SAP Master Data Governance

Security Guide

For

SAP Master Data Governance, Retail and Fashion Management extension by Utopia ™

CUSTOMER

Document Version: 30-AUGUST-2016

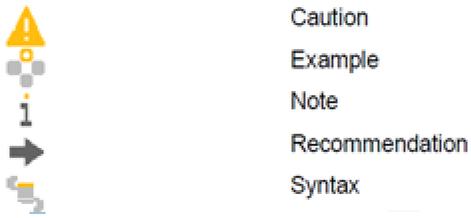
Copyright

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Please see http://www.sap.com/corporate-en/legal/copyright/index.epx# trademark for additional trademark information and notices.

Icons in Body Text



Icon	Meaning
⚠	Caution
⁘	Example
ℹ	Note
➡	Recommendation
⇆	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* → *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example Text	Emphasized words or phrases in body text, graphic titles, and table titles.
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, F2 or ENTER.

Master Data Governance Security Guide

The following guide covers the information that you require to operate Master Data Governance securely. To make the information more accessible, it is divided into a general part, containing information relevant for all components, and a separate part for information specific for individual components.

1. Introduction

This guide does not replace the administration or operation guides that are available for productive operations.

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guide provides information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to Master Data Governance. To assist you in securing Master Data Governance, we provide this Security Guide.

Since Master Data Governance is based on and uses SAP NetWeaver technology, it is essential that you consult the Security Guide for SAP NetWeaver. See SAP Service Marketplace at ▶ http://service.sap.com/securityguide ▸ *SAP NetWeaver*◀.

For all Security Guides published by SAP, see SAP Service Marketplace at http://service.sap.com/securityguide.

Overview of the Main Sections

The security Guide comprises of the following main sections:

- Before You Start [Page 6]

Security Guide

This section contains information about why security is necessary, how to use this document, and references to other Security Guides that build the foundation for this Security Guide.

- Technical System Landscape [Page 6]

  This section provides an overview of the technical components and communication paths that are used by Master Data Governance.

- User Management and Authentication [Page 6]

  This section provides an overview of the following user administration and authentication aspects:
  - Recommended tools to use for user management
  - User types that are required by Master Data Governance
  - Standard users that are delivered with Master Data Governance
  - Overview of the user synchronization strategy
  - Overview of how integration into Single Sign-On environments is possible

- Authorizations [Page 10]

  This section provides an overview of the authorization concept that applies to Master Data Governance.

- Network and Communication Security [Page 11]

  This section provides an overview of the communication paths used by Master Data Governance and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level

- Data Storage Security [Page 13]

  This section provides an overview of any critical data that is used by Master Data Governance and the security mechanisms that apply.

- Enterprise Services Security [Page 14]

  This section provides an overview of the security aspects that apply to the enterprise services delivered with Master Data Governance.

- Security-relevant Logs and Tracing [Page 14]

  This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach does occur.

- Appendix [Page 16]

  This section provides references to further information.

2. Before You Start

This table contains the most important SAP notes concerning the safety of Master Data Governance.

Title	SAP Note	Comment
Code injection vulnerability in UAC_ASSIGNMENT_CONTROL_TEST	1493809	MDG and XBRL

More Information

For more information about specific topics, see the sources in the table below:

Content	Quick Link on SAP Service Marketplace or SDN
Security	http://sdn.sap.com/irj/sdn/security
Security Guides	http://service.sap.com/securityguide
Related Notes	http://service.sap.com/notes http://service.sap.com/securitynotes
Allowed Platforms	http://service.sap.com/pam
Network Security	http://service.sap.com/securityguide
SAP Solution Manager	http://service.sap.com/solutionmanager
SAP NetWeaver	http://sdn.sap.com/irj/sdn/netweaver

3. Technical System Landscape

For information about the technical system landscape, see the sources listed in the table below.

