Configuring LDAP Connector in Compliant User Provisioning of GRC Access Control (Formerly Virsa Access Enforcer)

Applies to:

SAP GRC Access Control, release 5.x

Summary

When implementing compliant user provisioning in GRC Access Control the system is typically linked to a LDAP repository. This paper outlines the configuration of LDAP connector and provides sample mappings for Active Directory, SunOne, E-Directory, and Tivoli.

Authors: Alpesh Parmar, Aman Chuttani

Company: SAP

Created on: 21 January 2008

Author Bio

Alpesh Parmar is a principal consultant at Regional Implementation Group (RIG) SAP GRC. He is an expert in GRC Access Control and was instrumental in many successful Access Control ramp-up implementations. Prior to joining RIG he was part of the Access Control development team.

Aman Chuttani works as a consultant in SAP's GRC RIG. He has gained extensive experience supporting SAP's customers in the implementation of SAP GRC Access Control.

Table of Contents

Configuring LDAP System for Compliant User Provisioning in GRC Access Control

Connectors facilitate the transfer of data between Compliant User Provisioning (formerly Virsa Access Enforcer) and LDAP systems. Compliant User Provisioning (formerly Virsa Access Enforcer) supports different LDAP types. They include:

- Microsoft Active Directory
- SunOne
- Novell E-Directory
- IBM Tivoli

There are two important tasks which are required in order to have a successful communication between the Compliant User Provisioning (formerly Virsa Access Enforcer) and the LDAP systems. These include:

- Configuring an LDAP connector
- Mapping the LDAP fields to Compliant User Provisioning fields

Configuring LDAP Connector

Following is the description of fields in the LDAP connector screen:

Name: Input a name for the LDAP connector. This is a free form text.

Short Description: Input text such that it is easily distinguishable from other connectors since the text entered in this field will be displayed in various screens of AE.

Description: Input a larger description of the connector if you like.

Server Name: Input the server name hosting the LDAP directory. It is better to input the fully qualified name. An IP address will work too.

Domain: Input the domain name or the base of the directory. Following two formats are supported. 1. “DC=sap,DC=com”, 2. “sap.com”

Port: Input the port assigned to the directory server.

User Principal Name: Input the service user Id which will be used to access the directory.

Password: Input password of the service user.

User Path: Input the distinguished name of the root directory under which all the users/employees are stored. Please remove the domain components from the distinguished name.

Group Path: Leave this field blank. This field is not being used in Compliant User Provisioning (formerly Virsa Access Enforcer).

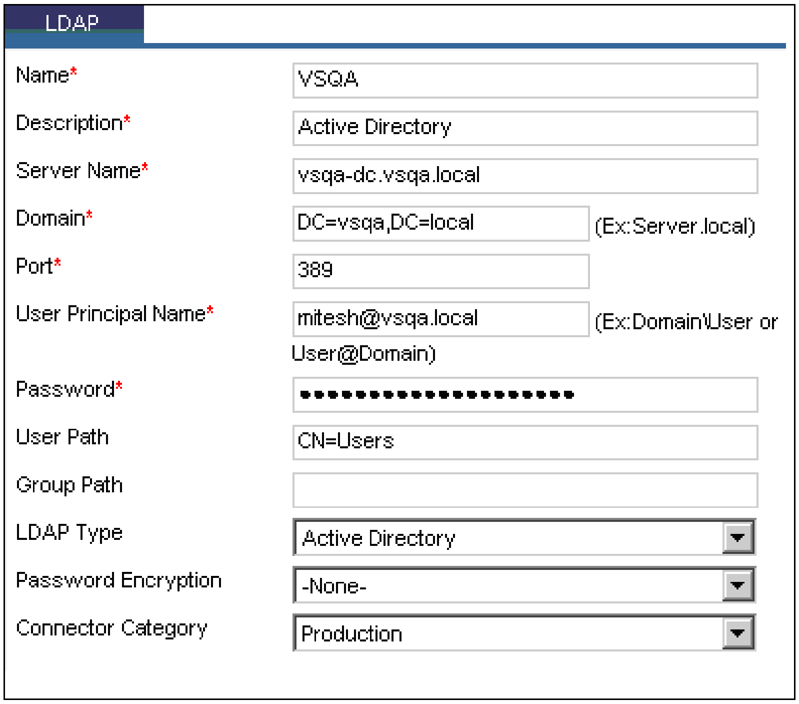
LDAP Type: Select the directory type which is being used.

