Directory Interface for User Management via LDAP BC-LDAP-USR 6.30 Test Catalog

Version 6.3

1 Overview

The BC-LDAP-USR 6.30 certification test consists of two separate parts:

- Test with SAP Web Application Server (WebAS) ABAP

  The test procedure is documented in Section 2, 3, 4, and 5. Section 8 contains an appendix for WebAS ABAP test.

- Test with SAP NetWeaver Portal User Management Engine (UME) 4.0

  The test procedure is documented in Section 6 and 7,

2 Test Plan BC-LDAP-USR 6.3: WebAS ABAP Part

This part of the document describes the steps of the directory interface certification for the user management of the SAP Web Application Server (WebAS).

Its target audience is the vendor that wants to certify a directory server and the SAP certification group in execution of the certification process.

2.1 Test Objective – WebAS ABAP Part

The SAP Web Application Server is able to perform a synchronization of its user master data with a directory server using the LDAP protocol. A mapping configuration allows the WebAS administrator to customize the object classes and attribute types that shall be used for the directory entries representing users of the WebAS.

The communication with the directory server does not use functionality outside of LDAP version 3, therefore each LDAP version 3 compliant directory server product can basically be used as synchronization partner.

2.2 Certified Functions – WebAS ABAP Part

The part of the certification covers:

- Correctness of a schema extension of the directory (provided by the vendor) to store SAP specific attributes
- Correctness of a mapping from WebAS user master data to attributes of the directory (provided by the vendor)
- Technical test of the LDAP functions used by the synchronization process
- Synchronization of user master data
- Delta management on the basis of timestamps in the directory

2.3 Test Environment – WebAS ABAP Part

2.3.1 Provided by SAP

SAP provides a SAP Web Application Server of the release for which the vendor want to certify its product.

The functionality to import and export mapping proposals from an XML file are part of the following support package levels:

- SAP WebAS 6.20: Support package 61
- SAP NetWeaver 2004: Support package 19
- SAP NetWeaver 2004s: Support package 11

An advance correction is available in SAP Note 983762.

As the result of a successful certification, a SAP Note will be created that declares that the directory server product is certified. The note contains a schema-extension file for the directory and an XML file with a proposal for a mapping from SAP fields to directory attributes (see below for the purpose of those files).

The LDAP Connector (part of the WebAS) must be separately patched to the highest patch level available at the time of certification. It can be found in the patch area of the SAP Service Marketplace at location of kernel patches.

On some hardware platforms, the LDAP client library is not part of the operating system and must be installed. These platforms are listed in a document specified in SAP Note 188371. Platforms known to have the LDAP client library included are Microsoft Windows and Linux[1].

The ABAP report for the technical tests needed in 5.2 can be found in SAP Note 699072 (SAP internal only) and must be implemented in the certification system. If the report is already present in the target system, check the version information contained in the comment block at the header. Update the report if the source given in the SAP Note is more current.

The version used during the certification must be noted down in the certification report.

2.3.2 Provided by the vendor

The vendor brings in the hardware and software needed to operate the directory, a schema-extension file and a mapping proposal from the SAP fields (see attachment) to the directory attributes.

The certification process does not require that SAP gets access to the directory software before or after the certification process.

3 Certification Preparation – WebAS ABAP Part

The certification process starts with offline communication between SAP and the vendor during which the vendor works out the schema extension and the mapping between SAP fields and the directory attributes.

3.1 Overview of Certification Steps – WebAS ABAP Part

The part of the certification consists of a couple of steps that are listed here to give an overview. The steps are described in detail later on:

- A vendor interested in the certification receives this test plan description.
- The vendor uses the given list of SAP fields to work out a mapping between the SAP fields and the attributes available in the directory.

  For those fields that cannot be mapped with the default schema, the vendor works out a schema extension text file.

  This file also describes how a customer can increase the potentially built-in size- and time limits for search operations that possibly exist in the directory. The file also describes how to put an index on an attribute, because efficient operation of the user master data synchronization requires an index on the attribute that stores the SAP-username.

[1] This information shall not establish a preference for certain operating systems. It is a guidance for the SAP certification group to set up the WebAS with the least possible effort.

- The vendor comes to the SAP certification location and takes a default installation of the directory product with them.
- SAP performs the schema extension using the schema-extension file provided by the vendor.
- SAP and vendor create the mapping proposal with the help of the data prepared by the vendor. Copying an already existing proposal as starting point is permitted and usually the best approach.
- SAP performs the technical tests and synchronization runs.
- Upon successful certification, a SAP Note is created that contains the schema-extension file and the mapping proposal data.in form of an XML file, exported from the certification execution system by SAP.

3.2 Demands on the Directory

In order to be used for user master data synchronization with the SAP Web Application Server, a directory must fulfill the following requirements. Compliance with these requirements is part of the certification:

- The directory must support access over the LDAP protocol of version 3 (LDAPv3) as described in RFC 2251. The user master synchronization only uses a subset of the available operations and only this subset is tested during this certification. SAP customers can access further LDAP functions using the LDAP API for Application Developers.
- Binding to the directory must be possible using username and password over an unprotected channel (that is: not using SSL).
- The directory must provide the attributes “createtimestamp” and “modifytimestamp” as described in RFC 2252. If during creation of an entry the “modifytimestamp” is additionally set (which not required according to the RFC), the time difference between “createtimestamp” and “modifytimestamp” must not be greater than the time spent during the create-operation.
- The directory must support entry modification with attribute addition, deletion and modification, where especially the attribute value replacement with an initial value set must be interpreted as attribute deletion.
- It must be possible to configure the directory with respect to the maximum number of entries returned from a search request and the maximum time that such a search request requires. The background of this requirement is that SAP does not utilize the LDAP paged search control on all supported application server platforms. A customer must be able to configure the directory so that all entries that represent a user of the WebAS can be read by a single search request. The number of such entries might well exceed 10 000 in an enterprise environment.
- The directory must support an extension of the schema using a text file.
- If the directory supports control type 1.2.840.113556.1.4.319 as described by RFC 2696 (“LDAP Control Extension for Simple Paged Results Manipulation”), the combination of all returned results pages must be equal to the result of a single search operation (if during the execution of the overall search process no changes were performed to the directory content). If the directory content is changed during the execution of a multi-page search, the guidelines of the RFC 2696 apply.

3.3 Definition of Attribute Mappings

The user master data synchronization of the SAP Web Application Server uses a fixed list of data that can be synchronized with the directory. These attributes must be mapped to attributes in the directory. The table in section 8.3 shows these fields.

In the mapping definition step, the vendor compares this table with the default attributes that the directory supports and defines the mapping to be used for his product. It is preferable if this mapping keeps up closely to the mapping proposal SAP makes in 8.3.

If fields are identified that cannot be mapped to a default directory attribute, a schema extension will be necessary for which SAP has defined attributes at hand.

