1 [identifies that the audit event was turned on before and has been turned off with this audit entry as the value is of type boolean]

Sample for enabling the login audit event

- UID_DialogWatchOperation = 3C61DA9D-FBF9-44E3-970B-308FBF62B1FD
- OperationType = U [for modification]
- OperationDate = 2019-03-22 10:19:15.421
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>DialogConfigParm</T><P>QBM-77C0BBF5293F414E8A7BF9F06CF2531D</P></Key> [identifies the audit event; in this case the login event]
- DisplayValue = Common\Journal\LoginAudit

For each entry in **DialogWatchOperation**, the **DialogWatchProperty** SQL table records one record per attribute modified as part of that operation.

Sample:

- UID_DialogWatchOperation = 3C61DA9D-FBF9-44E3-970B-308FBF62B1FD
- UID_DialogColumn = QBM-DE26DD4FAB774FC890756D65D73F887F "Enabled" property of the audit event.
- ContentShort = 0 [identifies that the audit event was turned off before and has been turned on with this audit entry as the value is of type boolean]

Modifications of One Identity Manager security function behavior (FMT_MOF.1)

Additional audit record contents:

- None

Sample audit records

All modifications to the relevant tables are logged in the **DialogWatchOperation** and **DialogWatchproperty** SQL tables as shown in the example in Creation or modification of

identity and credential data (ESM_ICD.1) on page 14 or in the example in Establishment and disestablishment of communications with audit server (FAU_STG_EXT.1) on page 17.

Sample for creating or updating an application role

- UID_DialogWatchOperation = 4388D503-CBF5-413F-AEFC-43CC58276898
- OperationType = U [for modification] or I [for creation]
- OperationDate = 2019-12-19 10:27:25.293
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>AERole</T><P>QER-AEROLE-ALLMANAGER</P></Key> [identifies the application role **Employee Managers**]
- DisplayValue = Employee Managers

Sample:

- UID_DialogWatchOperation = 4388D503-CBF5-413F-AEFC-43CC58276898
- UID_DialogColumn = QER-BACCCFD31D03488E93599A6C32CCF377 [identifies the attribute **UID_DialogGroup** which holds the permission group assigned to the application role]
- ContentShort = QER-6AB5A4DB041C43A698E2AB231BD56D30 [identifies the permission group **VI_4_ALLMANAGER**]

Sample for adding a user to an application role

- UID_DialogWatchOperation = 3DB8F633-DB7A-41FF-B848-23C6FD7EC843
- OperationType = I [for creation]
- OperationDate = 2019-12-19 10:38:00.343
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>PersonInAERole</T><P>QER-AEROLE-ALLMANAGER</P><P>65204767-5a25-4b38-a86c-de87344184b9</P></Key> [identifies the identity/person that has been added to an application role]
- DisplayValue = Employee Managers - Acree, Pierre - PIERREACR

Sample for removing a user from an application role

- UID_DialogWatchOperation = 56D5FE6D-777B-4E0F-9335-CB13F3477C43
- OperationType = D [for deletion]
- OperationDate = 2019-12-19 10:45:17.633
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>PersonInAERole</T><P>QER-AEROLE-ALLMANAGER</P><P>65204767-5a25-4b38-a86c-de87344184b9</P></Key> [identifies the identity/person that has been added to an application role]
- DisplayValue = Employee Managers - Acree, Pierre - PIERREACR

Sample property changes of the removal of a user from an application role:

First property change

- UID_DialogWatchOperation = 56D5FE6D-777B-4E0F-9335-CB13F3477C43
- UID_DialogColumn = QER-934043FCCF2445629722C569E301BABD [identifies the attribute **UID_AERole** which holds the application role this assignment belongs to]
- ContentShort = QER-AEROLE-ALLMANAGER [identifies the application role **Employee Managers**]

Second property change

- UID_DialogWatchOperation = 56D5FE6D-777B-4E0F-9335-CB13F3477C43
- UID_DialogColumn = QER-F449F40BA48B4B2A8F903132452574D8 [identifies the attribute **UID_Person** which holds the identity/person of the assignment]
- ContentShort = 65204767-5a25-4b38-a86c-de87344184b9 [identifies the identity/person **Acree, Pierre - PIERREACR**]

