Security Guide

SAP Identity Management 7.2
Document Version: 11 – 2017-02-20

PUBLIC

SAP NetWeaver Identity Management Security Guide

Content

1 SAP NetWeaver Identity Management Security Guide

This document provides an overview of the security-relevant information that applies to SAP NetWeaver Identity Management.

⚠ Caution

This guide does not replace the daily operations handbook that we recommend customers to create for their specific productive operations.

Target Audience

The target audience for this document is as follows:

- Technology 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, whereby the Security Guides provide 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 on your system should not result in loss of information or processing time.

The SAP NetWeaver Identity Management will have a central role in managing accounts and access rights in other applications. Any unauthorized changes to data in the Identity Management solution may therefore also affect other applications.

To assist you in securing the identity management solution, we provide this Security Guide.

Additional Documentation Resources

The most important SAP Notes that apply to the security of the SAP NetWeaver Identity Management, abbreviated Identity Management, are shown in the table below.

Table 1: Important SAP Notes

SAP Note Number	Title
1498369	SAP NetWeaver Identity Management 7.2

For more information about specific topics, see the quick links as shown in the table below.

Table 2: Quick Links to Additional Information

Content	Quick Link on the SAP Service Marketplace
Security	`service.sap.com/security`
Security Guides SAP NetWeaver Security Guide: The sections about SAP logon tickets and Secure Network Communications contain relevant information	`service.sap.com/securityguide`
Related SAP Notes	https://support.sap.com/notes
Released platforms	`service.sap.com/platforms`
Network security	`service.sap.com/network`

2 Technical System Landscape

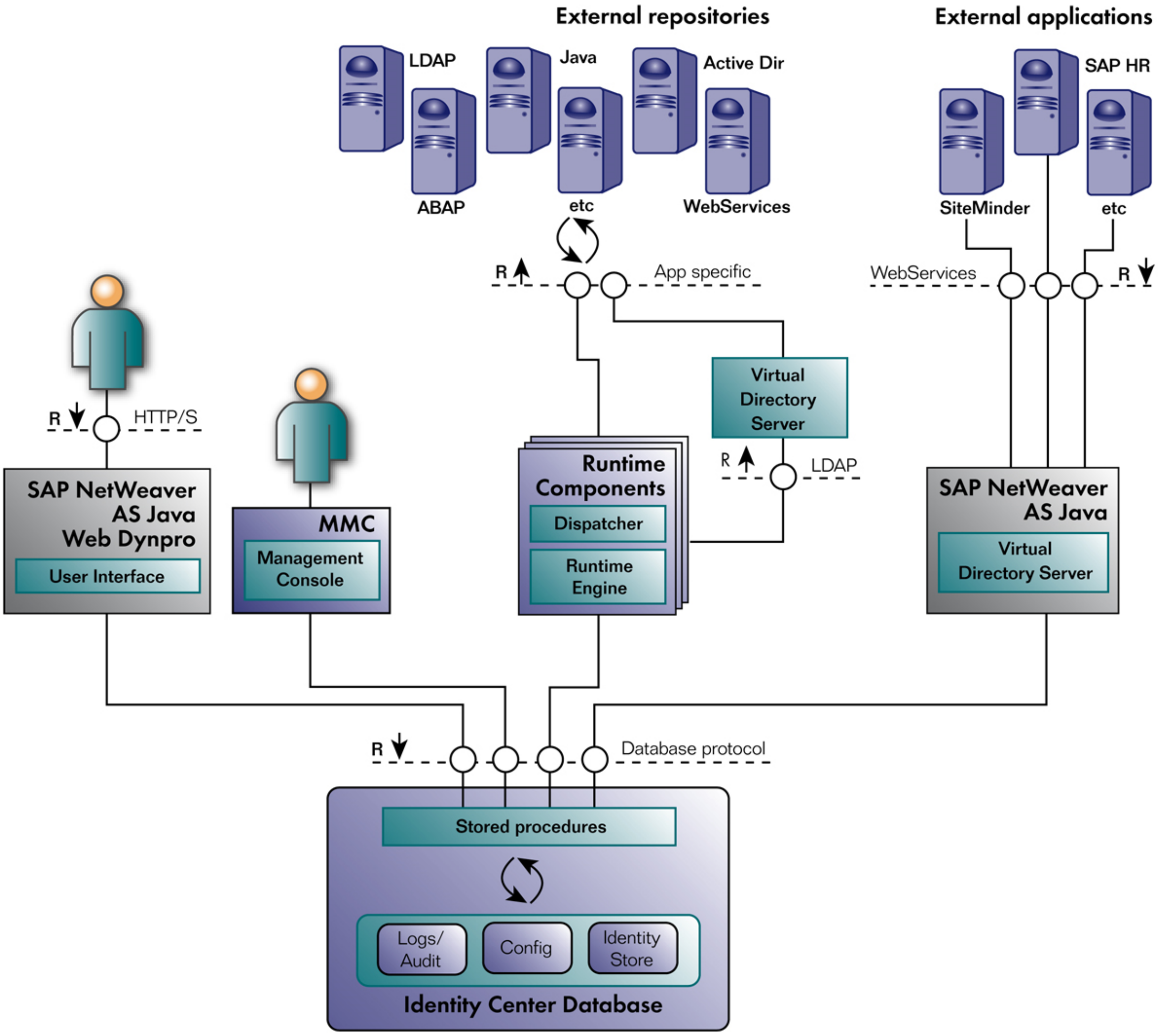
This section provides an overview of the technical components and communication paths that are used by the Identity Management.

Related Information

Architecture [page 7]
Usage [page 9]

2.1 Architecture

The figure below shows an overview of the technical system landscape for the SAP NetWeaver Identity Management.



The Identity Center database is used to hold all information about managed users and corresponding account information. All communication between the applications and the database uses the database libraries. In addition, external repositories are accessed from the Identity Center and Virtual Directory Server, to create user accounts and manage access rights. Which systems are accessed, depends on each specific implementation.

Note

The separate components have different installation jobs, and although it is possible to install everything (including the database) on the same server, different servers will be used in a production environment.

The Virtual Directory Server uses separate configuration files, which may be stored in the database. The Virtual Directory Server is deployed on SAP NetWeaver AS Java. By default logging for the Virtual Directory Server is done to SAP NetWeaver, but the logging is configurable.

The Identity Management User Interface is deployed on SAP NetWeaver AS Java.

To achieve high availability, as well as load balancing, the Identity Center solution should be installed on multiple servers.

The database should be clustered.

The Runtime Components should be installed on all servers running SAP NetWeaver AS Java. The Virtual Directory Server may also be installed on these same or separate servers.

For more information about the technical system landscape, see the resources listed in the Related Information section.

Related Information

SAP NetWeaver Identity Management Installation Guide
SAP NetWeaver Identity Management Solution Operation Guide
SAP NetWeaver Identity Management Identity Center Implementation guide - Disaster recovery

2.2 Usage

The Identity Management is used to manage accounts and access rights in other applications.

Information about all users and the corresponding accounts are held in the Identity Center database. The Runtime Components and the Virtual Directory Server are used to manage the users in the target systems.

The Identity Management User Interface provides self-service and management functions based on the task configuration of the identity store. The User Interface also provides monitoring functionality depending on access rights, as described in *Identity Management User Interface Authorizations* section.

Related Information

Identity Management User Interface Authorizations [page 13]

3 User Administration and Authentication

This section describes user administration and authentication for the different components of SAP NetWeaver Identity Management.

Related Information

Identity Center Database Logins and Roles [page 10]
Admin Login [page 11]
Run-time Login [page 12]
Binding Database Users to Operating System [page 12]
Identity Management User Interface Login [page 12]
Virtual Directory Server Login [page 12]

3.1 Identity Center Database Logins and Roles

When a new Identity Center database is created, a number of database roles and logins are also created, as described in this section. If required, additional database logins can be created, and given access rights, by assigning roles. This has to be done using the corresponding database administrator tool.

In the list of roles and logins below, all start with `mxmc_`. This is the default prefix when installing the Identity Center database. If a database is installed with a different prefix, all roles and user are created accordingly.

Table 3:

Login	Role	Description
`mxmc_oper`	`db_owner/dbo`	This login is the owner of the database, and has full access to all tables. It should only be used for database upgrades.
`mxmc_rt`	`mxmc_rt_role`	This login is only used by the Runtime Components, and has a very limited access to the database.
`mxmc_prov`	`mxmc_prov_role` `mxmc_transport_role`	This login is only used by the Identity Management User Interface, and has the necessary access rights for doing all the provisioning operations.

Login	Role	Description
mxmc_admin	mxmc_admin_role mxmc_delta_rw_role	A login with these roles has to be used when implementing an identity management solution in the Identity Center. It has all the necessary access rights for creating tasks, jobs and other objects in the database. It is highly recommended to create individual database users for each person/ role who needs access to the Identity Center database, as this will provide the necessary audit information for who made which changes when.
mxmc_user	mxmc_user_role mxmc_delta_r_role	A login with these roles has mostly read access to the database, and can be used to inspect the configuration in the Management Console. The same recommendation as for the mxmc_admin also applies for mxmc_user.

Note

On Microsoft SQL server, users are created in addition to logins. The users are created in the database context, and has the same name as the login, followed by _u, for example mxmc_admin_u.

3.2 Admin Login

The *SAP NetWeaver Identity Management Identity Center Getting Started* document describes how to add an Identity Center to the configuration UI, using the connection wizard.

For security reasons, the optional parameter *Allow password saving* should not be checked for the Admin user. In this case, the user will be prompted for the password, every time connecting to the database. If several people are using the configuration UI, separate logins should be created for each user. The mxmc_admin or mxmc_user role can be used, depending on the access required.