The shown syntax and equality rule settings for the attributes are proposals of SAP in case the attribute must be newly created for the product. It is permitted that the finally used attribute type has other properties. The requirement is that the minimum length of characters that the attribute value can have is greater or equal to the specified length and the type of values that can be stored is a superset of the values that can be stored in the proposed attribute type.

3.4 Definition of required schema extension

For those fields of the SAP WebAS user master data that do not fit into the delivered schema of the directory the customer must make a schema extension. These attributes were identified in section 3.3 using the table in section 8.3.

Furthermore, the synchronization process will use the SAP defined object class `sapAddOnUM` that carries the SAP Web AS attributes and will identify an entry in the directory as relevant for synchronization. This object class is described in section 8.1.

The vendor provides the text file that the customer can use to perform the schema extension in his installation of the product to create the required attribute types and the object class. The file must be self-contained including documentation on the procedure for the import of the schema extension. Section 8.2 shows an example of such a file. The example is a file in LDIF format, but SAP does not make any restrictions on the content of this file. It could also be a descriptive text how to make the schema extension in a visual tool with mouse and keyboard.

If the directory product has a default time- or size-limit regarding the maximum returned entries during a search operation, the schema extension file must contain a description how to increase these numbers because the WebAS must be able to search all entries in a single search request.

3.5 Specification of Object Classes for Users

The vendor specifies which object classes will be assigned to an entry in the directory that represents an SAP WebAS user. The SAP object class will always be `sapAddOnUM`.

Examples for object classes used by already certified vendors and products are: `inetOrgPerson`, `organizationalPerson`, `person`, `user`.

3.6 Re-Certification Short Cut – WebAS ABAP Part

If a vendor wants to certify a new version of a product that is already certified, and the new version is compatible with the old version regarding schema content and schema extension mechanism, for this part – WebAS ABAP – of the certification, the vendor can decide that the metadata present in the WebAS for the old version are re-used for the new version.

The confirmation that these data are suitable for the new version of the directory product is nevertheless produced during the certification process.

4 Test Preparation – WebAS ABAP Part

4.1 Connecting Systems

The hardware provided by the vendor and hosting the directory server is connected to the network that can be reached from the SAP Web Application Server.

4.2 Configuration of the LDAP Connection

4.2.1 Configure LDAP Connector

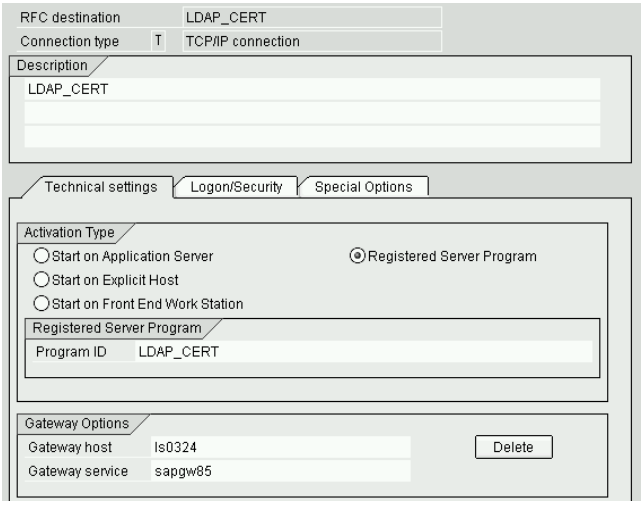
Start transaction LDAP. If content appears in the input field “Connector” you already have a configured LDAP Connector and may proceed with the next step.

Otherwise it is assumed that the LDAP Client library of the operating system is already installed (see 2.3.1).

In transaction SM59, create an RFC Destination with the following parameters:

- **Name:** LDAP_CERT
- **Type:** T
- **Description:** LDAP_CERT
- **Activation Type:** Registered Server Program
- **Program ID:** LDAP_CERT
- **Gateway host:** Enter the hostname of the SAP WebAS
- **Gateway service:** Enter sapgw<xx> where <xx> is the instance number of the SAP Web Application Server

Example for application server host ls0324 with instance number 85:

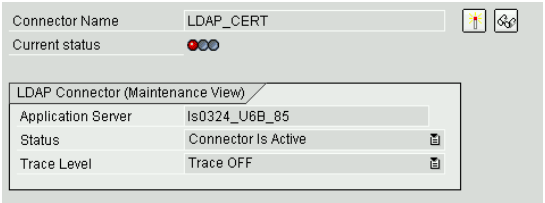


In transaction LDAP, press button “Connector”, go to change mode, press “New Entries”.

Enter the following data

- **Connector Name:** The RFC Destination created above
- **Application Server:** Use F4 help to select the application server whose name you entered in the “Gateway host” field in the RFC Destination
- **Status:** Connector Is Active
- **Trace Level:** Trace OFF

Save the data. A red traffic light indicates that the LDAP Connector is not started yet.



It would be started automatically by CCMS after a maximum time of 10 minutes, but it can also be started manually by pressing the “Start Connector” button. The traffic light will turn green. If it turns

yellow, you have to wait several seconds and then press enter to show the new status. It should be green now.

The configuration of the LDAP Connector is described in detail in the SAP Library.

4.2.2 Disable paged search support (Release 7.00 or higher)

The LDAP Connector that is delivered with the NetWeaver Application Server ABAP as of release 7.00 or higher automatically uses paged search support by default. This would obliterate the test that checks whether the directory supports search requests for large numbers of objects.

Therefore, you must disable the paged search support before this test.

On the application server of the LDAP Connector, go to the "work" directory of the ABAP instance and create a file named "ldap_rfc.cfg" with the following content:

```
pagesize = 0
```

and restart the LDAP Connector. Check in transaction ST11 that the startup message of the LDAP Connector in tracefile "dev_<connector name>.trc" contains the following line:

```
Page size (0 = no paging)  : 0 (configuration file)
```

4.2.3 Create System User

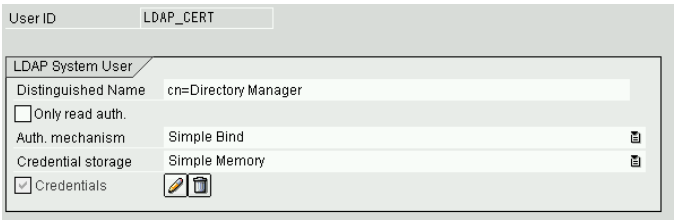
In order to log on to the directory in the background, the SAP WebAS must store the access data.

In transaction LDAP, press button "System Users", go to change mode, press "New Entries".