Sample for enabling the synchronization logging configuration

- UID_DialogWatchOperation = 7F25E53D-813F-4BA9-9F2A-B6B1D0A906E1
- OperationType = U [for modification]
- OperationDate = 2019-12-19 11:14:13.533
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>DPRSystemConnection</T><P>CCC-CB808ECB2BDB8846A81983876A2BCE95</P></Key> [identifies the target system connection to be modified]

- DisplayValue = Active Directory Domain (DC=IAM,DC=CORP) - Active Directory Service (Root DN dc=IAM,dc=corp, Server iams01.iam.corp)

Sample:

- UID_DialogWatchOperation = 7F25E53D-813F-4BA9-9F2A-B6B1D0A906E1
- UID_DialogColumn = DPR-D058D584A19E454A94C6ED6C89C6ADE1 [identifies the attribute **JournalLogObjectChanges** at the target system connection]
- ContentShort = 0 [identifies that the logging was turned off before and has been turned off with this audit entry as the value is of type Boolean]

Sample for disabling the synchronization logging configuration

- UID_DialogWatchOperation = D3DE515C-EF00-4D8D-878E-3711C6C67804
- OperationType = U [for modification]
- OperationDate = 2019-12-19 11:16:43.793
- OperationUser = viadmin
- ObjectKeyOfRow = <Key><T>DPRSystemConnection</T><P>CCC-CB808ECB2BDB8846A81983876A2BCE95</P></Key> [identifies the target system connection to be modified]
- DisplayValue = Active Directory Domain (DC=IAM,DC=CORP) - Active Directory Service (Root DN dc=IAM,dc=corp, Server iams01.iam.corp)

Sample:

- UID_DialogWatchOperation = D3DE515C-EF00-4D8D-878E-3711C6C67804
- UID_DialogColumn = DPR-D058D584A19E454A94C6ED6C89C6ADE1 [identifies the attribute **JournalLogObjectChanges** at the target system connection]
- ContentShort = 1 [identifies that the logging was turned on before and has been turned off with this audit entry as the value is of type Boolean]

Use of management functions (FMT_SMF.1)

Additional audit record contents:

- Management function performed

Sample audit records

All modifications to the relevant tables are logged in the **DialogWatchOperation** and **DialogWatchproperty** SQL tables as shown in the example in Creation or modification of identity and credential data (ESM_ICD.1) on page 14.

Use of trusted channel functions (FTP_ITC.1)

Additional audit record contents:

- Identity of the initiator and target of the trusted channel

Sample audit records

Refer to Attempts to transmit information (ESM_ICT.1) on page 16.

Attempted uses of the trusted path functions (FTP_TRP.1)

Additional audit record contents:

- Identification of users associated with all trusted path functions

Sample audit records

Refer to Use of the authentication mechanism (ESM_EAU.2) on page 14.

8

External audit trail storage (FAU_STG_EXT.1)

This chapter describes how to set up TLS connectivity to the SQL database.

Microsoft SQL Server

To configure the use of TLS for the connection of the audit trail data stored in the One Identity Manager database, it is required to configure the SQL server to force encrypted connections as described under https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017.

User-subject binding (FIA_USB.1)

In non-role-based authentication (for example in Designer):

- effective permission groups for a user are reloaded regularly after five minutes
- changing the system user associated with a person does not take effect until the user logs out and logs in again

In role-based authentication, changes in effective application roles for a user do not take effect until the user logs out and logs in again.

When an account is disabled while the user is logged in, the active session will stop working after 20 minutes. For more information, refer to the *One Identity Manager Authorization and Authentication Guide* chapter *Enabling the validity of a login*.

Users can be created using Manager (see the *One Identity Manager Identity Management Base Module Administration Guide* chapter *Entering employee master data*) and the Web Portal (see the *One Identity Manager Web Portal User Guide* chapter *Adding employees*). User data can also be created from external systems by means of synchronization and using the automatic employee assignment. For the automatic employee assignment, you first have to link the users of the connected target system to the employees in One Identity Manager as described in the *One Identity Manager Administration Guide for Connecting to Active Directory* in chapter *Linking user accounts to employees*. For more information regarding automatic employee assignment, refer to the *One Identity Manager Administration Guide for Connecting to Active Directory* chapter *Automatic assignment of employees to Active Directory user accounts* and *One Identity Manager Target System Base Module Administration Guide* chapter *Editing search criteria for automatic employee assignment*.