Password Encryption: Select encryption type to be utilized by the LDAP server.

Connection Category: Select Production or Non-Production.

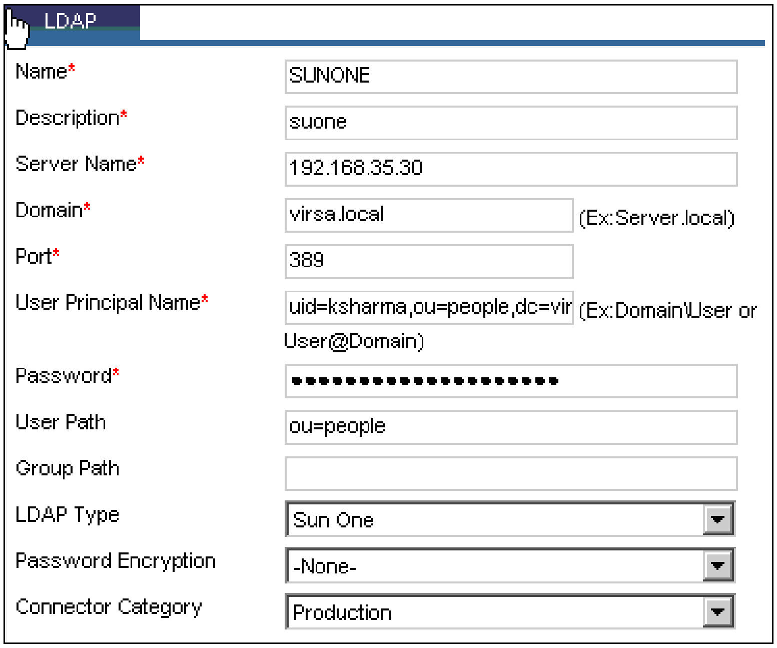
Sample Connector Configuration for Different LDAP Types

Active Directory:



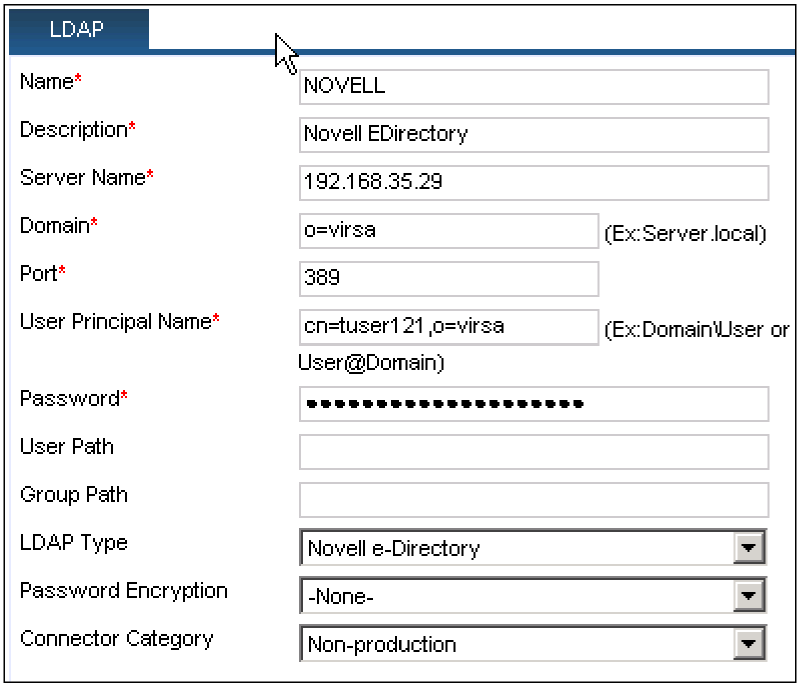
Name*	VSQA	
Description*	Active Directory	
Server Name*	vsqa-dc.vsqa.local	
Domain*	DC=vsqa,DC=local	(Ex:Server.local)
Port*	389	
User Principal Name*	mitesh@vsqa.local	(Ex:Domain\User or User@Domain)
Password*	••••••••••••••••••••	
User Path	CN=Users	
Group Path		
LDAP Type	Active Directory	
Password Encryption	-None-	
Connector Category	Production	