Create an entry with the following data:

- **User ID:** LDAP_CERT
- **Distinguished Name:** The DN of the user to access the directory.
- **Only read auth.**: Do NOT set this checkbox.
- **Auth. mechanism:** Only "Simple Bind" is supported.
- **Credential storage:** "Secure Storage". If you encounter problems using the secure storage and the option is available, use "Simple Memory".
- Press button "Change" and enter twice the password for access to the directory.
- Save the data

Example data:



4.2.4 Configure LDAP Server

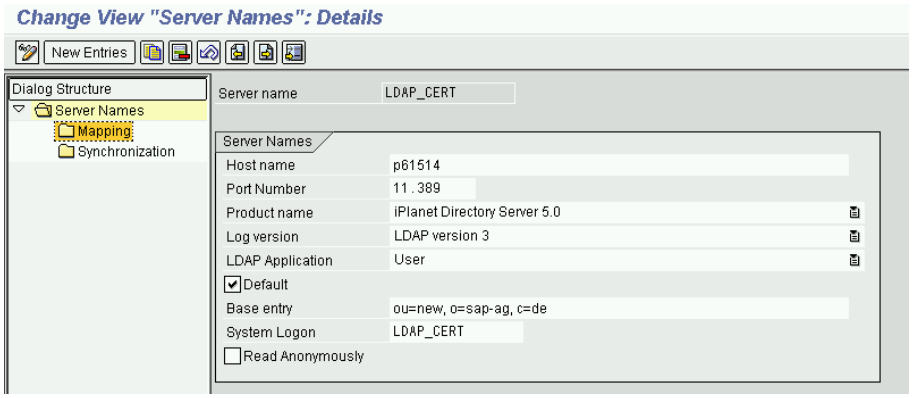
In transaction LDAP, press button "Server Names", go to change mode and "New Entries".

Enter the following data:

- **Server name:** LDAP_CERT
- **Host name:** The hostname of the directory server.
- **Port Number:** The port to be used.
- **Product name:** Select the entry "Other certified product". In fact, the content of this field is irrelevant for the runtime behavior of the SAP system.

- **Log version:** The field label is a translation error and means “Protocol version”. Choose “LDAP version 3”.
- **LDAP Application:** Choose “User”.
- **Default:** Set checkbox.
- **Base entry:** Enter the DN of the root entry for all following operations (directly underneath this entry the SAP Web Application Server will create the users, and anywhere underneath this entry users for synchronization will be searched).
- **System Logon:** Enter LDAP_CERT (this entry points to the data entered in 4.2.2).
- **Read Anonymously:** Do NOT set this checkbox.

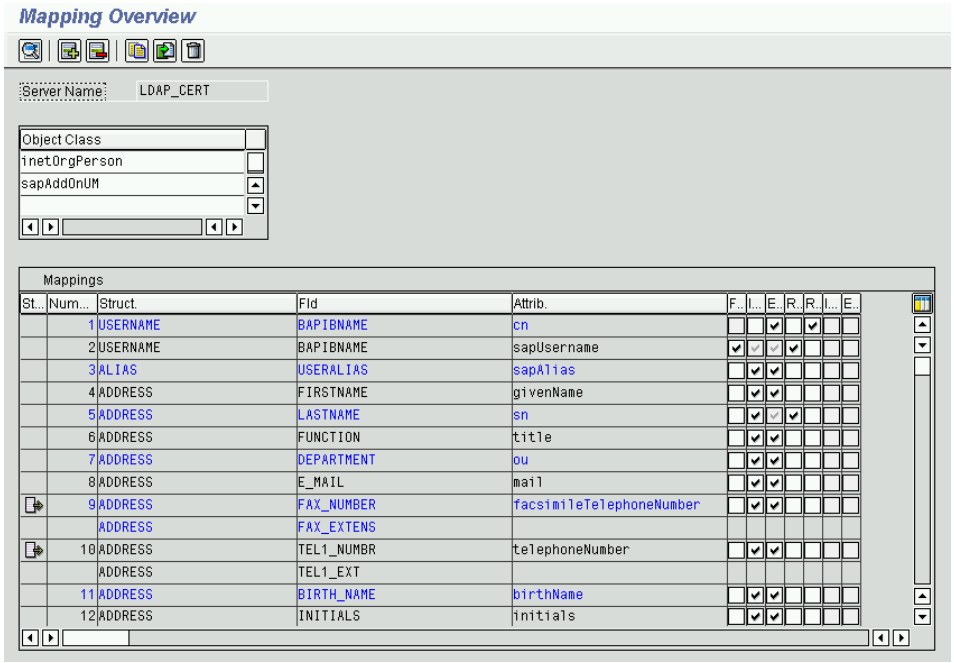
Then double click onto “Mapping” in the left tree:



Create the mapping using the data prepared by the vendor.

You may copy an already existing mapping by the menu function, or you may use the XML import function to import a proposal from the SAP Note of a previous certification process for an older version of the directory product.

The screen now shows the mapping from SAP fields to directory attributes.



In the example above, SAP users in the directory will be identified by the object classes `inetOrgPerson` and `sapAddOnUM` (this list was declared by the vendor in 3.5).

As an example for a field mapping, ADDRESS-LASTNAME is mapped to attribute “sn”.

Hint: To get field descriptions for the SAP fields in columns “Struct.” and “Fld” online, double click one of the lines and use F4 on the column “Field Name” in the next screen “Mapping Details”. Exit this screen with function “Cancel”, otherwise you will end up with a corrupt mapping that cannot be saved.

As in SAP Web Application Server 6.10 and 6.20 there is no field help on the checkboxes, here are some short explanations:

In the “Mapping” section of the LDAP Server configuration, the data mapping rules are defined. The meaning of the checkboxes is:

- **Filter:** This attribute is used to *find* a SAP user in the directory. Entries are found anywhere underneath the “Base Entry”.
- **Import Mapping:** This mapping can be used for data synchronized inwards.
- **Export Mapping:** This mapping can be used for data synchronized outwards.
- **Required:** This attribute is required to create an entry in the directory. It will always be written, even if the “Synchronization” settings (see below) do not specify so.
- **RDN Mapping:** This attribute defines the RDN used when the WebAS creates an entry in the directory. The new entry is created directly underneath the “Base Entry” configured above.

In the “Synchronization” section of the LDAP Server configuration, the same screen is shown, but this time the only fields open for input are the synchronization setting checkboxes which control the behavior of the synchronization report RSLDAPSYNC_USER:

- **Import:** This attribute will be imported to the WebAS with the next synchronization run.
- **Export:** This attribute will be exported from the WebAS with the next synchronization run.

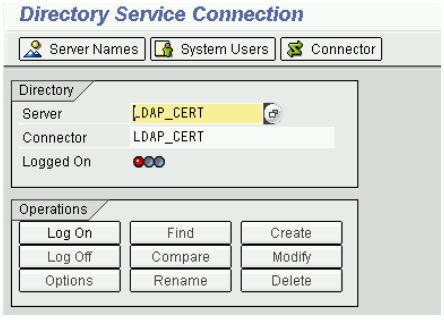
Please note the difference between “Mapping” and “Synchronization” settings. “Mapping” defines only the data conversion and data layout, but “Synchronization” controls the operative behavior.

From the “Mapping Overview” go back with “Back” and save the data.

4.2.5 Test Connection

In transaction LDAP, select “Server” LDAP_CERT.

The LDAP Connector should already be filled (LDAP_CERT if you created it according to 4.2.1).



Press button “Log On”, set checkbox “Use System User” and press “Execute”. You should now receive a success message and a green traffic light.