Management of functions behavior (FMT_MOF.1)

This chapter describes typical operations performed by users of One Identity Manager. Respectively, the following is covered in this chapter:

- Interfaces that can be used to perform these operations
- Roles that are needed to perform these operations
- Steps that are needed to perform these operations

Management of authentication data for both interactive users and authorized IT entities (ESM_EAU.2)

NOTE: This chapter refers to the Active Directory password used to access One Identity Manager itself as defined in Reliance on enterprise authentication (ESM_EAU.2) on page 5.

Management activities:

- Management of authentication data for both interactive users and authorized IT entities

Interfaces:

- Password Reset Portal (refer to the following instructions)
- REST API (refer to the following instructions)

Roles:

- The **VI_4_ALLUSER** application role is automatically assigned to every person. This application role grants permission to set passwords for accounts assigned to their identity.

- Members of the target system administrator application roles for a particular system are given permissions to set passwords for the accounts in this particular system.

Documentation:

- *One Identity Manager Web Portal User Guide* chapter *Change password*

To change your personal password using the Password Reset Portal

NOTE: The Password Reset Portal can be configured to allow users to log in with user accounts other than their central user account using password questions or a passcode. Although there is no difference from a security perspective, the Password Reset Portal should not be configured to allow a user to log in with user accounts other than their central user account (that is, the target system user account), as this is a new feature and was not part of the evaluation.

1. Open the Password Reset Portal.
2. Log in using one of the provided options.
3. On the **Manage my passwords** page, select the option **I want to reset one or more passwords**.
4. Perform one of the following tasks:
   - To change the passwords for your personal user accounts, click ▶ next to **Personal accounts**.
   - To change the passwords of other user accounts, click ▶ next to **Other accounts**
5. Select the check box next to the user accounts for which you want to change the password.
6. Click **Next**.
7. On the **Set a new password** page, in the **New password** box, enter the password you want to use.
8. In the **Repeat the password** box, enter the password again.
9. Click **Next**.

   The password is set for the previously selected user accounts.

To change an Active Directory account's password using the REST API

- Use a request to change the account's password.

  Example

  URL:

  ```
  PUT /AppServer/api/entity/ADSAccount/<UID>
  ```

  Where **<UID>** is the unique identifier of the account within One Identity Manager.

Request body:

```
{
   "values": {
      "UserPassword": "<value of the new password>"
   }
}
```

Definition of identity and credential data that can be associated with users (ESM_ICD.1)

TIP: For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`.

Creating users (ESM_ICD.1)

Interfaces:

- Web Portal
- REST API

Roles:

- For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`.

Documentation:

- *One Identity Manager Web Portal User Guide* chapter *Adding employees*

To create a user using the Web Portal

1. Log in to the Web Portal.
2. In the menu bar, click **Responsibilities** | **Governance Administration**.
3. On the **Governance Administration** page, click the **Employees** tile.
4. On the **People** page, click **Add a new employee**.
5. On the **Add a New Employee** page, enter the master data of the new user.
6. Click **Save**.

To create a user using the REST API

- Use a request to create a user.

Example

URL:

```
POST /AppServer/api/entity/Person
```

Person is the name of the table that holds the users within One Identity Manager.

Request body:

```
{
     "values": {
        "FirstName": "Jeremia",
        "LastName": "Bodewell"
        }
}
```

Editing users (ESM_ICD.1)

Interfaces:

- Web Portal
- REST API

Roles:

- For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`.

Documentation:

- *One Identity Manager Web Portal User Guide* chapter *Editing employee data*

To edit user data using the Web Portal

1. Log in to the Web Portal.
2. In the menu bar, click **Responsibilities** | **Governance Administration**.
3. On the **Governance Administration** page, click the **Employees** tile.
4. On the **People** page, click the user you want to edit.
5. On the **Employee** page, click the **Master data** tile.
6. On the **Master data** page, edit the master data of the user.
7. Click **Save**.