Subject	Guide / Tool	Quick Link to SAP Service Marketplace
Technical description of Master Data Governance and the underlying technical components, such as SAP NetWeaver	Master Guide	▶ http://service.sap.com/instguides › *SAP Business Suite Application* › *SAP Master Data Governance*›
High Availability	High Availability for SAP Solutions	http://sdn.sap.com/irj/sdn/ha
Design of Technical landscape	See available documents	http://sdn.sap.com/irj/sdn/landscapedesign
Security	See available documents	http://sdn.sap.com/irj/sdn/security

4. User Management and Authentication

Master Data Governance uses the user management and authentication mechanisms of the SAP NetWeaver platform, and in particular, SAP NetWeaver Application Server. Therefore, the security

recommendations and guidelines for user management and authentication that are described in the security guide for SAP NetWeaver Application Server for ABAP Security Guide [External] also apply to Master Data Governance.
In addition to these guidelines, we also supply information on user management and authentication that is especially applicable to Master Data Governance in the following sections:

- User Administration [Page 7]
  This section details the user management tools, the required user types, and the standard users that are supplied with Master Data Governance.

- User Data Synchronization [Page 9]
  The components of Master Data Governance can use user data together with other components. This section describes how the user data is synchronized with these other sources.

- Integration into Single Sign-on Environments [Page 9]
  This section describes how Master Data Governance supports single sign-on-mechanisms.

4.1. User Administration

Master Data Governance user management uses the mechanisms provided by SAP NetWeaver Application Server for ABAP, such as tools, user types, and the password concept. For an overview of how these mechanisms apply for Master Data Governance, see the sections below. In addition, we provide a list of the standard users required for operating components of Master Data Governance.

User Administration Tools

The following table shows the user administration tools for Master Data Governance.

Tool	**Description**
User maintenance for ABAP-based systems (transaction SU01)	For more information on the authorization objects provided by the components of Master Data Governance, see the component specific section.
Role maintenance with the profile generator for ABAP-based systems (PFCG)	For more information on the roles provided by Master Data Governance, see the component specific section. For more information, see User and Role Administration of Application Server ABAP [External]
Central User Administration (CUA) for the maintenance of multiple ABAP-based systems	For more information, see Central User Administration [External]
User Management Engine for SAP NetWeaver AS Java (UME)	Administration console for maintenance of users, roles, and authorizations in Java-based systems and in the Enterprise Portal. The UME also provides persistence options, such as ABAP Engine. For more information, see User Management Engine [External]

For more information on the tools that SAP provides for user administration with SAP NetWeaver, see SAP Service Marketplace at ▶ http://service.sap.com/securityguide ▸ *SAP NetWeaver 7.0 Security Guides (Complete)* ▸ *Release* ▸ *User Administration and Authentication* ◀ .

User Types

It is often necessary to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

User types required for Master Data Governance include, for example:

- Individual Users
  - Dialog Users
    Dialog users are used for SAP GUI for Windows

  - Internet Users for Web applications
    Same policies apply as for dialog users, but used for Internet connections.

- Technical Users
  - Service users are dialog users who are available for a large set of anonymous users (for example, for anonymous system access via an ITS service).

  - Communication users are used for dialog-free communication between systems.

  - Background users can be used for processing in the background.

For more information about user types, see User Types [External] in the Security Guide for SAP NetWeaver AS ABAP.

Standard Users

The following table shows the standard Users that are necessary for operating Master Data Governance.

System	User ID	Type	Password	Additional Information
SAP Web Application Server	(sapsid) adm	SAP system administrator	Mandatory	SAP NetWeaver installation guide
SAP Web Application Server	SAP Service (sapsid) adm	SAP system service administrator	Mandatory	SAP NetWeaver installation guide

SAP Web Application Server	SAP Standard ABAP Users (SAP*, DDIC, EARLYWATCH, SAPCPIC)	See SAP NetWeaver Security Guide		SAP NetWeaver
SAP Web Application Server	SAP Standard SAP Web Application Server Java Users	See SAP NetWeaver Security Guide		SAP NetWeaver Security Guide
SAP ECC	SAP Users	Dialog users	Mandatory	The number of users depends on the area of operation and the business data to be processed.

We recommend that you change the passwords and IDs of users that were created automatically during the installation.

4.2. User Data Synchronization

By synchronizing user data, you can reduce effort and expense in the user management of your system landscape. Since Master Data Governance is based on SAP NetWeaver, you can use all of the mechanisms for user synchronization in SAP NetWeaver here. For more information, see the SAP NetWeaver Security Guide on SAP Service Marketplace at ▶ *service.sap.com/securityguide* ▶ *SAP NetWeaver*◀

You can use user data distributed across systems by replicating the data, for example in a central directory such as LDAP.