Press “Find” and confirm that the “Base entry” is the correct value (you entered it in 4.2.4). Keep the other default values and “Execute”. The search result will contain all entries at and below the base entry.

Go back to the entry screen of transaction LDAP and “Log Off”.

5 Test Execution BC-LDAP-USR 6.30: Web AS ABAP

5.1 Schema Extension Import

Follow the instructions printed in the header of the schema-extension file provided by the vendor to make the schema extension on the directory server. Be aware that these instructions must enable a customer without vendor consultant on site to perform the schema extension.

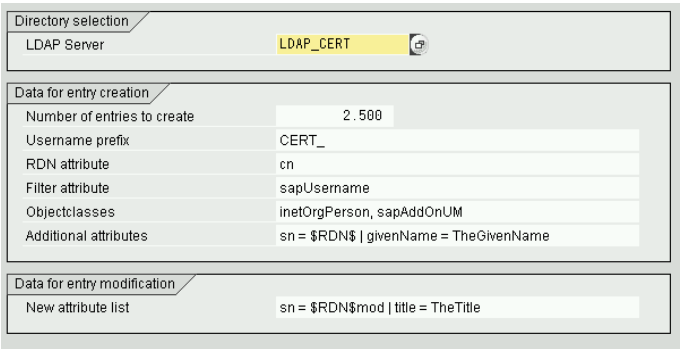
5.2 Technical Tests

To perform the technical tests, the test report from SAP Note 699072 must be implemented. The note is the only source of the current version of this report.

This report performs the following tests:

- Bind to the directory using the data configured in 4.2.
- Create of a number of user entries in the directory using configurable object classes, RDN, filter attribute and attribute list.
- Search for the created users with filter attribute and CREATETIMESTAMP and MODIFYTIMESTAMP.
- Modification of a single entry with attribute addition, deletion and modification.
- Check that timestamp changed during modification.

Start the report ZKLDAPCERT. On the entry screen, some data are already pre-filled:



In field “LDAP Server” the symbolic name of a configured LDAP Server must be entered. The default server for LDAP Application “User” is defaulted.

The “Number of entries to create” is filled with 2500. This test might take a longer time (a couple of minutes) due to this number, but 2500 is required for the certification. This especially tests the ability to perform searches for larger numbers of entries without the need for paging (which is not supported by the WebAS).

The following fields must possibly be adjusted to the directory schema in order for the test to run. The default values are to be considered as proposals.

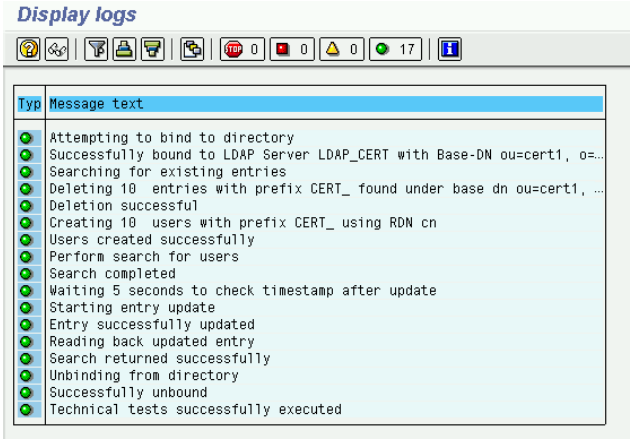
> The “Username prefix” together with an up-counting number forms the RDN of the new entries that are created which is stored in attribute “RDN attribute”.
>
> The “Filter attribute” is used by the WebAS to distinguish SAP user-master data from other data in the directory. The value `sapUsername` is the default filter attribute provided by object class `sapAddOnUM`.
>
> The “Objectclasses” are a comma separated list of object classes that the new entries are assigned to.

In “Additional attributes” further attributes for entry creation are specified. The default value fills the attribute “sn” with the value of the RDN (RDN is replaced by the current RDN value) and the attribute “givenName” with the fixed value “TheGivenName”. If the directory requires further attributes for entry creation, they must be added here.

For the entry modification test, the “New attribute list” contains, in the same syntax as “Additional attributes”, the attributes that are the new status of the entry. To test the full scope of possible operations, this list must have one attribute that is also part of “Additional attributes”, one new attribute and one attribute of “Additional attributes” must be missing (to simulate attribute deletion).

In the example, “sn” is modified, “title” is added and “givenName” is deleted.

During execution of the report, the status line indicates the progress. Finally, a log of the result is printed. The actual log result might differ in number an text of the messages.



The test is passed if no errors appear. If errors or warnings appear that cannot be fixed by reading the message text, please contact the development group.

A dump of the final log (obtain with System → List → Save → Local file) must be included into the certification report.

5.3 Synchronization Tests

In this step, report RSLDAPSYNC_USER will be used to synchronize user data between directory and WebAS user master.

Before starting, make sure that the base DN of the LDAP Server does not contain any entries that are interpreted by the synchronization tool as SAP users (entries having the object classes configured in LDAPMAP for the LDAP Server and the filter attribute).

These tests require that you are able to look at the directory data and change them outside of RSLDAPSYNC_USER. If the directory does not include tooling for directory browsing and changing, the generic LDAP functionality of transaction LDAP in the WebAS can be used.

5.3.1 Configuration of the Synchronization Settings

In transaction LDAPMAP, configure the *synchronization settings* for the certification server (example: LDAP_CERT) as described:

- “Export” indicator for: ADDRESS-FIRSTNAME, ADDRESS-LASTNAME, ADDRESS-FUNCTION, ADDRESS-DEPARTMENT and ACTIVITYGROUPS-SUBSYSTEM/AGR_NAME.
- “Import” indicator for: ADDRESS-E_MAIL.

5.3.2 Export of WebAS Users to the Directory

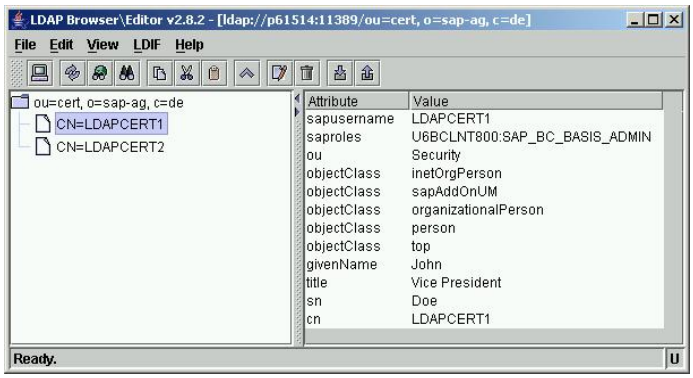
Create two users in the WebAS. Enter data into the following fields:

- Last name: free choice
- First name: free choice
- Function: free choice
- Department: free choice
- Roles: SAP_BC_BASIS_ADMIN

Start RSLDAPSYNC_USER with the following settings:

- **Server Name:** Name of certification server (example: LDAP_CERT).
- **User:** Restrict the run to the two users created above.
- **Objects that Only Exist in the Database:** Create in Directory, all others “Ignore Objects”.