3.3 Run-time Login

The run-time (RT) connection string must (unless the RT login is bound to an operating system login) have the *Allow password saving* set, as this is running as a background process, and there is no user to provide the password.

If using an operating system login, the service must be running at this user.

3.4 Binding Database Users to Operating System

On Microsoft Windows, it is possible to bind a Microsoft SQL Server database login to a Microsoft Windows login. This will avoid storing passwords in the connection string. For details on how to do this, and how to define the connection strings, see the documentation for the Microsoft SQL Server.

3.5 Identity Management User Interface Login

The Identity Management User Interface is a WebDynPro application that is configured and deployed on SAP NetWeaver AS Java. The connection string is configured in the SAP NetWeaver Visual Administrator using the `mxmc_prov` user. Storing and securing this connection string is handled by SAP NetWeaver AS Java.

Authentication of the users logging on to the User Interface is done by the User Management Engine (UME).

Normal users must also have an entry in the Identity Center's identity store with an MSKEYVALUE identical to the User ID in the UME.

3.6 Virtual Directory Server Login

The Virtual Directory Server authenticates the users against a table of users in the Virtual Directory Server configuration file, which holds the login name (which may be a DN, but this is not a requirement) in addition to a hashed password.

The Virtual Directory Server architecture allows for plugging in external authentication.

4 Authorization

This section describes authorization for the Identity Management.

Related Information

Identity Management User Interface Authorizations [page 13]
Identity Management Authorizations for Reporting Using SAP NetWeaver BW [page 17]
Authorizations for Identity Management REST Interface Version 2 and Identity Management User Interface for HTML5 [page 17]

4.1 Identity Management User Interface Authorizations

This section describes Identity Management User Interface authorizations.

Related Information

Access to the Identity Management User Interfaces (URLs) [page 13]
Providing General Access (UME Actions) [page 14]
Providing Specific Access (Identity Management Privileges) [page 14]

4.1.1 Access to the Identity Management User Interfaces (URLs)

There are three URLs that can be used to access the Identity Management User Interface:

- `http://<host>:<port>/idm` to access the main Identity Management User Interface containing the self-service tab and the manager tabs:
    - *Self Services* tab: giving general access (access to the self service tasks).
    - *To Do* tab: for handling of approvals.
    - *Manage* tab: for search and managing of entries.
    - *View Reports* tab: for viewing of the generated reports.

    - *History* tab: providing the status and history of the tasks executed.
- `http://<host>:<port>/idm/admin` to access the administrator tabs of the Identity Management Administration User Interface. The following tabs are available from this URL:
    - *Monitoring* tab: for system monitoring purposes and viewing logs. For more information about Monitoring, see *SAP NetWeaver Identity Management Solution Operation Guide*.
    - *Trace* tab: for viewing and downloading the entry trace. For more information about the entry trace, see *SAP NetWeaver Identity Management Solution Operation Guide*.
    - *Transport* tab: for transport of functionality and configuration (export and import). For more information about transport, see *SAP NetWeaver Identity Management Identity Center Implementation Guide: Transport*.
    - *Configuration History* tab: for viewing of all changes made to the configuration.
    - *System Parameters* tab: for viewing and changing of the configuration.
    - *Statement Execution* tab: for analyzing the performance of SQL queries. For more information, see *SAP NetWeaver Identity Management Solution Operation Guide*.
    - *Message Templates* tab: for viewing and editing message templates. For more information, see *SAP NetWeaver Identity Management Solution Operation Guide*.
- `http://<host>:<port>/idm/pwdreset` to run the password reset task. For more information, see *SAP NetWeaver Identity Management Identity Center Implementation Guide: Selfservice password reset*.

4.1.2 Providing General Access (UME Actions)

What parts of the User Interface is available depends on which UME actions are assigned to the user:

- `sap.com_tc~idm~jmx~ump.idm_authenticated` gives general access to the application and enables the *Self Services* tab.
- `sap.com_tc~idm~jmx~ump.idm_anonymous` provides access to the Password reset task. For details, see the document *SAP NetWeaver Identity Management Identity Center Implementation Guide – Self-service password reset*.
- `sap.com_tc~idm~jmx~ump.idm_monitoring_administration` or `sap.com_tc~idm~jmx~ump.idm_monitoring_support` enables the *Monitoring* tab.

4.1.3 Providing Specific Access (Identity Management Privileges)

Access to the other tabs in the User Interface is controlled by assigning privileges in the identity store to the person entries.

Related Information

Privileges for the Identity Management User Interface [page 15]

Privileges for the Identity Management Administration User Interface [page 15]

4.1.3.1 Privileges for the Identity Management User Interface

These are the privileges that specify access in the Identity Management User Interface (in alphabetical order):

Table 4:

Privilege	Description
MX_PRIV:MANAGED_APPROVALS:PROCESS	Gives access to the *Approval Management* tab. This tab provides a manager an overview over approvals assigned to users that he/she is manager for and he/she can escalate or decline the approval, if necessary.
MX_PRIV:MANAGED_APPROVALS:READONLY	Gives read only access to the *Approval Management* tab. This tab provides a manager an overview over approvals assigned to users that he/she is manager for.
MX_PRIV:WD:TAB_HISTORY	Gives access to the *History* tab. This tab provides the status and history of the tasks executed on own entry (self service tasks), on other entries (tasks available from the *Manage* tab) and the approvals.
MX_PRIV:WD:TAB_MANAGE	Gives access to the *Manage* tab. From this tab, the user is able to search for entries in the identity store and perform tasks on (manage) these. Which tasks are available is controlled by the access control defined on each task.
MX_PRIV:WD:TAB_REPORT	Gives access to the *View Reports* tab. In this tab, the generated reports can be viewed.
MX_PRIV:WD:TAB_TODO	Gives access to the *To Do* tab. In this tab, the approvals can be handled.

4.1.3.2 Privileges for the Identity Management Administration User Interface

These are the privileges that specify access in the Identity Management Administration User Interface (in alphabetical order):

Table 5:

Privilege	Description
MX_PRIV:APPROVALS:PROCESS	Gives access to the *Approval Management* tab. This tab provides an administrator an overview over all approvals in the system and he/she can escalate or decline the approval, if necessary.
MX_PRIV:APPROVALS:READONLY	Gives read only access to the *Approval Management* tab. This tab provides an administrator an overview over all approvals in the system.
MX_PRIV:CONFIG_AUDIT	Gives access to the *Configuration History* tab.
MX_PRIV:CONFIG_R	Gives read access to the *System Parameters* tab, that is, the user is only allowed to view the system parameter values in the *System Parameters* tab.
MX_PRIV:CONFIG_RW	Gives both read and write access to the *System Parameters* tab, that is, the user is allowed to both view and change the parameter values. This privilege always overrides the privilege MX_PRIV:CONFIG_R.
MX_PRIV:TRANSPORT:EXPORT	Gives access to the *Transport* tab, but only enables the export functionality. If the same user is to perform both export and import, then both transport privileges (MX_PRIV:TRANSPORT:EXPORT and MX_PRIV:TRANSPORT:IMPORT) need to be assigned to the user in question.
MX_PRIV:TRANSPORT:IMPORT	Gives access to the *Transport* tab, but only enables the import functionality. If the same user is to perform both export and import, then both transport privileges (MX_PRIV:TRANSPORT:EXPORT and MX_PRIV:TRANSPORT:IMPORT) need to be assigned to the user in question.
MX_PRIV:WD:MSGTEMPLATE:R	Provides read access to the *Message Templates* tab. This tab is used to maintain the templates used when sending messages from a notification task. For more information, see *SAP NetWeaver Identity Management Solution Operations Guide*.
MX_PRIV:WD:MSGTEMPLATE:RW	Provides both read and write access to the *Message Templates* tab. This tab is used to maintain the templates used when sending messages from a notification task. For more information, see *SAP NetWeaver Identity Management Solution Operations Guide*.
MX_PRIV:WD:TAB_THRESHOLD	Gives access to the *Statement Execution* tab. This tab is used to analyze the performance of SQL queries in the configuration. For more information about using the trace, see *SAP NetWeaver Identity Management Solution Operations Guide*.

Privilege	Description
MX_PRIV:WD:TAB_TRACE	Gives access to the *Trace* tab. This tab is used to configure and view trace information that can be used for troubleshooting purposes. For more information about using the trace, see *SAP NetWeaver Identity Management Solution Operations Guide*.

4.2 Identity Management Authorizations for Reporting Using SAP NetWeaver BW

When using SAP NetWeaver BW for identity reporting, it is possible to set up the authorizations so that managers and owners of objects are limited to seeing those identities, privileges, or roles for which they are responsible.

For this purpose, the following roles are delivered with the BI content for identity management:

Table 6:

Role	Description
SAP_BW_IDM_REP_ADMIN	A user with the SAP_BW_IDM_REP_ADMIN role will see all entries requested by the query.
SAP_BW_IDM_REP_OWNER	A user with the SAP_BW_IDM_REP_OWNER role will only see those identity or objects for which he or she is the owner. The ownership is determined for the logged on user for the current point in time based on the identity center attribute MX_OWNER.
SAP_BW_IDM_REP_MANAGER	A user with the SAP_BW_IDM_REP_MANAGER role will only see those identity or objects for which he or she is the manager. The relationship is determined for the logged on user for the current point in time based on the identity center attribute MX_MANAGER.

4.3 Authorizations for Identity Management REST Interface Version 2 and Identity Management User Interface for HTML5

This section describes authorizations for Identity Management REST Interface Version 2 and Identity Management User Interface for HTML5.