4.3. Integration into Single Sign-on Environments

Master Data Governance supports the single sign-on (SSO) mechanisms provided by SAP NetWeaver Application Server for ABAP technology. Therefore, the security recommendations and guidelines for user management and authentication that are described in the SAP NetWeaver Security Guide [External] also apply to Master Data Governance. Master Data Governance supports the following mechanisms:

Secure Network Communication (SNC)

SNC is available for user authentication and provides for an SSO environment when using the SAP GUI for Windows or Remote Function Calls.

SAP Logon Tickets

Master Data Governance supports the use of logon tickets for SSO when using a Web browser as the front-end client. In this case, users can be issued a logon ticket after they have authenticated themselves with the initial SAP system. The ticket can then be submitted to other systems (SAP or external systems) as an authentication token. The user does not need to enter a user ID or password for authentication, but can access the system directly once it has checked the logon ticket. For more information, see *SAP Logon Tickets* in the *Security Guide* for *SAP NetWeaver Application Server*.

Client Certificates

As an alternative to user authentication using a user ID and passwords, users using a Web browser as a front-end client can also provide X.509 client certificates to use for authentication. In this case, user authentication is performed on the Web server using the Secure Sockets Layer Protocol (SSL Protocol). No passwords have to be transferred. User authorizations are valid in accordance with the authorization concept in the SAP system.

For more information see Client Certificates in the Security Guide for SAP NetWeaver Application Server. For more information about available authentication mechanisms, see SAP Library for SAP NetWeaver under User Authentication and Single Sign-On [External].

5. Authorizations

Master Data Governance uses the authorization concept of SAP NetWeaver Application Server ABAP. Therefore, the security recommendations and guidelines for authorizations that are described in the Security Guide for SAP NetWeaver Application Server ABAP also apply to Master Data Governance. You can use authorizations to restrict the access of users to the system, and thereby protect transactions and programs from unauthorized access.

The SAP NetWeaver Application Server authorization concept is based on assigning authorizations to users based on roles. For role maintenance in SAP NetWeaver Application Server ABAP, use the profile generator (transaction PFCG), and in SAP NetWeaver Application Server for Java, the user management console of the User Management Engine (UME). You can define user-specific menus using roles.

ℹ

For more information about creating roles, see Role Administration [External].

Standard Roles and Standard Authorization Objects

SAP delivers standard roles covering the most frequent business transactions. You can use these roles as a template for your own roles. For a list of the standard roles and authorization objects used by components of Master Data Governance, see the section of this document relevant to each component.

ℹ

Before using the roles listed, you may want to check whether the standard roles delivered by SAP meet your requirements.

Authorizations for Customizing Settings

You can use Customizing roles to control access to the configuration of Master Data Governance in the SAP Customizing Implementation Guide (IMG).

6. Network and Communication Security

Your network infrastructure is extremely important in protecting your system. Your network needs to support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the devices and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN (local area network), they cannot exploit known bugs and security holes in network services on the server machines.

The network topology for Master Data Governance is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to Master Data Governance. Details that relate directly to SAP ERP Central Component are described in the following sections:

- Communication Channel Security [Page 11]

  This section contains a description of the communication channels and protocols that are used by the components of Master Data Governance.

- Network Security [Page 12]

  This section contains information on the network topology recommended for the components of Master Data Governance. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also contains a list of the ports required for operating the subcomponents of Master Data Governance.

- Communication Destinations [Page 12]

  This section describes the data needed for the various communication channels, for example, which users are used for which communications.

For more information, see the following section in the SAP NetWeaver Security Guide: Security Guides for Connectivity and Interoperability Technologies [External]

6.1 Communication Channel Security

Communication channels transfer a wide variety of different business data that needs to be protected from unauthorized access. SAP makes general recommendations and provides technology for the protection of your system landscape based on SAP NetWeaver. The table below shows the communication channels used by Master Data Governance, the protocol used for the connection, and the type of data transferred.

Communication Path	**Protocol Used**	**Type of Data Transferred**	**Data Requiring Special Protection**
Application Server to application server	RFC, HTTP(S)	Integration data	Business data

Application server to application of a third party administrator	HTTP(S)	Application data	For example, passwords, business data

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTP connections are protected using the Secure Sockets Layer protocol (SSL protocol).

➡

We strongly recommend that you use secure protocols (SSL, SNC).

For more information, see Transport Layer Security [External] and Web Services Security [External] in the SAP NetWeaver Security Guide.