Result: No errors in the synchronization log and the two users are visible in the directory with the corresponding attributes filled.



Note: This screen shot (and the following with similar appearance) was created using the external tool “LDAP Browser/Editor”. Its appearance in this document demonstrates that the new entries can be seen also with external tools.

It is not part of the certification that an external tool is used to verify that the entries in the directory were created. A tool provided by the directory vendor (possibly integrated into the directory management interface) or the generic transaction LDAP of the WebAS serve the same purpose.

5.3.3 Import Data from Directory

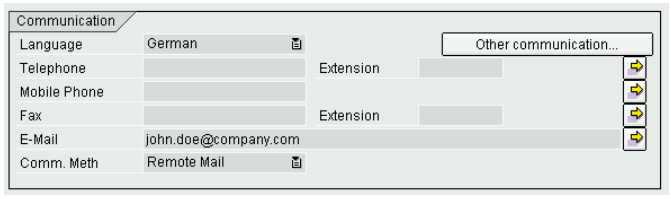
Add the attribute “mail” (or whatever is mapped to ADDRESS-E_MAIL) with a value in the directory:

Run RSLDAPSYNC_USER with “Ignore Objects” for all but “Objects that Exist Both in the Directory and in the Database” set to “Compare Time Stamp”.

Result: The log should show

```
Object ... successfully updated between database and directory
```

and in SU01 the mail address is visible:



5.3.4 Timestamp Management

Restart RSLDAPSYNC_USER for the same users and settings.

Result: The log should contain the statement

```
Object ... does not need to be updated
```

indicating that there was no update necessary.

Now change the entry in the directory by modifying any attribute except `objectclass`, `sapUsername` and `cn`, e.g. firstName.

Restart RSLDAPSYNC_USER for the same settings.

Result: The entry is synchronized again and the changes are updated (if you changed the mail address, this change was propagated to the WebAS, if you changed one of the other attributes (first name, last name, title, department) it was overwritten with the WebAS settings (because these attributes are synchronized outbound from the WebAS).

5.3.5 Search Moved Entries (Optional)

This step is optional because SAP does not require that the directory supports the move operation[2].

Underneath the base DN of the LDAP Server, create a child entry (e.g. an organizationalUnit) and move one of the directory entries to the new subtree.

The other entry is renamed to have another RDN, but remains at its position

Run RSLDAPSYNC_USER with the setting “Objects that Exist Both in the Directory and in the Database” set to “Ignore Time Stamp”. This forces the system to perform synchronization even if nothing was changed.

Result: The log should indicate that both entries were synchronized.

5.3.6 Deletion of Entries in the Directory

Delete the users in the WebAS and run RSLDAPSYNC_USER with the setting “Objects that Only Exist in the Directory” set to “Delete from Directory”.

Result: The entries are deleted from the directory.

5.4 Export Mapping Proposal

Export the mapping that was used during the certification from transaction LDAPMAP using the menu function “XML Export”.

5.5 Certification Result – WebAS ABAP Part

The result of this part of the certification process is the test protocol which must contain the following information:

- Schema extension (if necessary) done using the schema extension file provided by the vendor
- Schema extension file explains how the size-limit and time-limit of the directory server can be increased, if such limits exist.
- Mapping proposal file.
- Technical tests executed successfully and printout of the log of ZKLDAPCERT.
- Synchronization tests executed successfully with the expected results.

[2] Nevertheless the move operation is part of LDAPv3 and therefore should be supported by the directory.

5.6 Organizational Data

Customers experiencing problems with the directory during user master synchronization often arrive at SAP Support channels. For these channels it is helpful to be able to guide the customer to the documentation and support channels of the certified product.

As part of the certification process, the vendor gives SAP the following information (SAP is aware that these data only reflect a temporary state at the time of certification and might change):

- Information about support channels for customers
- Mail contact for SAP in case of difficult problems that require collaborative investigation
- Optional: Link to directory server documentation in the Internet (especially schema reference)

6 Test Plan BC-LDAP-USR 6.30: UME 4.0 Part

Consistent user management requires the integration of the numerous data repositories scattered through the enterprise. SAP User Management Engine (UME) enables you to leverage your existing system infrastructure by accessing user-related data on an existing corporate directory, a database, or an SAP system.

With UME you can connect to an LDAP directory server using an LDAP persistence adapter. You can even read data from and write data to multiple different physical LDAP directory servers, or different branches of the same LDAP directory server.

Entries in an LDAP directory server are organized in a tree-like structure called the Directory Information Tree (DIT). UME supports certain methods of arranging users and groups in a DIT in the LDAP directory server, which are:

- Groups as tree (deep hierarchy)
- Flat hierarchy

You can configure secure connections using the Secure Sockets Layer (SSL) protocol between UME and an LDAP directory server. When SSL is used, the data transferred between the two parties (client and server) is encrypted.

UME also supports data partitioning. This means that you can use different data sources for different user sets or attribute sets. You can partition data in two ways:

- *User-based data partitioning:* Different sets of users are written to different data sources. For example, in a collaboration scenario, where both users internal to your company and users from other companies work together in the same application, the external users need a user account as well. In this case you can configure the persistence manager to store company internal users in the corporate directory, whereas external users are stored in a separate directory.
- *Attribute-based data partitioning:* Different sets of attributes are written to different data sources. For example, global user attributes, such as telephone number, email address, and so on, are written to a corporate directory while SAP-specific data is written to a database.

To guarantee interoperability with the SAP software, the external directory product has to be certified for the BC-LDAP-USR 6.30 interface. This document describes the test environment and the tests performed during certification.

6.1 Test Objective – UME Part

This part of the BC-LDAP-USR 6.30 certification covers the usage of an LDAP directory server as user persistence store by UME. In addition, it covers the directory server configuration together with UME. This configuration includes object classes mapping and attribute mapping. Through attribute mapping the logical attribute names as used by the UME Java API are mapped to the physical attribute names in the directory server.

6.2 Test Environment – UME Part

The BC-LDAP-USR 6.30 certification requires the following preinstalled and pre-configured hardware and software.

Provided by SAP:

A server running UME 4.0 and EP 6.0.

Provided by the partner:

An LDAPv3 compliant directory server, the schema description in detail, as well as the attribute mapping between the directory schema and the UME API.

6.3 Certified Functions – UME Part

- Connecting to the LDAP directory server by UME LDAP adapter
- Object classes mapping
- Attribute mapping
- Reading data from the LDAP directory server by UME LDAP adapter
- Writing data to the LDAP directory server by UME LDAP adapter

6.4 Test Scenario Overview – UME Part

The interoperability between UME and the LDAPv3 compatible directory are tested using the following steps and scenarios.