SunOne:



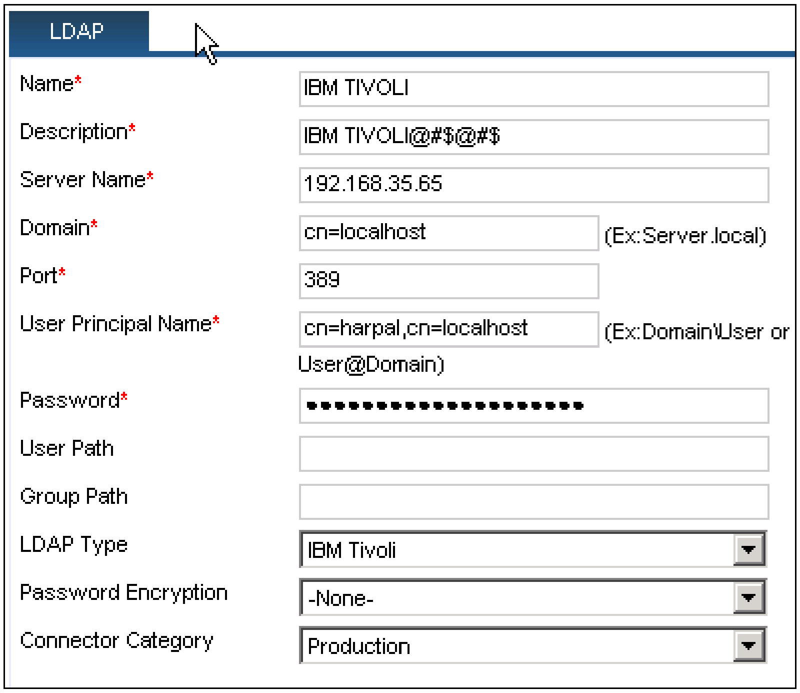
Name*	SUNONE	
Description*	suone	
Server Name*	192.168.35.30	
Domain*	virsa.local	(Ex:Server.local)
Port*	389	
User Principal Name*	uid=ksharma,ou=people,dc=vir	(Ex:Domain\User or User@Domain)
Password*	••••••••••••••••••••	
User Path	ou=people	
Group Path		
LDAP Type	Sun One	
Password Encryption	-None-	
Connector Category	Production	

Novell's E-Directory:



Name*	NOVELL	
Description*	Novell EDirectory	
Server Name*	192.168.35.29	
Domain*	o=virsa	(Ex:Server.local)
Port*	389	
User Principal Name*	cn=tuser121,o=virsa	(Ex:Domain\User or User@Domain)
Password*	••••••••••••••••••••	
User Path		
Group Path		
LDAP Type	Novell e-Directory	
Password Encryption	-None-	
Connector Category	Non-production	

IBM Tivoli:



Name*	IBM TIVOLI	
Description*	IBM TIVOLI@#$@#$	
Server Name*	192.168.35.65	
Domain*	cn=localhost	(Ex:Server.local)
Port*	389	
User Principal Name*	cn=harpal,cn=localhost	(Ex:Domain\User or User@Domain)
Password*	••••••••••••••••••••	
User Path		
Group Path		
LDAP Type	IBM Tivoli	
Password Encryption	-None-	
Connector Category	Production	

Mapping LDAP Fields

The LDAP mapping helps in mapping the fields between Compliant User Provisioning and corresponding LDAP fields (attributes). The field values are accordingly pulled from the LDAP directory and populated in Compliant User Provisioning. Most of the fields in the LDAP mapping screen are self explanatory except for few. Those fields are explained below.