Related Information

Identity Management REST Interface Version 2 [page 18]
Identity Management User Interface for HTML5 [page 18]

4.3.1 Identity Management REST Interface Version 2

The Identity Management REST Interface requires the following UME actions:

- `sap.com_tc~idm~jmx~ump.idm_authenticated`
- `sap.com_tc~idm~jmx~ump.idm_authenticated_restapi`

For more information, see the *Security* section in *SAP NetWeaver Identity Management REST Interface Version 2 Technical Reference*.

4.3.2 Identity Management User Interface for HTML5

For Identity Management User Interface for HTML5, the following additional UME actions are required:

- `sap.com_tc~idm~jmx~ump.idm_authenticated_ui5`

The role `idm.user` includes all these actions and can be assigned to the users to provide access to the Identity Management User Interface for HTML5.

5 Integration into Single Sign-On Environments

We strongly recommend using a single sign-on (SSO) solution to provide central authentication for you system landscape. For more information about SAP's SSO solution, see the Related Information section.

If it is not possible to use SSO for some or all systems, SAP NetWeaver Identity Management's password synchronization can be deployed to ensure that the user has the same password in the respective or all systems which support the password synchronization feature. See the *Password Hook* section.

Related Information

User Authentication and Single Sign-On

Password Hook [page 50]

6 Network and Communication Security

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

Related Information

Identity Management User Interface: HTTP Security (SSL) and Clickjacking Protection [page 20]
Identity Management User Interface for HTML 5: HTTP Security (SSL) [page 21]
Identity Center: Database Security [page 21]
Identity Center: Repository Security [page 21]
Identity Center: SSL Security [page 21]
Virtual Directory Server: SSL Security [page 27]
Securing AS ABAP Connections [page 28]
Securing Connections for Reporting Using SAP NetWeaver BW [page 28]
Firewall Settings [page 29]
AS ABAP Connections [page 29]
AS Java Connections [page 30]
SAP HANA Connections [page 30]
External Applications Credentials [page 30]

6.1 Identity Management User Interface: HTTP Security (SSL) and Clickjacking Protection

Security between the end user and the web application is done by securing the web server, and is outside the scope of Identity Center security. Make sure to use HTTPS to secure the connection between the clients and the web server.

To prevent malicious applications from misusing the Web Dynpro Java application Identity Management User Interface for clickjacking attacks, you need to enable the clickjacking protection service for the AS Java. See how to enable it for your SAP NetWeaver version:

- Enabling the Clickjacking Protection Service for SAP NetWeaver 7.3
- Enabling the Clickjacking Protection Service for EHP 1 for SAP NetWeaver 7.3
- Enabling the Clickjacking Protection Service for SAP NetWeaver 7.4

6.2 Identity Management User Interface for HTML 5: HTTP Security (SSL)

Security between the end user and the web application is done by securing the web server, and is outside the scope of Identity Center security. Make sure to use HTTPS to secure the connection between the clients and the web server.

6.3 Identity Center: Database Security

All connections between the components and the database uses standard database protocols, and are defined using database connection strings. To secure these, please use the secure connection strings, as defined by the database.

6.4 Identity Center: Repository Security

Communication with the repositories uses either LDAP, SPML, database or application specific communication. The communication options are defined for each job connecting to the given repository.

The LDAP protocol supports simple authentication, SSL, NTLM or Kerberos.

SPML supports SSL.

For database connections, either JDBC or OLEDB connection strings are used, and security is handled by the corresponding database library.

For application specific communication, security must be considered in each case.

6.5 Identity Center: SSL Security

This section describes how you install the necessary certificates to be used for SSL communication and how you connect to an LDAP or SPML server over SSL.

Related Information

SSL Communication Using the Java Runtime Engine [page 22]

SSL Communication Using the Windows Runtime [page 25]

6.5.1 SSL Communication Using the Java Runtime Engine

The Java Runtime Engine supports SSL both for LDAP and SPML communication. In both cases you need keystore(s) with the necessary certificate(s).

Related Information

Installing the Certificate [page 22]
Connecting to an LDAP Server over SSL [page 23]
Connecting to an SPML Server over SSL [page 24]

6.5.1.1 Installing the Certificate

To be able to connect securely to a server using SSL, you must have the certificate, either of the server itself, or by the authority which issued the server certificate. This should be exported as a file with extension `.der`.

This certificate has to be imported to the keystores of all servers with dispatchers needing SSL communication with the server.

The default keystore for the certificate is: `<JAVA_HOME>\lib\security\cacerts`.

This location depends on the location of your Java Virtual Machine.

To install the server certificate, you must use the keytool utility: `<JAVA_HOME>\bin\keytool`. For more information, see keytool - Key and Certificate Management Tool .

To install the certificate, issue the following command (in one line):

```
keytool -import -alias <local certificate name> -keystore cacerts
<JAVA_HOME>\lib\security\cacerts> -file <certificate file> -storepass
<password>
```

`<local certificate name>` is the name you want to give this certificate. This can be any name accepted by keytool.

If the keystore (cacerts) file does not exist, it will be created.

The initial password of the cacerts keystore is **`changeit`**. System administrators should change that password and the default access permissions of that file after installing the JDK.

6.5.1.2 Connecting to an LDAP Server over SSL

This section describes how you connect to an LDAP server using SSL. Authentication is done using the LDAP directory login and password, which is sent over this secure channel. The connection is configured in a To or From LDAP directory pass.

Prerequisites

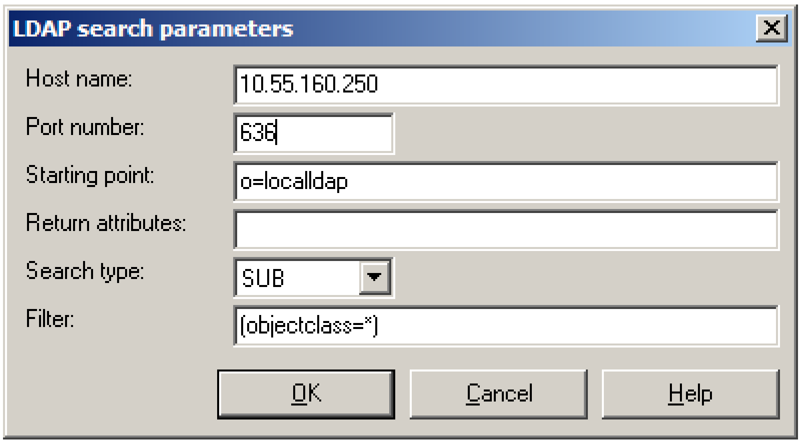
The certificate used to authenticate against the directory server is available in the keystore. See Installing the Certificate [page 22].

Context

You configure the connection details on the *Source* or *Destination* tab of the To or From LDAP directory pass. In the From LDAP directory pass you enter or construct an LDAP URL while in a To LDAP directory pass you specify only the host name and the port of the LDAP server.

Procedure

1. In the From LDAP directory pass, choose the ... button after the URL, and fill in the search parameters.



LDAP search parameters

Host name: 10.55.160.250

Port number: 636

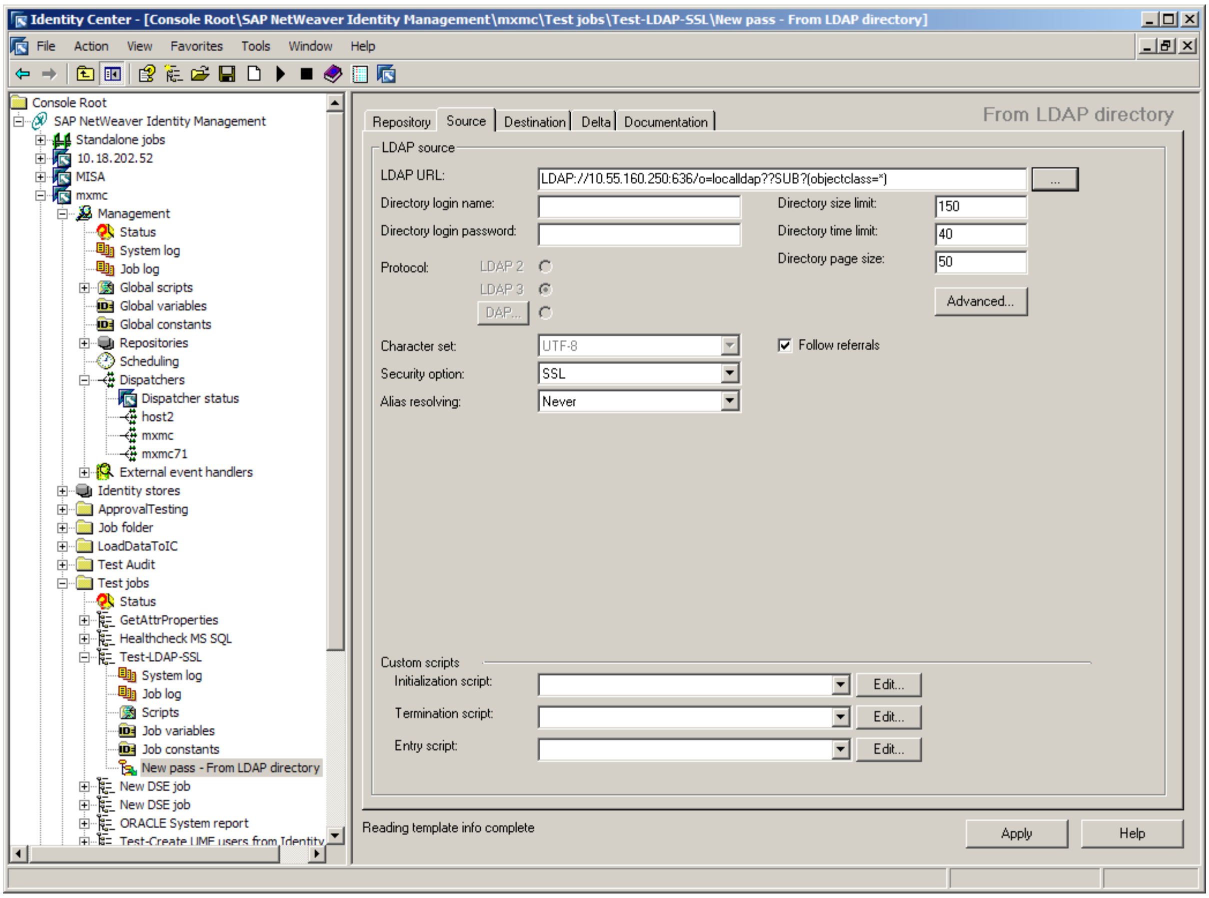
Starting point: o=localldap

Return attributes:

Search type: SUB

Filter: (objectclass=*)

Note that the default port number for SSL is 636 (and not 389).