6.4.1 Preparation Work

6.4.1.1 Prepared by SAP

- Install UME 4.0 and EP 6.0

6.4.1.2 Prepared by LDAP Directory Vendor

- Install LDAP directory server
- Generate vendor-specific schema for LDAP directory server
- Configure LDAP directory server to support SSL
- Configure attribute mapping

6.4.1.3 Done by SAP on Day of Certification

- Configure UME for using LDAP directory server as persistence store
- Fill LDAP directory server with user and group data

6.4.2 Configuration Scenarios

- Organization of users and groups in directory server with flat hierarchy
- SSL communication between UME and directory server

6.4.3 Test Scenarios (For Each Configuration Scenario)

- Search existing user in directory server
- Search existing group in directory server
- Search existing user account in directory server
- Create new user
- Modify existing user
- Delete existing user
- Create n new users
- Create new group

- Modify existing group
- Delete existing group
- Create n new groups
- Create new user account
- User authentication through userID and password verification against LDAP directory server
- Change password
- Try to log on with old and new password
- Delete user account
- Read all important data for a user from directory
- User authentication through client certificate (mapping)

7 Test Procedure BC-LDAP-USR 6.30: UME 4.0

This chapter describes details of the test procedure, the required steps and actions and the expected results.

7.1 Preparation Work – UME Part

7.1.1 Prepared by SAP

7.1.1.1 Install UME and EP 6.0

For detailed information about installation of UME 4.0 and EP 6.0 please visit SAP Service Marketplace at *http://service.sap.com/ep60*. There, you will find documentation for installation, upgrades, patches and hotfixes.

7.1.2 Prepared by LDAP Directory Vendor

7.1.2.1 Install LDAP Directory Server

For detailed information about installation of the LDAP directory server, please refer to the vendor-specific documentation.

7.1.2.2 Generate Vendor-Specific Schema for LDAP Directory Server

For detailed information about how to generate the schema for the LDAP directory server, please refer to the vendor-specific documentation.

7.1.2.3 Configure LDAP Directory Server to Support SSL

Generate a certificate for the directory server (either self-signed or issued by a CA) and configure the LDAP directory server to support SSL.

See also section 7.2.2.

Note: If technically required, the server certificate might have to be created on the day of certification.

7.1.2.4 Configure Attribute Mapping

For detailed information about how to configure attribute mapping, please refer to the *SAP Enterprise Portal 6.0 Administration Guide → Portal Platform → System Administration → User Management Configuration → Configuration of Data Sources Used for User Management → Defining Which Combination of Data Sources to Use → Mapping Attributes*.

7.1.3 Done by SAP on Day of Certification

7.1.3.1 Configure UME for Using LDAP Directory Server as Persistence Store

Use the user management configuration tool to provide the details required to connect to an LDAP directory. For detailed information please refer to the *SAP Enterprise Portal 6.0 Administration Guide → Portal Platform → System Administration → User Management Configuration*.

UME provides a set of pre-configured XML files that contain configuration settings for a set of standard scenarios regarding data sources. This configuration step also comprises object class mapping.

Use the pre-configured XML file for using an LDAP directory server as user persistence store. Use the pre-configured XML file where existing users and group data is read from an existing LDAP directory server and newly created users are written to the same LDAP directory server.

Then modify the settings in the XML file to suit the vendor-specific configuration and requirements.

7.1.3.2 Fill LDAP Directory Server With User and Group Data

Fill the LDAP directory server with user and group data. SAP provides a test framework based on iViews for this task. (Alternatively, an LDIF file for importing user and group data into the test environment could be used.)

Note: Groups can only be created by the iView test framework in a flat hierarchy.

7.2 Configuration Scenarios – UME Part

Configure UME and the LDAP directory server with the following options.

7.2.1 Organization of Users and Groups in Directory Server With Flat Hierarchy

In a flat hierarchy, the DIT has separate branches for user and group data. There are two possibilities:

- either each group has an attribute that lists the members of that group, for example by providing the user IDs of the members, or
- each user in the people branch has an attribute listing the groups that that user is a member of.

Organize the user and group data in the LDAP directory server with a flat hierarchy as described above.

7.2.2 SSL Communication Between UME and Directory Server

Configure secure connections using the SSL protocol between UME and the directory server.

Only SSL server authentication is used. This means that the server (i.e. the directory server) provides its identity to the client (i.e. UME) using a digital certificate, but the client does not provide its identity to the server. Once the SSL connection is set up, UME binds to the directory server with the LDAP protocol using user ID and password.

The following steps are required to configure SSL communication between UME and directory server:

- Generate a certificate for the directory server (either self-signed or issued by a CA). The certificate should be in DER format.
- Configure the directory server to support SSL.
- Configure the SAP J2EE Engine for SSL to the directory server.
- Configure UME to use SSL.

For more detailed information on setting up a secure SSL connection between UME and the LDAP directory server, see the section on *Secure Communications* in the *SAP Enterprise Portal 6.0 Security Guide.*

7.3 Test Scenarios – UME Part

Use the configuration as defined in the scenarios in section 7.2 with the following functions.

For performing these tasks, SAP provides an automated test framework based on iViews using the UME API. The test results are reported in a log file.

7.3.1 Search Existing User in Directory Server

Use the provided test framework to search for an existing user in the LDAP directory server.

7.3.2 Search Existing Group in Directory Server

Use the provided test framework to search for an existing group in the LDAP directory server.

7.3.3 Search Existing User Account in Directory Server

Use the provided test framework to search for an existing user account in the LDAP directory server.

7.3.4 Create New User

Use the provided test framework to create a new user in the LDAP directory server.

7.3.5 Modify Existing User

Use the provided test framework to modify the user information of an existing user in the LDAP directory server.

7.3.6 Delete Existing User

Use the provided test framework to delete an existing user in the LDAP directory server.

7.3.7 Create *n* New Users

Use the provided test framework to create *n* new users in the LDAP directory server.

7.3.8 Create New Group

Use the provided test framework to create a new group in the LDAP directory server.

Note: Groups can only be created in a flat hierarchy.

7.3.9 Modify Existing Group

Use the provided test framework to modify an existing group in the LDAP directory server. Perform the following tasks:

- Create a new member (assign a user to a group)
- Modify an existing member (modify group assignment)
- Delete an existing member (delete group assignment)

7.3.10 Delete Existing Group

Use the provided test framework to delete an existing group in the LDAP directory server.

7.3.11 Create *n* New Groups

Use the provided test framework to create *n* new groups in the LDAP directory server.

Note: Groups can only be created in a flat hierarchy.

7.3.12 Create New User Account

Use the provided test framework to create a new user account in the LDAP directory server.

7.3.13 User Authentication Through UserID and Password Verification Against LDAP Directory Server

Set up UME for form-based logon with user ID and password authentication. Use the pre-configured authentication scheme (“default”) provided. For more detailed information on setting up user ID and password authentication for UME, see the section on *Authentication* in the *SAP Enterprise Portal 6.0 Security Guide*.

Log on to UME by providing the user ID and password of an end-user.

Since an LDAP bind operation is used, the end-user's password will be sent in clear text. If SSL is used, the end-user's password will be sent in encrypted form.

7.3.14 Change Password

Change the password of a user in the LDAP directory server.