To edit user data using the REST API

- Use a request to edit user data.

Example

URL:

```
PUT /AppServer/api/entity/Person/<UID>
```

Where **<UID>** is the unique identifier of the user in the **Person** table that holds the users within One Identity Manager.

Request body:

```
{
     "values": {
        "LastName": "Garcia",
        "City": "Berlin"
        }
}
```

Changing passwords of users (ESM_ICD.1)

Interfaces:

- Web Portal
- REST API

Roles:

- For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`

Documentation:

- *One Identity Manager Web Portal User Guide* chapter *Change password*

To change the password of a user using the Password Reset Portal

1. Open the Password Reset Portal.
2. Log in using one of the provided options.
3. On the **Manage my passwords** page, select the option **I want to reset my central password**.
4. Click **Next**.
5. On the **Set a new password** page, in the **New password** box, enter the password you want to use.

6. In the **Repeat the password** box, enter the password again.
7. Click **Next**.

   The central password is changed.

To change the password of a user using the REST API

- Use a request to set the password of a user.

  Example

  URL:

  `PUT /AppServer/api/entity/Person/<UID>`

  Where **<UID>** is the unique identifier of the user in the **Person** table that holds the users within One Identity Manager.

  Request body:

```
{
     "values": {
        "CentralPassword": "<value of the new password>"
     }
}
```

Locking/unlocking users (ESM_ICD.1)

Interfaces:

- Web Portal
- REST API

Roles:

- For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`.

Documentation:

- *One Identity Manager Identity Management Base Module Administration Guide* chapter *Disabling and deleting employees*
- *One Identity Manager Web Portal User Guide* chapter *Editing employee data*

To lock a user using the Web Portal

1. Log in to the Web Portal.
2. In the menu bar, click **Responsibilities** | **Governance Administration**.
3. On the **Governance Administration** page, click the **Employees** tile.

4. Click the user you want to lock.
5. On the **Employee** page, click the **Master data** tile.
6. On the **Master data** page, select the **Temporarily disable until** check box.

   If you want to lock the user for a specific time, select the date and time when the user should be unlocked again.
7. Click **Save**.

To unlock a user using the Web Portal

1. Log in to the Web Portal.
2. In the menu bar, click **Responsibilities** | **Governance Administration**.
3. On the **Governance Administration** page, click the **Employees** tile.
4. Click the user you want to unlock.
5. On the **Employee** page, click the **Master data** tile.
6. On the **Master data** page, clear the **Temporarily disable until** check box.
7. Click **Save**.

To lock a user using the REST API

- Use a request to lock the user.

  Example

  URL:

  `PUT /AppServer/api/entity/Person/<UID>`

  Where **<UID>** is the unique identifier of the user in the **Person** table that holds the users within One Identity Manager.

  Request body:

```
{
     "values": {
        "IsTemporaryDeactivated": true,
        "DeactivationEnd": <Date/time value>
     }
}
```

To unlock a user using the REST API

- Use a request to unlock the user.

  Example

URL:

`PUT /AppServer/api/entity/Person/<UID>`

Where **<UID>** is the unique identifier of the user in the **Person** table that holds the users within One Identity Manager.

Request body:

```
{
     "values": {
        "IsTemporaryDeactivated": false
     }
}
```

Assigning/removing application roles to/from users (ESM_ICD.1)

Interfaces:

- Manager
- REST API

Roles:

- For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`.

To assign an application role to a user using Manager

1. Start Manager.
2. In the navigation, click **Employees**.
3. In the navigation under **Employees**, click **Employees**.
4. In the **Employees** list, double-click the user you want to assign an application role to.
5. Under **Tasks**, click **Assign One Identity Manager application roles**.
6. Under **Add assignments**, double-click the application role you want to assign to the user.
7. Click **Save**.

To remove an application role from a user using Manager

1. Start Manager.
2. In the navigation, click **Employees**.

3. In the navigation under **Employees**, click **Employees**.
4. In the **Employees** list, double-click the user you want to remove an application role from.
5. Under **Tasks**, click **Assign One Identity Manager application roles**.
6. Under **Remove assignments**, double-click the application role you want to remove from the user.
7. Click **Save**.