LDAP URL: LDAP://10.55.160.250:636/o=localldap??SUB?(objectclass=*)

Directory login name:

Directory login password:

Directory size limit: 150

Directory time limit: 40

Directory page size: 50

Protocol: LDAP 2 ○ LDAP 3 ● ○

Character set: UTF-8

☑ Follow referrals

Security option: SSL

Alias resolving: Never

Initialization script:

Termination script:

Entry script:

Reading template info complete

2. Select *SSL* as the security option.
3. Directory login name and password must be supplied if required by the server.

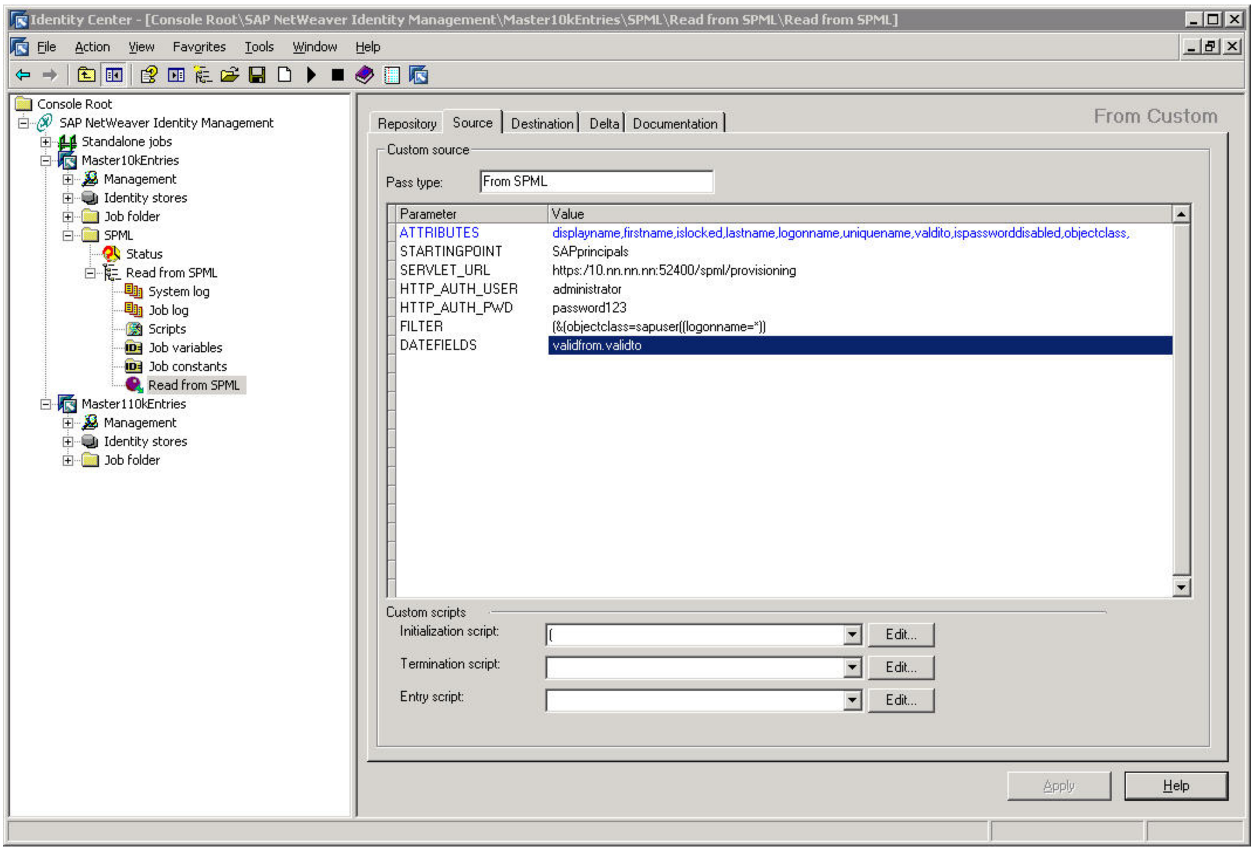
6.5.1.3 Connecting to an SPML Server over SSL

This section describes how you access an SPML server using SSL.

The connection is configured as a From Custom pass to read from an SPML server and a To Custom pass to write data to an SPML server.

> **Note**
>
> Make sure that the certificate used to authenticate against the web server is available in the keystore.

You define the connection to the SPML server on the *Source* or *Destination* tab of the To or From Custom pass.



Custom source

Pass type: From SPML

Parameter	Value
ATTRIBUTES	displayname,firstname,islocked,lastname,logonname,uniquename,valdito,ispassworddisabled,objectclass,
STARTINGPOINT	SAPprincipals
SERVLET_URL	https:/10.nn.nn.nn:52400/spml/provisioning
HTTP_AUTH_USER	administrator
HTTP_AUTH_PWD	password123
FILTER	(&(objectclass=sapuser)(logonname=*))
DATEFIELDS	validfrom.validto

Initialization script: (

Termination script:

Entry script:

When accessing an SPML server using SSL, use HTTPS as the protocol when specifying the URL in the SERVLET_URL parameter.

6.5.2 SSL Communication Using the Windows Runtime

When using the Windows Runtime Engine, only SSL security for LDAP communication is relevant.

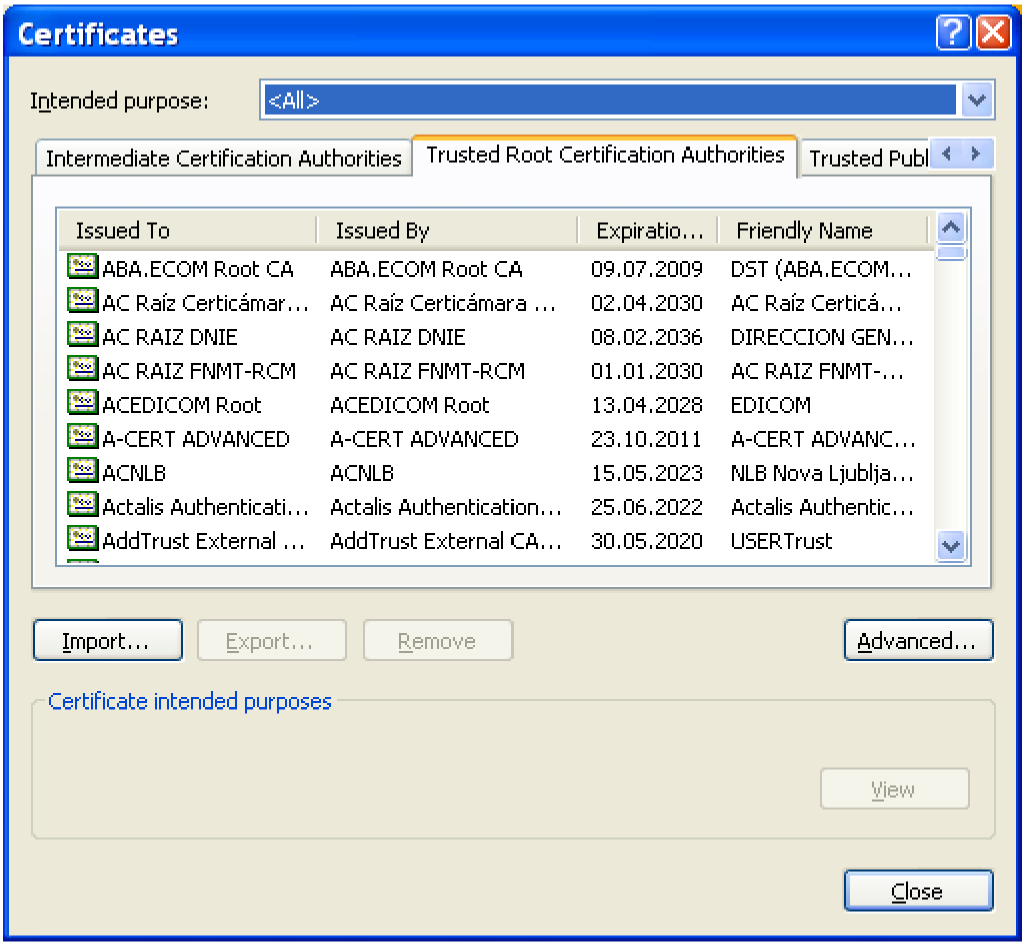
Context

To access a secure LDAP server, you need to trust the server's certificate. The Identity Center uses Microsoft's LDAP library and the certificate validation is done in this library.

The certificate that can be validated must be installed on the system. You can do this by using Microsoft Internet Explorer.