7.3.15 Try to Log On with Old and New Password

Log on to UME with the old password of the user (see section 7.3.14). Access is denied.

Log on to UME with the new password of the user (see section 7.3.14). Access is granted.

7.3.16 Delete User Account

Use the provided test framework to delete an existing user account in the LDAP directory server.

7.3.17 Read All Important Data for a User From Directory

Use the provided test framework to read all important data for a user from the LDAP directory server.

7.3.18 Client Certificate Mapping and Handling

Download the test application "UME_Certificate_Test.zip" from the BC-LDAP-USR interface scenario webpage.

Extract the file and adjust the file conf.props.

Set the property *ldap.certificate.base64* to false as this is the default bahaviour of the UME. Change this property only to true in case you face problems with the certificate handling. Set this property to true if the directory server doesn't support the storage of certificates in binary format and also doesn't support the search for users with certificates in binary formats.

Start the test application by calling certtest.cmd.

7.4 Additional Requirements

7.4.1 Indexed Attributes

For performance reasons indexes on attributes must be supported. SAP recommends to create a new index on the following logical attributes used in the Java API of the UME:

- j_user <logon id>
- uniquename
- PRINCIPAL_RELATION_MEMBER_ATTRIBUTE

The object class attribute should also be indexed.

If the vendor's standard schema is used, the important attributes are already indexed.

7.4.2 Information / Documentation

Supply a URL of directory server documentation in the Web (especially schema reference).

7.4.3 Contact for Future Support and Quick Answers

Supply information about support channels, mail contact, technical contact person.

8 Appendix – WebAS ABAP Part

This appendix is relevant for the WebAS ABAP part of the certification.

8.1 sapAddOnUM Object Class

An entry in the directory that represents a user in the SAP WebAS must be tagged with a dedicated object class. This object class also declares the SAP specific attributes that the entry can store.

The object class is named `sapAddOnUM` and has the OID 1.3.6.1.4.1.694.2.2.6. It should be declared as "auxiliary" object class, meaning that an entry in the directory can be "upgraded" to an SAP WebAS user by giving it this object class in addition to the other object classes it already possesses.

Object class `sapAddOnUM` has the superior (SUP) object class "top".

The following attributes are obligatory (MUST) attributes for the object class:

- sapUsername
- sn

The following attributes are optional (MAY) attributes for the object class:

- sapAlias
- sapCompanyKey
- birthName
- buildingName
- commType
- ou
- mail
- facsimileTelephoneNumber
- givenName
- floor
- title
- inhouseMail
- initials
- initialsSig
- middleName
- nickname
- firstPrefix
- secondPrefix
- roomNumber
- secondName
- telephoneNumber
- titleAcademic1
- titleAcademic2
- salutation

- personalTitle
- employeeNumber
- sapClass
- sapValidTo
- sapValidFrom
- sapLanguage
- sapTimeZone
- sapUserType
- sapCATT
- sapDateFormat
- sapDecimalFormat
- costCenter
- sapLoginLanguage
- sapPrintParam3
- sapPrintParam2
- sapSpool
- sapPrintParam1
- sapStartMenu
- sapParameters
- sapSncGuiFlag
- sapSncName
- sapRefUser
- sapGroups
- sapProfiles
- sapRoles

8.2 Example of schema extension file

The following content of a schema extension file demonstrate the style of text file that the vendor must provide to SAP in order to implement it into the SAP WebAS for usage by the customer.

See the remark regarding “Equality rule” in section 8.3.

```
# ------------------------------------------------------
# PROPRIETARY/CONFIDENTIAL
# Use of this product is subject to license terms
# Copyright (c) 2004 SAP AG, Germany
# All rights reserved
#
# Schema used by the SAP Directory Interfaces for
# - User Management
#
# ------------------------------------------------------
# Version 1
#
# Usage: <DESCRIBE HERE WHAT A CUSTOMER MUST DO TO MAKE A SCHEMA EXTENSION USING THIS FILE>
#        <NAME ALL TOOLS AND STEPS REQUIRED>
#
# ------------------------------------------------------
# History
#
# Version 1: initial release
#
# ------------------------------------------------------
#
dn: cn=schema
```

```
attributetypes: ( 1.3.6.1.4.1.694.2.1.101 NAME 'sapUsername' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.102 NAME 'sapAlias' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.103 NAME 'sapCompanyKey' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.104 NAME 'birthName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 0.9.2342.19200300.100.1.48 NAME 'buildingName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: ( 1.3.6.1.4.1.694.2.1.106 NAME 'commType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.107 NAME 'floor' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.108 NAME 'salutation' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.109 NAME 'inHouseMail' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.110 NAME 'initialsSig' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.111 NAME 'middleName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.112 NAME 'nickname' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.113 NAME 'firstPrefix' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.114 NAME 'secondPrefix' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.115 NAME 'secondName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.116 NAME 'titleAcademic1' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.117 NAME 'titleAcademic2' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.119 NAME 'sapClass' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.120 NAME 'sapValidTo' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.121 NAME 'sapValidFrom' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.122 NAME 'sapLanguage' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.123 NAME 'sapTimeZone' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.124 NAME 'sapUserType' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.125 NAME 'sapCATT' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.126 NAME 'sapDateFormat' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.127 NAME 'sapDecimalFormat' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.128 NAME 'costCenter' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.129 NAME 'sapLoginLanguage' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.130 NAME 'sapPrintParam3' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.131 NAME 'sapPrintParam2' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.132 NAME 'sapSpool' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.133 NAME 'sapPrintParam1' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.134 NAME 'sapStartMenu' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.135 NAME 'sapParameters' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: ( 1.3.6.1.4.1.694.2.1.136 NAME 'sapSncGuiFlag' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.137 NAME 'sapSncName' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.138 NAME 'sapRefUser' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE )
attributetypes: ( 1.3.6.1.4.1.694.2.1.139 NAME 'sapGroups' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: ( 1.3.6.1.4.1.694.2.1.140 NAME 'sapProfiles' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes: ( 1.3.6.1.4.1.694.2.1.141 NAME 'sapRoles' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
objectclasses: ( 1.3.6.1.4.1.694.2.2.6 NAME 'sapAddOnUM' SUP top AUXILIARY MUST ( sapUsername $ sn ) MAY ( sapAlias $ sapCompanyKey $
birthName $ buildingName $ commType $ ou $ mail $ facsimileTelephoneNumber $ givenName $ floor $ title $ inhouseMail $ initials $
initialsSig $ middleName $ nickname $ firstPrefix $ secondPrefix $ roomNumber $ secondName $ telephoneNumber $ titleAcademic1 $
titleAcademic2 $ salutation $ personalTitle $ employeeNumber $ sapClass $ sapValidTo $ sapValidFrom $ sapLanguage $ sapTimeZone $
sapUserType $ sapCATT $ sapDateFormat $ sapDecimalFormat $ costCenter $ sapLoginLanguage $ sapPrintParam3 $ sapPrintParam2 $ sapSpool $
sapPrintParam1 $ sapStartMenu $ sapParameters $ sapSncGuiFlag $ sapSncName $ sapRefUser $ sapGroups $ sapProfiles $ sapRoles ) )
```

8.3 Fields for Mapping

The following table lists the fields of the SAP Web Application Server user master data that can be synchronized with a directory and lists the attributes to which these fields are mapped to for some products that are already certified.