To assign a user to an application role using the REST API

- Use a request to assign the user to the application role.

Example

URL:

`PUT /AppServer/api/assignments/PersonInAERole/UID_Person/<UID>`

Where **<UID>** is the unique identifier of the user within One Identity Manager.

Request body:

```
{
    "members": [
        "<UID of the application role>"
    ]
}
```

To remove a user from an application role using the REST API

- Use a request to remove the user from the application role.

Example

URL:

`DELETE /AppServer/api/assignments/PersonInAERole/UID_Person/<UID>`

Where **<UID>** is the unique identifier of the user within One Identity Manager.

Request body:

```
{
    "members": [
        "<UID of the application role>"
    ]
}
```

Assigning/removing accounts to/from users (ESM_ICD.1)

Interfaces:

- Manager
- REST API

Roles:

- For default identity and account permissions on tables, refer to `Default_Permissions_on_Tables_and_Attributes_for_Identities_and_Accounts.xlsx`.

Documentation:

- *One Identity Manager Administration Guide for Connecting to Active Directory* chapter *Entering master data for Active Directory user accounts*

To assign an Active Directory user account to a user using Manager

1. Start Manager.
2. In the navigation, click **Employees**.
3. In the navigation under **Employees**, click **Employees**.
4. In the **Employees** list, double-click the user you want to assign an Active Directory user account to.
5. Under **Tasks**, click **Assign Active Directory user accounts**.
6. Under **Add assignments**, double-click the Active Directory user account you want to assign to the user.
7. Click **Save**.

To remove an Active Directory user account from a user using Manager

1. Start Manager.
2. In the navigation, click **Employees**.
3. In the navigation under **Employees**, click **Employees**.
4. In the **Employees** list, double-click the user you want to remove an Active Directory user account from.
5. Under **Tasks**, click **Assign Active Directory user accounts**.
6. Under **Remove assignments**, double-click the Active Directory user account you want to remove from the user.
7. Click **Save**.

To assign an Active Directory account to a user using the REST API

- Use a request to assign the Active Directory account to the user.

Example

URL:

`PUT /AppServer/api/entity/ADSAccount/<UID>`

Where **<UID>** is the unique identifier of the account within One Identity Manager.

Request body:

```
{
    "values": {
       "UID_Person": <user identifier>
    }
}
```

To remove an Active Directory account from a user using the REST API

- Use a request to remove the Active Directory from the user.

Example

URL:

`PUT /AppServer/api/entity/ADSAccount/<UID>`

Where **<UID>** is the unique identifier of the account within One Identity Manager.

Request body:

```
{
    "values": {
       "UID_Person": <null>
    }
}
```

Managing password policies (ESM_ICD.1)

Interfaces:

- Manager

Roles:

- Members of the **Identity Management** | **Employees** | **Administrators** application role can create password policies for employee data stored in the **Person** table.
- For each target system type, members of the target system administrator role can create password policies for accounts in that target system.

Documentation:

- *One Identity Manager Authorization and Authentication Guide* chapter *Application roles for target systems*
- *One Identity Manager Identity Management Base Module Administration Guide* chapter *Password policies for employees*
- *One Identity Manager Administration Guide for Connecting to Active Directory* chapter *Password policies for Active Directory user accounts*

To create a password policy for Active Directory

1. Start Manager.
2. In the navigation, select **Active Directory**.
3. In the navigation, under **Active Directory**, click **Basic configuration data** | **Password policies**.
4. Under **Password policies**, click **Create**.
5. On the master data form, enter the master data for the password policy.
6. Click **Save**.

To edit a password policy for Active Directory

1. Start Manager.
2. In the navigation, select **Active Directory**.
3. In the navigation, under **Active Directory**, click **Basic configuration data** | **Password policies**.
4. In the **Password policies** list, double-click the password policy you want to edit.
5. Under **Tasks**, click **Change master data**.
6. On the master data form, edit the master data for the password policy.
7. Click **Save**.

To delete a password policy for Active Directory

1. Start Manager.
2. In the navigation, select **Active Directory**.
3. In the navigation, under **Active Directory**, click **Basic configuration data** | **Password policies**.
4. In the **Password policies** list, click the password policy you want to delete.
5. Under **Password policies**, click **Delete**.
6. In the confirmation dialog, click **Yes**.