Procedure

1. Choose *Tools/Internet Options*.
2. Select the *Content* tab and choose *Certificates*.


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	09.07.2009	DST (ABA.ECOM...
AC Raíz Certicámar...	AC Raíz Certicámara ...	02.04.2030	AC Raíz Certicá...
AC RAIZ DNIE	AC RAIZ DNIE	08.02.2036	DIRECCION GEN...
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM	01.01.2030	AC RAIZ FNMT-...
ACEDICOM Root	ACEDICOM Root	13.04.2028	EDICOM
A-CERT ADVANCED	A-CERT ADVANCED	23.10.2011	A-CERT ADVANC...
ACNLB	ACNLB	15.05.2023	NLB Nova Ljublja...
Actalis Authenticati...	Actalis Authentication...	25.06.2022	Actalis Authentic...
AddTrust External ...	AddTrust External CA...	30.05.2020	USERTrust

3. Select the *Trusted Root Certification Authorities* tab. Choose *Import...* and follow the wizard to add the certificate.

   The LDAP passes are configured in the same way as described in *Connecting to an LDAP Server over SSL*. When configuring the To or From directory server pass, make sure that the server name is the same as specified in the certificate. The server name must be a fully qualified domain name, such as `ldapserver.domain.com`. It can not be a NetBIOS name or IP address.

6.6 Virtual Directory Server: SSL Security

The Virtual Directory Server can use SSL both when accessing its data sources and when accepting requests from the clients.

In the first case, the Virtual Directory Server acts as a client towards these data sources, and in the second case, it is a server.

As a client it can submit LDAP and SPML requests over SSL. As a server it can receive LDAP and SPML requests from the clients connecting to it. The configuration depends on whether the Virtual Directory Server should support SSL both as a server and as a client and which protocol is to be used.

Related Information

Configuring the Virtual Directory Server as a Server [page 27]
Configuring the Virtual Directory Server as a Client [page 28]

6.6.1 Configuring the Virtual Directory Server as a Server

The Virtual Directory Server can act as a server either for incoming LDAP or SPML requests.

Virtual Directory Server Deployed as an LDAP Server

The Virtual Directory Server supports SSL for incoming LDAP requests. See the document *SAP NetWeaver Identity Management Virtual Directory Server Using SSL for LDAP communication* for details about how to configure this.

Virtual Directory Server Deployed as a Web Service

When you deploy a Virtual Directory Server configuration as a web service, the clients connect to the SAP NetWeaver where this web service is deployed. The necessary certificates must be installed both on this web server and on the clients connecting to this web service. This does not affect the configuration of the Virtual Directory Server.

6.6.2 Configuring the Virtual Directory Server as a Client

The Virtual Directory Server can use SSL when accessing its back-end data sources, either with LDAP or SPML.

Virtual Directory Server as an LDAP Client

The Virtual Directory Server can access an LDAP data source using SSL. See the document *SAP NetWeaver Identity Management Virtual Directory Server Using SSL for LDAP communication* for details about how to configure this.

Virtual Directory Server as an SPML Client

When the Virtual Directory Server connects to a web service as a back-end data source, you specify HTTPS as the protocol. Additionally the Java keystore must contain a certificate that can be used to authenticate against the web service. See *Installing the Certificate* for information about how you maintain the keystore.

6.7 Securing AS ABAP Connections

Connections to AS ABAP systems use the Java Connector (JCo), which uses Remote Function Calls (RFC). These connections can be secured using Secure Network Communications (SNC).

For more information, see the following documents: *Secure Network Communications (SNC)* and *Provisioning Framework for SAP Systems: Connectivity* available on the SAP Community Network.

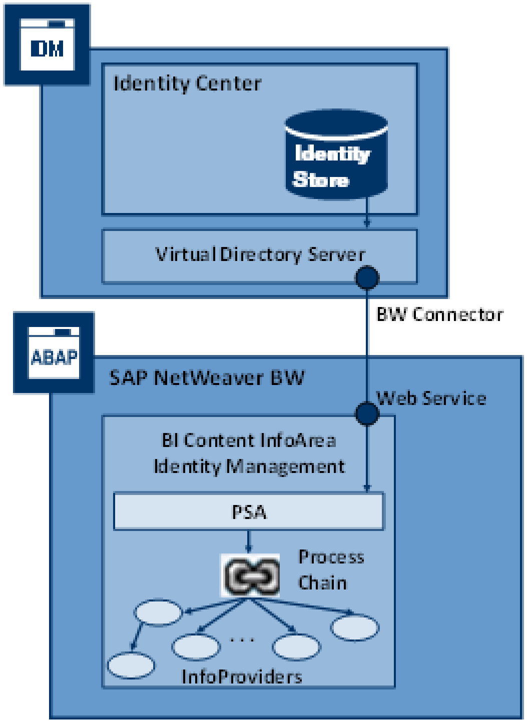
Related Information

Secure Network Communications (SNC)

http://scn.sap.com/community/security

6.8 Securing Connections for Reporting Using SAP NetWeaver BW

When using SAP NetWeaver BW for identity reporting, the Virtual Directory Server is used to send the identity data to the BW system using a Web service. See the figure below.



The connection between the Identity Center and the Virtual Directory Server can be secured with SSL for LDAP as previously mentioned. SSL can also be used to secure the Web service call to the BW system. For more information about how to configure SSL for these connections, see *Identity Reporting Using SAP NetWeaver Business Warehouse*.

6.9 Firewall Settings

Firewall must be open to allow database communication between the components and the database.

Firewall must be open to allow the Runtime Components and Virtual Directory Server to communication with external applications. Ports depend on communication protocol.

There are no specific requirements regarding firewall in the solution, but it is important to protect the systems from unauthorized access.

6.10 AS ABAP Connections

Connection to AS ABAP applications uses the RCF/JCo, and can be secured using Secure Network Communication (SNC).

6.11 AS Java Connections

Connections to AS Java applications, the HTTP protocol is used, and can be secured using SSL.

6.12 SAP HANA Connections

How to secure connections to SAP HANA is described in the *SAP HANA Security Guide*, section *Configuring SSL for ODBC/JDBC Client Access*.

Related Information

SAP HANA Security Guide

6.13 External Applications Credentials

Make sure to set up procedures for handling password changes of the accounts in the external applications being used by the Identity Center and the Virtual Directory Server, as this will also require changes in the configuration.

For the Identity Center, the passwords should always be stored encrypted in a repository definition.

For the Virtual Directory Server, the passwords are stored in the single source definitions.

7 Data Storage Security

This section provides an overview of any critical data that is used by the Identity Management and the security mechanisms that apply.

Related Information

7.1 Hashing and Encryption

Identity Management uses hashing and encryption to protect sensitive data.

Hashing

Hashing is used in the following cases:

- Authentication (from the Virtual Directory Server (MX_PASSWORD) and the password recovery (MX_AUTHQ_nnn))
- Internal authentication in the Virtual Directory Server
- Data hashed with the internal function uGenHash.
- Any attribute can be configured to use the defined hashing algorithm. (See *Defining the default hashing and encryption algorithms* for information about how to configure which hashing algorithm to use.) When an attribute is hashed, so are all historic values for the given attribute. However, changing the hashing algorithm on an existing attribute does not change any values in the identity store.

There are two hashing algorithms:

- MD5 (Message Digest 5)
- SSHA (Salted SHA1)

What is the default hashing algorithm is defined as part of the configuration of the Identity Center, as described below.

Encryption

The following information can be encrypted:

- Connection strings, used to connect to the Identity Center database or other repositories. These are always encrypted.
- Passwords, which are stored in configurations. These are always encrypted.
- Job constants and global constants can be encrypted if desired.
- Any attribute can be configured to use the defined encryption algorithm. (See *Defining the default hashing and encryption algorithms* for information about how to configure which encryption algorithm to use.) When an attribute is encrypted, so are all historic values for the given attribute. However, changing the encryption setting on an existing attribute does not change any values in the identity store.
- Any data encrypted with the internal function uEncrypt.

There are three options for encryption:

- Scrambling
- DES3/ECB
- DES3/CBC

What is the default encryption algorithm is defined as part of the configuration of the Identity Center, as described below.

i Note

The Java Cryptographic Extension Jurisdiction Policy files are a prerequisite for the SAP JVM must be downloaded separately as described in Note 1240081.

Related Information

Defining the Default Hashing and Encryption [page 33]

7.1.1 Defining the Default Hashing and Encryption

Context

The default algorithms are defined in the configuration of the Management Console of the Identity Center.

> Note
>
> Before changing the encryption or hashing algorithm, make sure that all components accessing the identity store supports the new algorithm. This is especially important if there are "standalone" Runtime Components or Virtual Directory Server configurations in the system landscape.

Procedure

1. In the Identity Center Management Console, choose *Tools/Options...* to open the *Options* dialog.
2. Select the default encryption algorithm:
   - *Scramble* - This is a built-in proprietary mechanism with a hardcoded password. This does not provide very high security.
   - *DES3/ECB* (Electronic Code Book) - Triple DES without initialization vector.
   - *DES3/CBC* (Cipher Block Changing) - Triple DES with initialization vector. This is the default value.
3. Select the default hashing mechanism:
   - *MD5* (Message Digest 5)
   - *SSHA* (Salted SHA1) - This is the default value.

7.2 Managing the Keys.ini File

Since the encrypted values must be accessible from many components, the encryption keys are stored in a file in the file system, called `Keys.ini`. This file must be accessible by the Identity Management User Interface, the Virtual Directory Server and all runtime engines in the system.

This file must be maintained centrally and distributed to all necessary locations.

> Note
>
> The Keys.ini file must be protected using file system protection, to ensure no unauthorized access. Anyone with access to this file may be able to decrypt all data in the identity store. The file must be accessible by the service user running the dispatcher and from the Identity Management User Interface.