6.2 Network Security

Since Master Data Governance is based on SAP NetWeaver technology, for information about network security, see the following sections of the SAP NetWeaver Security Guide at ▶ http://help.sap.com ▸ SAP ERP ▸ Release/Language ▸ SAP NetWeaver Library ▸ Administrator's Guide ▸ NetWeaver Security Guide ▸ Network and Communication Security ▸ Network Services◂:

Using Firewall Systems for Access Control [External]

Using Multiple Network Zones [External]

If you provide services in the Internet, you should protect your network infrastructure with a firewall at least. You can further increase the security of your system or group of systems by placing the groups in different network segments, each of which you then protect from unauthorized access by a firewall. You should bear in mind that unauthorized access is also possible internally if a malicious user has managed to gain control of one of your systems.

Ports

Master Data Governance is executed in SAP NetWeaver and uses the ports of AS ABAP or AS Java. For more information see the corresponding security guides for SAP NetWeaver in the topics for AS ABAP Ports [External] and AS Java Ports [External]. For information about other components, such as SAPinst, SAProuter, or SAP Web Dispatcher, see the document TCP/IP Ports Used by SAP Applications in SAP Developer Network at ▶ http://sdn.sap.com/irj/sdn/security under ▶ *Infrastructure Security* ▸ *Network and Communications Security*◂.

6.3 Communication Destinations

The use of users and authorizations in an irresponsible manner can pose security risks. You should therefore follow the security rules below when communicating between systems:

- Employ the user types *system* and *communication*.
- Grant a user only the minimum authorizations.
- Choose a secure password and do not divulge it to anyone else.
- Only store user-specific logon data for users of type *system* and *communication*.
- Wherever possible, use trusted system functions instead of user-specific logon data.

6.4 Use of Virus Scanners

If you upload files from application servers into Master Data Governance and you want to use an virus scanner, a virus scanner must then be active on each application server. For more information, see SAP Note 964305 (solution A).

- Work through the Customizing activities in the Implementation Guide under the Virus Scan Interface node.
- When doing this, use the virus scan profile /MDG_BS_FILE_UPLOAD/MDG_VSCAN, which is delivered for Master Data Governance

When you upload files from the front-end into Master Data Governance, the system uses the configuration you defined for virus scan profile /SIHTTP/HTTP_UPLOAD. For more information, see SAP Note 1693981.

7. Data Storage Security

Using Logical Paths and File Names to Protect Access to the File System

Master Data Governance saves data in files in the file system. Therefore, it is important to explicitly provide access to the corresponding files in the file system without allowing access to other directories or files (also known as directory traversal). This is achieved by specifying logical paths and file names in the system that map to the physical paths and file names. This mapping is validated at runtime and if access is requested to a directory that does not match a stored mapping, then an error occurs. In the application-specific part of this guide, there is a list for each component of the logical file names and paths, where it is specified for which programs these file names and paths apply.

Activating the Validation of Logical Paths and File Names

The logical paths and file names are entered in the system for the corresponding programs. For downward compatibility, the validation at runtime is deactivated by default. To activate the validation at runtime, maintain the physical path using the transactions FILE (client independent) and SF01 (client-dependent). To determine which paths are used by your system, you can activate the appropriate settings in the Security Audit Log.

More Information

- Logical File Names [External]
- Protecting Access to the File System [External]
- Security Audit Logs [External]

For information about data storage security, see the SAP NetWeaver Security Guide at ▶ http://help.sap.com ▶ *SAP NetWeaver* ▶ *Release/Language* ▶ *SAP NetWeaver Library* ▶ *Administrator's Guide* ▶ *NetWeaver Security Guide* ▶ *Security Guides for the Operating System and Database Platforms*◀

8. Enterprise Services Security

The following sections in the NetWeaver Security Guide are relevant for Master Data Governance:

- Web Services Security Guide [External]
- Recommended WS Security Scenarios [External]

9. Security-Relevant Logs and Tracing

The trace and log files of Master Data Governance use the standard mechanisms of SAP NetWeaver. For more information, see the following sections in the SAP NetWeaver Security Guide at http://service.sap.com/securityguide:

Auditing and Logging [External]

Tracing and Logging [External] (AS Java)

10. Segregation of Duties

Segregation of duties can be achieved by assigning roles to users and in addition by a strict separation of the user groups for the workflow.

Activities

Assigning Roles to Users

You can assign roles to a user using the following transactions:

- *User Maintenance SU01*

Use this transaction to assign one or more roles to one user.