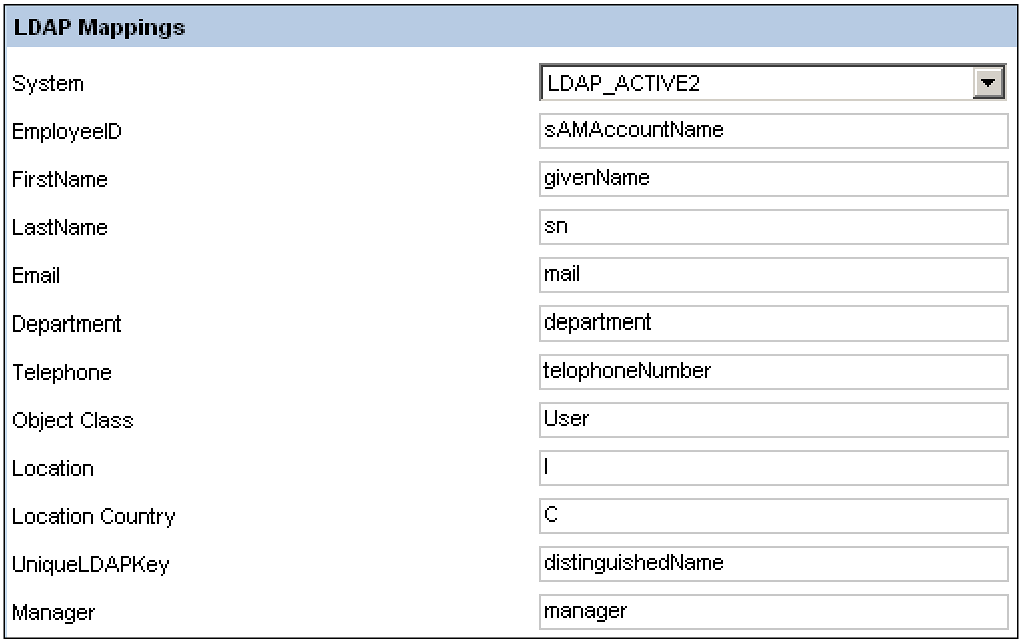
- Object Class
- UniqueLDAPKey

Object Class is the Common-Name (cn) of the object class attribute (or super class) of the users/employees/people.

UniqueLDAPKey is the attribute name which holds the DN of the user/employee/people objects.

Sample LDAP Mapping Screenshots for Different Directory Types

LDAP Mapping for Microsoft Active Directory

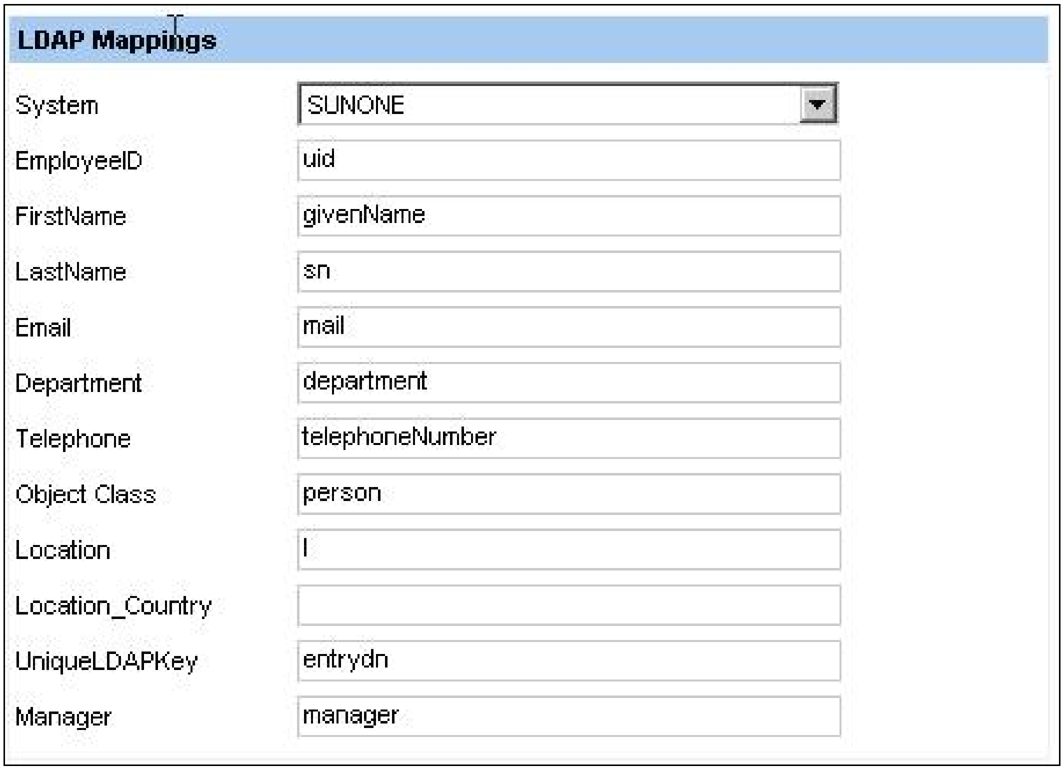


LDAP Mappings

System	LDAP_ACTIVE2
EmployeeID	sAMAccountName
FirstName	givenName
LastName	sn
Email	mail
Department	department
Telephone	telophoneNumber
Object Class	User
Location	l
Location Country	C
UniqueLDAPKey	distinguishedName
Manager	manager