7.2.1 Keys.ini File Format

The `Keys.ini` file consists of the following sections:

Table 7:

Section	Description
[ALGORITHMS]	This section specifies the defined hashing and encryption algorithms.
[KEYS]	This section contains up to 999 parameters which are the encryption keys. The name of the parameters is KEYnnn, where nnn is a key number. The key itself must be exactly 48 hex characters.
[CURRENT]	This section contains only one parameter called KEY. The value is the name of the key currently being used for encryption.

Below is a sample `Keys.ini` file.

```
[ALGORITHMS]
ENCRYPTION=DES3CBC
HASH=SSHA
[KEYS]
KEY001=78664478B8AA7899FF1009887837FFEDCCBAA77897DDA009
KEY002=7749487289BBCBD9A9E9F888D9E8F900A98F7D543A4566B6
[CURRENT]
KEY=KEY002
```

Possible values for ENCRYPTION are:

- *CRYPT* - The encryption algorithm is "Scramble".
- *DES3* - The encryption algorithm is DES3/ECB.
- *DES3CBC* - The encryption algorithm is DES3/CBC.

Possible values for HASH are:

- *SSHA* - The hashing algorithm is SSHA.
- *MD5* - The hashing algorithm is MD5.

7.2.2 Encrypted Data

The `Keys.ini` file can hold up to 999 keys. Only one of the keys is used for encryption. The other keys are old keys, which are kept in the `Keys.ini` file, to be able to decrypt older data.

When data is encrypted, the result is prefixed by an identifier for the encryption algorithm followed by the key number used when encryption. Then the encrypted data is stored as base64. Below is a sample of encrypted data:

```
{DES3}7:7d081564e69f342d81174fc8c6f19ce9
{DES3CBC}7:fd6e72e1371ac428-ffd210770dbdd65a0b7d728d05d3ae6f58b9bad51e550daf
```

The algorithm identifier is the same as in the `Keys.ini` file described above.

This data is encrypted using key number 7.

For DES3CBC the initialization vector precedes the encrypted data, separated by a hyphen.

7.2.3 Maintaining the Keys.ini File

It is important that all components encrypting and decrypting data use the same set of encryption keys. This section describes how to maintain the Keys.ini file in a multi-server environment. 8.2.3.1 Setting

Related Information

Setting Up the Initial Key [page 35]
Adding a New Key [page 36]
Maintaining the Keys.ini File in Separate Environments [page 37]

7.2.3.1 Setting Up the Initial Key

If the `Keys.ini` file does not exist when you start the Management Console, it will create the file containing a random key. The file is located in the following directory: `<installation directory>\KEY\Keys.ini`.

In a default installation, this will be: `C:\usr\SAP\IdM\Identity Center\KEY\Keys.ini`.

Below is a sample of the contents of the file:

```
[ALGORITHMS]
ENCRYPTION=DES3
HASH=SSHA
[KEYS]
KEY001=78664478B8AA7899FF1009887837FFEDCCBAA77897DDA009
[CURRENT]
KEY=KEY001
```

Then copy this file to all servers running the Identity Management User Interface, the Runtime Components, the Management Console and the Virtual Directory Server. Any encryption is now done using key number 1, and the encrypted data is prefixed with {DES3}:1.

Note

If desired, you may manually modify the randomly generated key before distribution of the file.

7.2.3.2 Adding a New Key

Context

After some time (dictated by the security policy of your organization), a new key should be added.

> **Note**
>
> Changing the key does not affect any data which is encrypted with that key. This is the reason that the old key must be kept to enable decryption of previously encrypted data.

You can add a new key in the Management Console.

Procedure

1. Select the SAP NetWeaver Identity Management node in the console tree and choose *Add encryption key*. This will append a key to the list of keys.

   ```
   [ALGORITHMS]
   ENCRYPTION=DES3
   HASH=SSHA
   [KEYS]
   KEY001=78664478B8AA7899FF1009887837FFEDCCBAA77897DDA009
   KEY002=7749487289BBCBD9A9E9F888D9E8F900A98F7D543A4566B6
   [CURRENT]
   KEY=KEY001
   ```

   The current key is still set to 1.
2. Distribute the file to all relevant locations, as described in *Setting Up the Initial Key*. Now all applications are able to decrypt data, which in the future will be encrypted with key number 2.
3. After the file is distributed, update the current key to key number 2. This must be done manually using a text editor. Distribute the file again.

   ```
   [ALGORITHMS]
   ENCRYPTION=DES3
   HASH=SSHA
   [KEYS]
   KEY001=78664478B8AA7899FF1009887837FFEDCCBAA77897DDA009
   KEY002=7749487289BBCBD9A9E9F888D9E8F900A98F7D543A4566B6
   [CURRENT]
   KEY=KEY002
   ```

Results

Any new encryptions are now performed using key number 2, while old data which are still encrypted using key number 1 can be decrypted.

The reason why this has to be done in two steps is that if you were to update the current encryption key before distribution the key file, you could run the risk that some data was encrypted with the new key, and attempted decrypted by a different process, before the `Keys.ini` file was in place. By doing this in two steps, you will always distribute the new encryption key to all locations, before you start using it.

Related Information

Setting Up the Initial Key [page 35]

7.2.3.3 Maintaining the Keys.ini File in Separate Environments

If you have several separate environments (development, QA and production), you must consider how you maintain and manage the `Keys.ini` file.

This is necessary both to ensure that data in the production system cannot be decrypted with keys from the development/QA system, but at the same time that the data in the development/QA system can be decrypted with keys from any system.

It is recommended to use a range of keys for the production system that is not available in the development/QA system, for instance all keys above 100 are reserved for the production system. Any new keys are added in the development/QA system must be added to the production system if it is required that the production system should be able do decrypt data from the development/QA system.

The Keys.ini file must be distributed in each of the environments as described here.

7.2.4 Identity Center Components

This section describes how the various Identity Management components handle the `Keys.ini` file.

Management Console

The Management Console from where the `Keys.ini` is maintained, will have access to the file as described in *Maintaining the Keys.ini File*. If the Management Console is installed on other servers in the system landscape, the `Keys.ini` must be distributed to that server and placed in the corresponding location.

Runtime Components

For the Runtime Components, the `Keys.ini` file is stored in the following directory: `<installation directory>\KEY\Keys.ini`

> **Note**
>
> A Unix system is case sensitive, and the casing is exactly as shown here. In a default installation on Microsoft Windows, this will be: `C:\usr\SAP\IdM\Identity Center\KEY\Keys.ini`.

Identity Management User Interface

For the Identity Management User Interface, the reference to the `Keys.ini` file is configured as part of the JMX parameters, as described in *Installing and Configuring the Identity Management User Interface*.

The location of this file depends on whether the Runtime Components are installed on the server or not. If it is installed on the server, the User Interface should use the same file as the Runtime Components located in the directory as described in the section above.

If the Runtime Components are not installed on the server, it can be located anywhere in the file system that can be referenced from the JMX properties. If there are several servers running SAP NetWeaver AS Java in the cluster, the file must be copied to the same location on all servers.

Related Information

Maintaining the Keys.ini File [page 35]

Installing and Configuring the Identity Management User Interface

7.2.5 Virtual Directory Server Components

This section describes how the Virtual Directory Server components handle the `Keys.ini` file.

Management Console

The Virtual Directory Management Console (configuration user interface) checks for `Keys.ini` in the following locations:

- The folder specified with the parameter KEYS_INI_FILE in the file `.vdssettings`.
- The folder specified with the environment variable VDS_HOME.

If no `Keys.ini` file is found, the Management Console will give a warning when it is started (even if encryption is not or will not be used). All encryption will be done using the built-in scrambling and all hashing will be done with MD5.

Decryption will fail, except for scrambled values.

Deployed Mode

A configuration is deployed on SAP NetWeaver AS Java retrieves the location of `Keys.ini` from the configuration in SAP NetWeaver AS Java.

Every deployed configuration has a corresponding `sap.application.global.properties` associated with it. Use Visual Administrator and locate the property `com.sap.idm.vds.keyfile` and enter the path to the `Keys.ini` file.

If no `Keys.ini` file is found, encryption will be done with scrambling and hashing with MD5.

Decryption will fail, except for scrambled values.

> Note
>
> This is a fatal error preventing the deployed configuration to start.

Standalone Mode

A configuration is run in standalone mode retrieves the location of `Keys.ini` file in the following locations:

- A file specified with the command line parameter KEYS_INI_FILE (Java option).
- The folder specified with the environment variable DSE_HOME.
- The folder specified with the environment variable VDS_HOME.

If no `Keys.ini` is found, encryption will be done with scrambling and hashing with MD5.

Decryption will fail, except for scrambled values.

> Note
>
> This is a fatal error preventing the deployed configuration to start.

7.3 Password Provisioning

By using password provisioning, you will ensure that the user has the same password in all applications.

The security policy of your organization may not allow this, or only allow this to a limited number of applications.

ℹ Note

The password policy of the different applications must be considered when doing password provision.

ℹ Note

Not all applications allow setting the productive password.

7.3.1 Storing the Password to be Distributed

The attribute MX_ENCRYPTED_PASSWORD contains user passwords used for password provisioning. This attribute must be encrypted using 3DES.

In addition, this attribute does not have password history enabled, and when implementing password provisioning, you should ensure that the MX_ENCRYPTED_PASSWORD attribute is kept when the password is provisioned to all applications.

- If a new system is added, the password must be provisioned also to this system.
- If a system requires the old password to set the new one.

ℹ Note

Storing the password in the identity store means that anyone with access to the identity store also has access to the password.