Column description:

- **SAP WebAS Field of user master data:** Describes the field of the user master that shall be synchronized.
- **Attribute type:** This attribute type seems suitable to hold the information and is the current mapping proposal of SAP for some certified products.
- **OID:** The OID of the attribute type that should be used if the attribute must be created in the schema. The namespace starting with 1.3.6.1.4.1.694 is assigned to SAP AG.
- **Syntax:** The attribute syntax that should be used if the attribute must be created in the schema. If a vendor wants to map WebAS field to another attribute type with a different syntax this is permitted, given that the finally used syntax allows storing all information that the proposed syntax could also store.
- **Equality rule:** The equality rule that should be used if the attribute must be created in the schema. If a vendor wants to map WebAS field to another attribute type with a different equality rule this is permitted. An exception from that freedom is the “sapUsername” attribute. It must be created in a way that equality comparison uses “caseIgnoreMatch” and additionally substring matches must be supported with “caseIgnoreSubstringMatch”. The example LDIF file shown in 8.2 was created for a directory which sets these rules automatically. If your directory does not do so, an explicit specification of the rules must be made,. Example: “… NAME 'sapUsername' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch …”.
- **Single:** Specifies whether the attribute type must be capable of storing multiple values.
- **Min. Width:** Specifies the length of the field in the SAP WebAS. The attribute type used for this field must be capable of holding at least this length of character data.

Please see section 3.3 for information how the information from this table should be used.

SAP WebAS Field of user master data	Attribute type	OID	Syntax	Equality rule	Single	Min. Width
Fields using re-used attribute types						
Last name	sn	2.5.4.4	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		40
First telephone number	telephoneNumber	2.5.4.20	1.3.6.1.4.1.1466.115.121.1.50	telephoneNumberMatch	X	41
Department	ou	2.5.4.11	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		40
First fax number	facsimileTelephoneNumber	2.5.4.23	1.3.6.1.4.1.1466.115.121.1.22			41

Function of a person, e.g. as contact person in a company	title	2.5.4.12	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		40
First name	givenName	2.5.4.42	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		40
"Middle Initial" or personal initials	initials	2.5.4.43	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		10
Room or apartment Number	roomNumber	0.9.2342.19200300.100.1.6	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	10
E-Mail address	mail	0.9.2342.19200300.100.1.3	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	241
Building (number or code)	buildingName	0.9.2342.19200300.100.1.48	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		10
Employee identifier	employeeNumber	2.16.840.1.113730.3.1.3	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	12
Fields using SAP defined attribute types						
SAP username	sapUsername	1.3.6.1.4.1.694.2.1.101	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch caseIgnoreSubstringMatch	X	12
Logon alias	sapAlias	1.3.6.1.4.1.694.2.1.102	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	40
Company identifier	sapCompanyKey	1.3.6.1.4.1.694.2.1.103	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	42
Name of person at birth	birthName	1.3.6.1.4.1.694.2.1.104	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	40
Communication Method (SAP key)	commType	1.3.6.1.4.1.694.2.1.106	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	3
Floor in building	floor	1.3.6.1.4.1.694.2.1.107	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	10
Title text	salutation	1.3.6.1.4.1.694.2.1.108	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	30
Internal mail postal code	inHouseMail	1.3.6.1.4.1.694.2.1.109	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	10
Short name for correspondence	initialsSig	1.3.6.1.4.1.694.2.1.110	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	10
Middle name or second forename of a person	middleName	1.3.6.1.4.1.694.2.1.111	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	40
Nickname or name used	nickname	1.3.6.1.4.1.694.2.1.112	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	40
Name prefix	firstPrefix	1.3.6.1.4.1.694.2.1.113	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	20
Second name prefix	secondPrefix	1.3.6.1.4.1.694.2.1.114	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	20
Second surname of a person	secondName	1.3.6.1.4.1.694.2.1.115	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	40
Academic title: Written form	titleAcademic1	1.3.6.1.4.1.694.2.1.116	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	20
Second academic title: Written form	titleAcademic2	1.3.6.1.4.1.694.2.1.117	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	20
Name supplement, e.g. noble title (written form)	personalTitle	1.3.6.1.4.1.694.2.1.118	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	20
User group in user master maintenance	sapClass	1.3.6.1.4.1.694.2.1.119	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	12

User logon account valid to	sapValidTo	1.3.6.1.4.1.694.2.1.120	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	8
User logon account valid from	sapValidFrom	1.3.6.1.4.1.694.2.1.121	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	8
Language according to ISO 639	sapLanguage	1.3.6.1.4.1.694.2.1.122	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	2
Time zone	sapTimeZone	1.3.6.1.4.1.694.2.1.123	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	6
User type	sapUserType	1.3.6.1.4.1.694.2.1.124	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
Internal control flag for CATT (computer aided test tool)	sapCATT	1.3.6.1.4.1.694.2.1.125	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
SAP key for date format	sapDateFormat	1.3.6.1.4.1.694.2.1.126	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
SAP key for decimals format	sapDecimalFormat	1.3.6.1.4.1.694.2.1.127	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
Cost center of user	costCenter	1.3.6.1.4.1.694.2.1.128	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	8
Login language (SAP internal key)	sapLoginLanguage	1.3.6.1.4.1.694.2.1.129	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
SAP internal printing parameter	sapPrintParam3	1.3.6.1.4.1.694.2.1.130	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
SAP internal printing parameter	sapPrintParam2	1.3.6.1.4.1.694.2.1.131	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
SAP printer name	sapSpool	1.3.6.1.4.1.694.2.1.132	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	4
SAP internal printing parameter	sapPrintParam1	1.3.6.1.4.1.694.2.1.133	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
Entry point for SAP Easy Access menu	sapStartMenu	1.3.6.1.4.1.694.2.1.134	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	30
User parameters	sapParameters	1.3.6.1.4.1.694.2.1.135	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		61
Insecure communication permitted (user-specific)	sapSncGuiFlag	1.3.6.1.4.1.694.2.1.136	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	1
SNC (Secure Network Connection): Printable name of user	sapSncName	1.3.6.1.4.1.694.2.1.137	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	255
Reference user for role assignment	sapRefUser	1.3.6.1.4.1.694.2.1.138	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch	X	12
SAP User Groups the user is assigned to	sapGroups	1.3.6.1.4.1.694.2.1.139	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		12
SAP Authorization profiles the user is assigned to	sapProfiles	1.3.6.1.4.1.694.2.1.140	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		23
SAP Roles the user is assigned to	sapRoles	1.3.6.1.4.1.694.2.1.141	1.3.6.1.4.1.1466.115.121.1.15	caseIgnoreMatch		41