AE Field	**LDAP Mapped Field**	**Description**
EmployeeID	sAMAccountName	Default field for account name.
FirstName	givenName	Default field for first name
LastName	Sn	Default field for last name
Email	Mail	Default field for email ID
Department	Department	Default field for department
Telephone	telephoneNumber	Default field for telephone number
ObjectClass	User	Default structure for the user details
Location	L	Default field for base location
Location_Country	C	Default field for country
UniqueLDAPKey	distinguishedName	Unique key in the LDAP system
Manager	Manager	Default field for manager ID

LDAP MAPPING for SUNONE

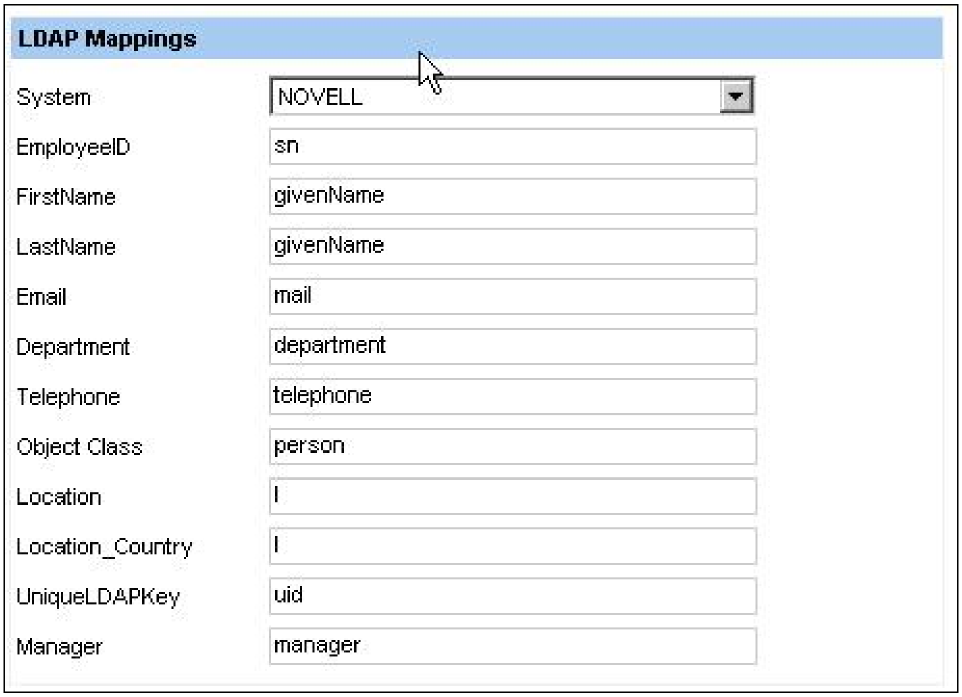


LDAP Mappings

System	SUNONE
EmployeeID	uid
FirstName	givenName
LastName	sn
Email	mail
Department	department
Telephone	telephoneNumber
Object Class	person
Location	l
Location_Country	
UniqueLDAPKey	entrydn
Manager	manager

AE Field	LDAP Mapped Field	Description
EmployeeID	Uid	Default field for account name.
FirstName	givenName	Default field for first name
LastName	Sn	Default field for last name
Email	Mail	Default field for email ID
Department	Department	Default field for department
Telephone	telephoneNumber	Default field for telephone number
ObjectClass	Person	Default structure for the user details
Location	L	Default field for base location
Location_Country	C	Default field for country
UniqueLDAPKey	Entrydn	Unique key in the LDAP system
Manager	Manager	Default field for manager ID