7.3.2 Obtaining the New Password

Before a new password can be provisioned, it must be stored in the MX_ENCRYPTED_PASSWORD attribute. This can be done in one of the following ways:

- By the Microsoft Active Directory Password hook
- By another job/task which receives the password from another application
- By any task that sets the MX_PASSWORD attribute

7.3.3 Distributing the New Password

A set password task must be created for each target application. This task will decrypt the password and update the target application with the new password.

Note

You must always handle the situation that the new password is rejected by the target application because it does not comply with the password policy.

7.4 Virtual Directory Server Keystores

The Virtual Directory Server uses keystores for holding private and public keys, which are used for various purposes.

To set up an SSL connection over LDAP, the Virtual Directory Server needs a private key, which is stored in a keystore. Information about the keystore, including the password to access the private key, is stored in the Virtual Directory Server configuration file.

The Virtual Directory Server configuration file must be encrypted to protect from unauthorized access to the keystore passwords.

7.5 Configuration Files

The configuration files used by the Identity Center will in most cases contain a connection string, which is used when the application connects to the Identity Center database.

7.6 Management Console

The configuration data for the configuration UI is stored in the file `<install dir>\EMSConfig.xml`. It contains an encrypted connection string. By default, the *allow password saving* is not set by the connection wizard, and if so the connection string will not contain a password, and should not pose a security risk.

If you choose allow password saving, the encrypted connection string will contain the password.

It is also possible to create a database user as described in *Identity Center Database Logins and Roles*, which is bound to a Microsoft Windows account, and use this for login. In this case, the connection string will not contain any sensitive information. Consult the database documentation for information about how this is done.

Related Information

Identity Center Database Logins and Roles [page 10]

7.7 Dispatcher

When creating a new dispatcher, the `.prop` file contains the connection string to the database. The key MC_JDBCURL holds the encrypted connection string.

7.8 Event Agent Server

When creating a new event agent server, the `.prop` file contains the connection string to the database. The key MC_JDBCURL holds the encrypted connection string.

7.9 Import/Export

When running export or import, a file called `import_start.bat` or `export_start.bat` containing the encrypted connection string to the database is created in the installation directory.

7.10 Identity Management User Interface/ Identity Management User Interface for HTML 5

The connection string is configured in SAP NetWeaver AS Java/the REST API, and is subject to the built-in security.

Related Information

Uploading Binary Data [page 42]

7.10.1 Uploading Binary Data

New binary data that is uploaded into the identity store can be scanned for viruses by using the Virus Scan Interface (VSI) of SAP NetWeaver AS Java.

Enabling the Virus Scan Interface also prevents other types of security attacks, such as cross-site scripting. For information about the different versions of SAP NetWeaver AS Java, see the Related Information section.

Additionally, a maximum size for uploaded files is enforced.

Related Information

Virus Scan Interface for SAP NetWeaver AS Java as of Release 7.0

Virus Scan Interface for EHP 1 for SAP NetWeaver CE 7.11

Virus Scan Interface for SAP NetWeaver CE 7.2

Virus Scan Interface for SAP NetWeaver 7.3

7.11 Virtual Directory Server Configuration File

The Virtual Directory Server uses an XML based configuration file for storing the configuration. All passwords used to connect to other applications are scrambled, using the standard encryption algorithm, as 3DES is not implemented in the Virtual Directory Server. It is therefore essential to protect the Virtual Directory Server configuration files.

The passwords used for authentication by the Virtual Directory Server (i.e. to authenticate incoming requests) are hashed using the default hashing algorithm.

Any global constants can be scrambled.

The Virtual Directory Server stores the configuration in an `.xml` file. One Virtual Directory Server installation may run multiple configurations, each stored in a different file.

As the configuration files contain information to connect to external applications, it is essential that the file system security is used to protect these configuration files from unauthorized access.

It is possible to store the Virtual Directory Server configuration in a database table. In this case, the connection string for connecting to the database is stored in tile file `<installation directory>\.vcssettings`. This connection string is scrambled, so it is essential to protect this file using file system security.

When starting a server, a local copy of the configuration file is created on the computer running the server. It is therefore recommended to scramble the connection strings also when storing the configuration in the database.

Related Information

Password Protection of the Configuration File [page 44]

7.11.1 Password Protection of the Configuration File

It is also recommended that you password protect the configuration file. This is done by selecting the *Advanced* tab of the *Server properties* dialog box. This is described in the help file of the Virtual Directory Server.

7.12 Avoiding By-Passing of the Authorization Checks in the Virtual Directory Server

When developing a configuration in the Virtual Directory Server, you can run the server in test mode which by-passes all authorization checks within the Virtual Directory Server. When running the Virtual Directory Server configuration in a production environment this should always be turned off.

For details, see the help file for the Virtual Directory Server.

8 Security Issues When Developing a Solution

This section contains information about specific security issues which should be considered when developing a solution.

SAP NetWeaver Identity Management offers a lot of very powerful functions, and security should always be considered during implementation. Note that this chapter does not offer a complete list of security issues. Always do a security review of the implementation before deploying it into a production environment.

Related Information

Using a Shell Execute Pass [page 45]
Using the uShell or uShellRead Functions in a Script [page 47]
Using To Database Pass with SQL Updating [page 47]

8.1 Using a Shell Execute Pass

The pass type Shell Execute offers functionality to execute operating system commands, where also attributes of the entry being processed can be included.

Consider the following example, which is used to create a file system directory for the user. The name of the directory is held in the attribute USERHOMEDIRECTORY. The destination of the Shell Execute pass can look something like this:

Sample Code

```
cmd /c md %USERHOMEDIRECTORY%
```

In a normal case, a new directory is created for the user.

However, if an attacker is able to update the %USERHOMEDIRECTORY% attribute, and for example, enters the following value:

Sample Code

```
dir1 && net user attacker /add /expires:never && net localgroup
administrators /add attacker
```

Given that the operating system user running the dispatcher has the proper authorizations, this malicious code would result in a directory called `dir1`. But in addition, it will create a new user called “attacker” and add this user to the administrator group.

To reduce the risk, any attributes used in a Shell Execute pass should be parsed for malicious code before execution. Creating a script for doing this is simple. Please see the help system of the Management Console.

Also, make sure that the user running the dispatcher does not have more access rights than required. The code executed by the Shell Execute pass will run with the access rights of this user.

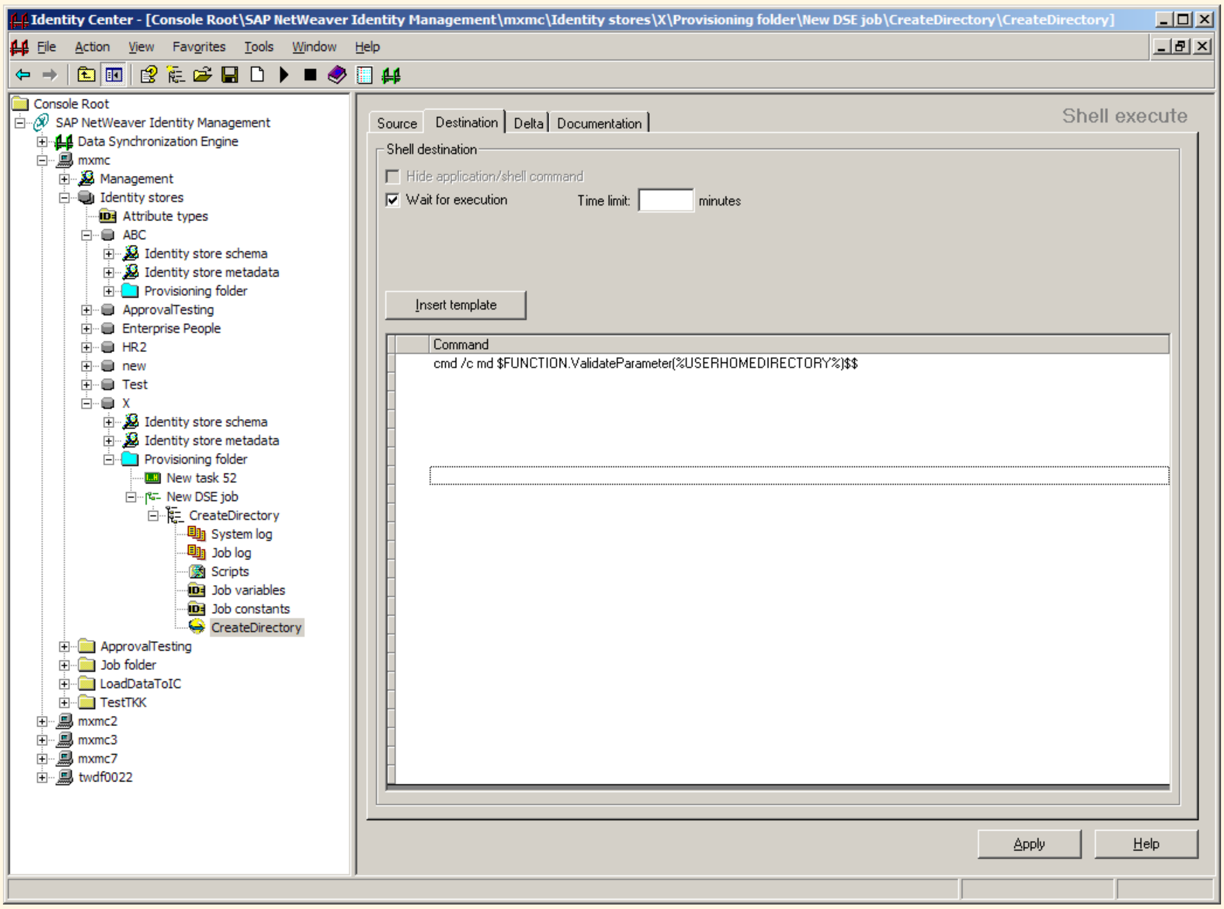
Example

This sample script will remove everything after two && characters.