Management of credential status (ESM_ICD.1)

Refer to Definition of identity and credential data that can be associated with users (ESM_ICD.1) on page 27

Enrollment of users into repository (ESM_ICD.1)

Refer to Definition of identity and credential data that can be associated with users (ESM_ICD.1) on page 27.

In addition, new users may be enrolled indirectly through setting up synchronization with an external system. In this way, creating a new user on that system will cause a new employee to be created in the TOE (target of evaluation). For more information, refer to User-subject binding (FIA_USB.1) on page 24.

Configuration of circumstances in which transmission of identity and credential data is performed (ESM_ICT.1)

Transmission is configured using startup configurations. The startup configurations are configured as part of the initial setup process of a target system synchronization.

Specifically, a startup configuration can be associated with a schedule, which determines when transmission should happen.

Interfaces:

- Synchronization Editor

Roles:

- The **vi_4_SYNCPROJECT_ADMIN** application role grants permissions to perform the function.

Documentation:

- *One Identity Manager Target System Synchronization Reference Guide* chapter *Setting up start up configurations*

- *One Identity Manager Target System Synchronization Reference Guide* chapter *Specifying a schedule*

Configuration of external audit storage location (FAU_STG_EXT.1)

By default, all audit trail data is stored in the One Identity Manager database. For more information, refer to External audit trail storage (FAU_STG_EXT.1) on page 23.

Definition of default subject security attributes, modification of subject security attributes (FIA_USB.1)

Refer to Definition of identity and credential data that can be associated with users (ESM_ICD.1) on page 27.

Management of sets of users that can interact with security functions (FMT_MOF.1)

Sets of users are managed using application roles. For details on how to assign users to application roles, refer to Assigning/removing application roles to/from users (ESM_ICD.1) on page 32.

Management of the users that belong to a particular role (FMT_SMR.1)

Sets of users are managed using application roles. For details on how to assign users to application roles, refer to Assigning/removing application roles to/from users (ESM_ICD.1) on page 32.

For details on how to create new application roles from existing permissions, refer to Security management roles (FMT_SMR.1) on page 42.

Configuration of actions that require trusted channel (FTP_ITC.1)

The following application roles grant permissions to start Synchronization Editor:

- **vi_4_PERSONADMIN**
- **vi_4_STRUCTADMIN_ADMIN**
- **vi_4_SYNCPROJECT_ADMIN**
- **vi_4_ROLEADMIN_ADMIN**
- **vi_4_RULEADMIN_SAPRIGHTS**

The following permissions groups grant permission to create or edit schedules, which can trigger actions that require a trusted channel.

Non-role-based:

- **VI_Attestation_EditRights**
- **VI_Compliance_EditRights**
- **DPR_EditRights_Methods**
- **VI_EBS_EditRights**
- **VI_QERPolicy_EditRights**
- **VID**

Role-based:

- **vi_4_SYNCPROJECT_ADMIN**
- **vi_4_ATTESTATIONADMIN_ADMIN**
- **vi_4_QERPOLICYADMIN_ADMIN**
- **vi_4_RULEADMIN_ADMIN**
- **vi_4_NAMESPACEADMIN_EBS**

Interfaces:

- Synchronization Editor

Roles:

- One Identity Manager administrator

Configuration of actions that require trusted path (FTP_TRP.1)

No configuration is necessary because HTTPS is enabled by default during installation.

Application server

By default, the installation of the application server enforces the use of HTTPS-enabled IIS web sites. For more information, refer to the *One Identity Manager Installation Guide* chapter *Installing and updating an application server*.

Web server

By default, the installation of the Web Portal enforces the use of HTTPS-enabled IIS web sites.

The Web Portal utilizes either one channel to an application server or one channel to the SQL server and an additional channel to the application server. To set up a secure channel to the application server, use HTTPS in the connection URL during the installation. To set up a secure channel to the SQL server, follow the recommendations in External audit trail storage (FAU_STG_EXT.1) on page 23.

For more information, refer to the *One Identity Manager Installation Guide* chapter *Installing, configuring and maintaining the Web Portal*.