LDAP Mapping for Novell's E-Directory

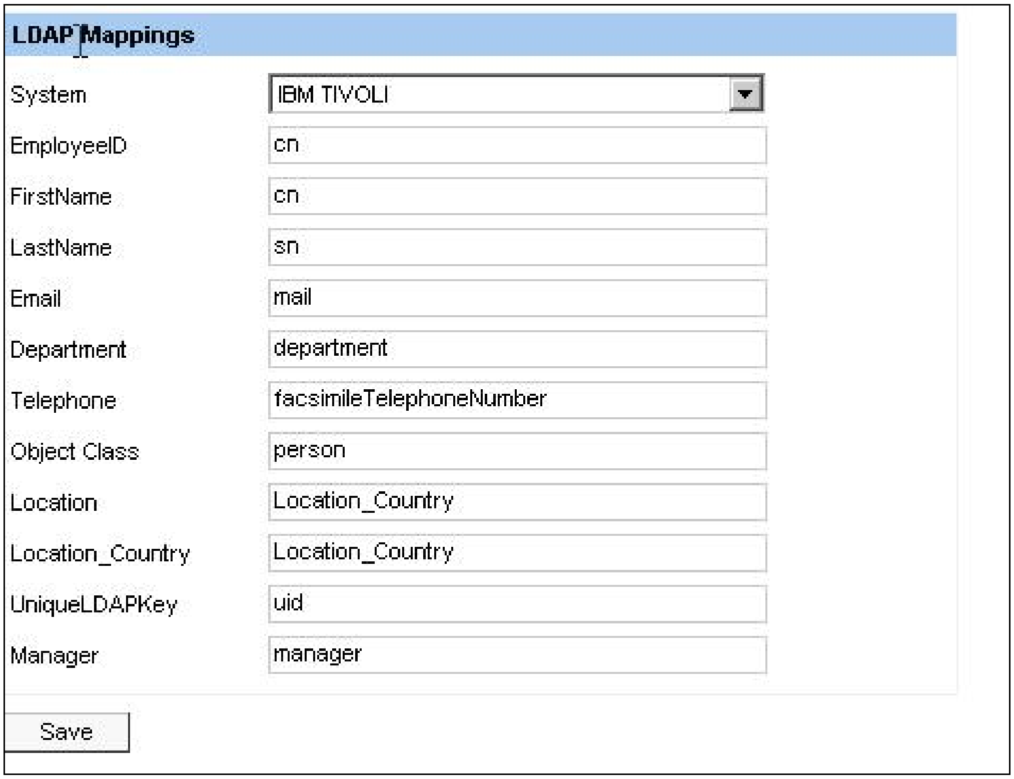


LDAP Mappings

System	NOVELL
EmployeeID	sn
FirstName	givenName
LastName	givenName
Email	mail
Department	department
Telephone	telephone
Object Class	person
Location	l
Location_Country	l
UniqueLDAPKey	uid
Manager	manager

AE Field	LDAP Mapped Field	Description
EmployeeID	Sn	Default field for account name.
FirstName	GivenName	Default field for first name
LastName	GivenName	Default field for last name
Email	Mail	Default field for email ID
Department	Department	Default field for department
Telephone	Telephone	Default field for telephone number
ObjectClass	User	Default structure for the user details
Location	L	Default field for base location
Location_Country	L	Default field for country
UniqueLDAPKey	Uid	Unique key in the LDAP system
Manager	Manager	Default field for manager ID

LDAP Mapping for IBM Tivoli



LDAP Mappings

System	IBM TIVOLI
EmployeeID	cn
FirstName	cn
LastName	sn
Email	mail
Department	department
Telephone	facsimileTelephoneNumber
Object Class	person
Location	Location_Country
Location_Country	Location_Country
UniqueLDAPKey	uid
Manager	manager

AE Field	**LDAP Mapped Field**	**Description**
EmployeeID	Cn	Default field for account name.
FirstName	Sn	Default field for first name
LastName	Sn	Default field for last name
Email	Mail	Default field for email ID
Department	Department	Default field for department
Telephone	facsimileTelephoneNumber	Default field for telephone number
ObjectClass	Person	Default structure for the user details
Location	Location_Country	Default field for base location
Location_Country	Location_Country	Default field for country
UniqueLDAPKey	Uid	Unique key in the LDAP system
Manager	Manager	Default field for manager ID

Copyright

These materials are subject to change without notice. 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.

These materials are provided “as is” without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

Any software coding and/or code lines/strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.