- *Role Maintenance PFCG*

Use this transaction to assign one or more users to one role. Separating User Groups for the Workflow Depending on the component of Master Data Governance you intend to configure, use the following Customizing activities to separate the user groups:

Separating User Groups for the Workflow

Depending on the component of Master Data Governance you intend to configure, use the following Customizing activities to separate the user groups:

- MDG-RFM (Master Data Governance for Retail and Fashion Management)
  Run the Customizing activity under ▶ *Master Data Governance* ▸ *General Settings* ▸ *Process Modeling* ▸ *Workflow* ▸ *Rule-Based Workflow* ▸ *Configure Rule-Based Workflow* ◀ .

11. Authorization Objects and Roles Used by Master Data Governance

Authorization Objects

The following authorization objects are used by all components of Master Data Governance.

To obtain more detailed information about specific authorization objects proceed as follows:

1. Choose ▶ *SAP Menu* ▶ *Tools* ▶ *ABAP Workbench* ▶ *Development* ▶ *Other Tools* ▶ *Authorization Objects* ▶ *Objects* ▶ *(Transaction SU21).*
2. Select the authorization object using (Find) and then choose (Display).
3. On the *Display authorization object* dialog box choose *Display Object Documentation*.

Authorization Object	Description
MDG_MDF_TR	Master Data: Transport
MDG_IDM	Key Mapping
USMD_CREQ	Change Request
USMD_MDAT	Master Data
USMD_UI2	UI Configuration
DRF_RECEIVE	Authorization for outbound messages for receiver systems
DRF_ADM	Create Outbound Messages
CA_POWL	Authorization for iViews for personal object worklists
BCV_SPANEL	Execute Side Panel
BCV_USAGE	Usage of Business Context Viewer
MDG_DEF	Data Export
MDG_DIF	Data Import
S_DMIS	Authority object for SAP SLO Data migration server

Standard Role

Role	**Name**
MDG-RFM	
/UGI4/MDGRFM_MENU	Master Data Governance for Article: Menu
/UGI4/MDGRFM_REQ	Master Data Governance for Article: Requester
/UGI4/MDGRFM_SPEC	Master Data Governance for Article: Specialist
/UGI4/MDGRFM_STEW	Master Data Governance for Article: Data Steward
/UGI4/MDGRFM_DISP	Master Data Governance for Article: Display
MDG-RFM for FMS	
/UGI4/MDGRFM_FMS_MENU	Master Data Governance for FMS: Menu
/UGI4/MDGRFM_FMS_REQ	Master Data Governance for FMS: Requester
/UGI4/MDGRFM_FMS_SPEC	Master Data Governance for FMS: Specialist
/UGI4/MDGRFM_FMS_STEW	Master Data Governance for FMS: Data Steward
/UGI4/MDGRFM_FMS_DISP	Master Data Governance for FMS: Display

This role contains authorizations needed for administrative tasks and for setting up a base configuration in all components of Master Data Governance. Some authorizations enable critical activities. If multiple users in your organization are entrusted with the administration and configuration of Master Data Governance, we recommend that you split the role into several roles, each with its own set of authorizations. The role does not contain the authorizations for the respective master data transactions.

12. Change Settings of Generated MDG Database Tables

The SAP system generates database tables for the entities of all defined data models. The settings of these database tables are the following:

- Buffering and log of data changes is switched on.
- Display and maintenance is allowed with restrictions.

Activities

To change these settings of generated MDG database tables run the transaction `MDG_TABLE_ADJUST`.

The results of the transaction are listed in the transaction `SLG1` (*Analyse Application Log*), using Object `FMDM` and *Subobject* `ADJUST_TABLE`.

⚠

- You have to execute the transaction in each system manually.
- After a model activation it might be necessary to execute the transaction again

More Information

For more information see SAP note 1828363

13. Appendix

For more information about the security of SAP applications see SAP Service Marketplace at http://service.sap.com/security .

You can also access additional security guides via SAP Service Marketplace at http://service.sap.com/securityguide.

For more information about security issues, see SAP Service Marketplace at http://service.sap.com followed by:

Topic	**SAP Service Marketplace**
Master guides, installation guides, upgrade guides, and Solution Management guides	/instguides
	/ibc
Related notes	/notes

Platforms	/platforms
Network security	/network /securityguide
Technical Infrastructure	/ti
SAP Solution Manager	/solutionmanager