Code Syntax

```
// Main function: ValidateParameter
function ValidateParameter(Par){
    ix = Par.indexOf("&&");
    if (ix > 0)
    {
        return Par.substring(0,ix);
    }
    return Par;
}
```

The function can then be called like this:



Shell destination

☐ Hide application/shell command

☑ Wait for execution   Time limit: ____ minutes

Command
cmd /c md $FUNCTION.ValidateParameter(%USERHOMEDIRECTORY%)$$

8.2 Using the uShell or uShellRead Functions in a Script

There are two built-in function (uShell and uShellRead) which executes an operating system command. This should be used with care, in the same way as the Shell Execute pass.

8.3 Using To Database Pass with SQL Updating

By selecting the *SQL updating* in the To Database pass, it is possible to enter any SQL statement. Consider the following example, which is used to add a row in a database table, based on data from the given user:

Code Syntax

```
INSERT INTO users (username,userid)
    VALUES ('%USERNAME%',%USERID%)
```

However, an attacker could add the following code in the USERID attribute:

Code Syntax

```
12); DELETE FROM TABLE users
```

This malicious code would remove all entries from the users table.

To reduce the risk, any attributes used in a To Database pass using SQL updating should be parsed for malicious code before execution. Creating a script for doing this is simple. Please see the help system of the Management Console for details on creating scripts.

Also, make sure that the user used to connect to the database does not have extensive access rights. The %IdentityCenter% connection string will log in to the identity center database using the credentials of the runtime user (MXMC_RT). For passes which performs SQL updating, it is advised to create a separate user, which has access only to the required tables.

9 Other Security-Relevant Information

This section contains other security-relevant information.

Related Information

Management Console [page 49]
Disaster Recovery [page 49]
Backup [page 49]
Password Hook [page 50]
Identity Provider for SAP NetWeaver AS Java [page 50]
Logon Help [page 51]
REST Interface Version 2 [page 51]
Identity Management User Interface for HTML 5 [page 52]

9.1 Management Console

The Identity Center Management Console is intended for implementation of a solution. It should not be made available in a production environment, unless there are very good reasons to use it. Logs and other information can be accessed in the Monitoring section of the Identity Management User Interface.

9.2 Disaster Recovery

For setting up a DR solution, please see the document *SAP NetWeaver Identity Management Identity Center Implementation Guide: Disaster recovery*.

9.3 Backup

All configuration information and data is stored in the Identity Center database. This database should be backed up according to the organization's backup policy. For details about backup and restore of an Identity Center database, see *SAP NetWeaver Identity Management Identity Center Operations Guide*.

9.4 Password Hook

The Password Hook is an optional component, which will catch password changes done in a Microsoft Windows Domain, and forward the new passwords to the Identity Center, for provisioning to other systems.

For single sign-on, see *Integration into Single Sign-On Environments*.

The Password Hook is implemented using the Microsoft Password Filter, as described in *Password Filters*.

For more information about the Password Hook, see the document *SAP NetWeaver Identity Management Password Hook Configuration Guide*.

The use of this component is optional. Although care is taken to make this as secure as possible, the use of this component may raise some security issues:

- It is strongly recommended to select *Encrypt password*. Not only for security reasons, but without this, a user would be able to run a program with administrator privileges with a carefully crafted password. This is because the `CreateProcess()` function starts your script in a valid shell. Microsoft Windows does not give the programmer any means of escaping those shell variables, hence a password that contains shell code can be executed as code. The encrypt option also prevents this.
- Passwords are stored using two-way encryption in the identity store, normally in the attribute MX_ENCRYPTED_PASSWORD. When deploying a solution, care must be taken to protect the Identity Center encryption file (described in section Error! Reference source not found.).
- If possible, the MX_ENCRYPTED_PASSWORD attribute should be deleted after the password has been provisioned to the target systems, to reduce the risk of exposure.
- For the same reason as above, attribute history should not be enabled on the MX_ENCRYPTED_PASSWORD attribute.
- Make sure access to the domain controller is limited and controlled.
- When deploying, one must consider the password policy of the various systems, to ensure that a password is accepted by all systems. This means that the user must only choose such passwords that are in the intersection set of all password policies. In general that will result in a fairly weak password policy.
- One should also consider if it is wise to have the same password across all systems. If the password is cracked in a low-security system, this password may also be used in a high-security system. Also note that the total number of possible password logon attempts increase with the number of systems with the same password (i.e. the sum of all "permissible failed password logon attempts" of all systems).

Related Information

Integration into Single Sign-On Environments [page 19]

Password Filters ➦

9.5 Identity Provider for SAP NetWeaver AS Java

For security relevant information for the SAP NetWeaver Identity Provider, see the following documents:

- *SAP NetWeaver Identity Management Identity Provider Implementation Guide*
- *SAP NetWeaver Identity Management Security Token Service Implementation Guide*

9.6 Logon Help

SAP NetWeaver Identity Management Logon Help is a client application for Microsoft Windows Workstations for users to reset their passwords.

Logon help does this in conjunction with the Password Reset Self-Service scenario of SAP NetWeaver Identity Management Identity Center and a Microsoft Windows domain controller. Business users set their security questions and answers as part of the self-service scenario. If the business users forget their password to log on to the Windows domain on their workstation, business users can use the front-end client, Logon Help, to enter answers to security questions and a new password. If the business users enter their data correctly, Logon Help logs the business users on to the Windows domain with the new password.

Logon Help sends passwords and answers to security questions to Identity Center. Logon Help communicates with the Identity Center by means of a REST service over HTTP with Secure Sockets Layer (SSL). Logon Help refuses to use connections that do not support HTTPS. You must configure a port on the SAP NetWeaver Application Server Java that hosts SAP NetWeaver ID Management Identity Center to support HTTPS, then configure Logon Help to use that port.

Identity Center synchronizes the password data with the Windows domain controller.

Related Information

Logon Help for SAP Identity Management Implementation Guide

9.7 REST Interface Version 2

SAP NetWeaver Identity Management REST interface version 2 is a service application programming interface (API) that supports the new user interfaces for SAP NetWeaver Identity Management 7.2 and other new custom-made user interfaces

The following security-relevant aspects exist:

- Authentication of Users and Assignment of Authorizations to Users
  The default configuration of the REST interface forces a logon on all requests using the provided basic authentication credentials. To improve performance, set up single signon.
  Existing users who already have access to the traditional SAP NetWeaver Identity Management user interface do not automatically have access to the REST interface version 2.
  In addition to the overall authorization to access SAP NetWeaver Identity Management, access to the REST interface is controlled by the security role, idm_authenticated_restapi, on SAP NetWeaver Application Server (SAP NetWeaver AS) Java.

- Network security
  Make sure the connection between the user interface and the REST server is secured using HTTPS.
- Cross-Site Request Forgery Protection (XSRF)
  To protect against attacks of this type, the REST interface uses a standard filter provided by SAP NetWeaver AS Java. The XSRF protection for the REST interface is based on an XSRF token that is retrieved with a non-modifying request and must be presented with all modifying requests.
- Access to Identity Store Data
  Access to identity store data is protected by the same mechanism as access for the traditional user interface, which means, using UI tasks. This affects who can log on and what data he or she can access.
- Access to Security-Relevant Attributes
  Security-relevant attributes like passwords and encrypted data are protected by additional means. You can require a secured connection to view specific attributes or to completely hide them from display.
- Access to Binary Attributes
  See section *Uploading Binary Data*.

For more information, see the section *Security* in *SAP NetWeaver Identity Management REST Interface Version 2*.

Related Information

Uploading Binary Data [page 42]

9.8 Identity Management User Interface for HTML 5

For network security, see *Identity Management User Interface for HTML 5: HTTP Security (SSL)*.

The Identity Management User Interface for HTML 5 accesses the Identity Center data using the REST Interface. See section *REST Interface Version 2*

Related Information

Identity Management User Interface for HTML 5: HTTP Security (SSL) [page 21]
REST Interface Version 2 [page 51]

10 Trace and Log Files

Authentication in the Identity Management User Interface is handled by UME, which also will log any security related events.

Internal Identity Management authentication is done using database security. The database will therefore log any security relevant events.

As for a deployment of Identity Management, security incidents may occur as a result of executing tasks or jobs. In this case, the corresponding log record (which can be viewed in the Monitoring tab in the User Interface or in the Management Console) will hold information about the event.

Finally, the system log (which can be viewed in the Monitoring tab in the User Interface, or in the Management Console) can include system related log information, as a result of tasks and jobs logging to this log.

ℹ Note

Setting log level to *Debug* on dispatcher or job may result in passwords being written to the log. It is not recommended to use *Debug* as log level in a production environment.

11 Appendix

Security Checklist for Identity Center

- Encryption algorithm set to 3DES (Verify in the configuration UI)
- Keys.ini file updated, and distributed to all relevant systems
- Keys.ini file protected by file system.
- Database security enabled where relevant.
- Separate database logins for each administrator External application security enabled where relevant.
- External application security enabled where relevant.
- If password provisioning is being used:
  - No history for MX_ENCRYPTED_PASSWORD
  - MX_ENCRYPTED_PASSWORD deleted after provisioning is done

Security Checklist for Virtual Directory Server

- Protect the Virtual Directory Server configuration file(s) from unauthorized access
- Verify that *Test mode* is turned off before the configuration is deployed in a production environment
- If applicable: Set up secure communication from clients to the Virtual Directory Server
- If applicable: Set up secure communication to repositories

Important Disclaimers and Legal Information

Coding Samples

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 to 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, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).

go.sap.com/registration/ contact.html