11

Management of security data (FMT_MTD.1)

One Identity Manager users can manage their own password data using the Password Reset Portal. For more information, refer to the *One Identity Manager Web Portal User Guide* chapter *Change password*. For information on how to set up the Password Reset Portal, refer to the *One Identity Manager Web Application Configuration Guide* chapter *Setting up a Password Reset Portal*.

One Identity Manager users can also manage their personal user data and their own password questions using the Web Portal. For more information, refer to the *One Identity Manager Web Portal User Guide* chapters *Changing contact information* and *Managing password questions*.

12

Security management roles (FMT_SMR.1)

This chapter describes how you can create new administrators/roles and assign new administrators to new or existing roles.

In One Identity Manager identities (persons) performing administrative tasks can be assigned to administrator application roles. An administrator can create and edit application roles. For more general information regarding application roles, refer to the *One Identity Manager Authorization and Authentication Guide* chapter *Creating and editing application roles*.

Permissions are granted through permissions groups. Each application role is mapped to a permissions group.

The default permissions groups that grant permissions to manage users belonging to an application role are as follows.

- Non-role-based permissions groups:
  - **AAD_EditRights_Methods**
  - **VI_ADS_EditRights_Methods**
  - **VI_Attestation_EditRights**
  - **VI_Compliance_EditRights**
  - **CSM_EditRights**
  - **VI_EBS_EditRights**
  - **VI_Exchange_EditRights**
  - **VI_Notes_EditRights**
  - **O3S_EditRights_Methods**
  - **PAG_EditRights_Methods**
  - **VI_QERPolicy_EditRights**
  - **VI_ITShop_EditRights**
  - **UNX_EditRights_Methods**
- Role-based permissions groups:

- For each type of target system, there is a dedicated target system administrator application role.
- **vi_4_ATTESTATIONADMIN_ADMIN**
- **vi_4_CUSTOM_ADMIN**

For more information regarding permissions groups and application roles, refer to the *One Identity Manager Authorization and Authentication Guide*:

- General information can be found in chapter *Granting One Identity Manager schema permissions*.
- Building permissions groups is described in chapter *Creating permissions groups*.
- Modifying the permissions associated with a permissions group is described in chapter *Editing table permissions and column permissions*.
- Nesting of hierarchical permission groups is described in chapter *Permissions group dependencies*.
- Mapping an identity to the effective permissions groups is described in chapter *Rules for determining the valid permissions for tables and columns*.
- The application roles are described in chapter *Application roles overview*.
- The dedicated target system administrator application roles for each type of target system are described in chapter *Application roles for target systems*.

13

Trusted channel (FTP_ITC.1)

The setup of the trusted channel for external systems/endpoints is described in Identity and credential transmission (ESM_ICT.1) on page 8.

NOTE: If the setup of a trusted channel for a system/endpoint is not mentioned in Identity and credential transmission (ESM_ICT.1) on page 8, the underlying API uses a secure channel automatically.

14

Trusted path (FTP_TRP.1)

This chapter describes how to set up a trusted path to specific internal systems/endpoints.

Application server

The installation of the application server enforces the use of HTTPS-enabled IIS web sites by default. For more information, refer to the *One Identity Manager Installation Guide* chapter *Installing and updating an application server*.

Web server

The installation of the Web Portal enforces the use of HTTPS-enabled IIS web sites by default.

The Web Portal utilizes either one channel to an application server or one channel to the SQL server and an additional channel to the application server. To set up a secure channel to the application server, use HTTPS in the connection URL during the installation. To set up a secure channel to the SQL server, follow the recommendations in External audit trail storage (FAU_STG_EXT.1) on page 23.

For more information, refer to the *One Identity Manager Installation Guide* chapter *Installing, configuring and maintaining the Web Portal*.

Fat clients

The fat clients utilize either a channel to an application server or a channel to the SQL server. To set up a secure channel to the application server, use HTTPS in the connection URL during the setup of the connection to the application server.

To setup a secure channel to the SQL Server, follow the recommendations in External audit trail storage (FAU_STG_EXT.1) on page 23.

For more information, refer to the *One Identity Manager Installation Guide* chapter *Logging in to the One Identity Manager database*.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product