



One Identity Manager 8.2

LDAP Connector for IBM AS/400 Reference Guide

Copyright 2021 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

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

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

Contents

Initializing and configuring the LDAP connector for IBM AS/400	4
Prerequisites	4
Platform support	5
How to initialize and configure the AS/400 LDAP connector	5
System variables	6
Domain filter setting	7
User mapping information	8
Mandatory AS/400 user attributes	9
Property mapping rules	10
Object matching rules	12
Sample user mapping	13
Group mapping information	13
Mandatory AS/400 group attributes	14
Property mapping rules	15
Object matching rules	17
Sample group mapping	17
Appendix: AS/400 attributes	19
About us	22
Contacting us	22
Technical support resources	22

Initializing and configuring the LDAP connector for IBM AS/400

This document describes how to initialize and configure the AS/400 LDAP connector into an existing One Identity Manager system. This enables a One Identity Manager system to access, read, and update data stored on an AS/400 system.

NOTE: Although the AS/400 system has been given more recent names, such as iSeries and System i, it will be referred to as AS/400 throughout this document.

Detailed information about this topic

- [Prerequisites](#) on page 4
- [Platform support](#) on page 5
- [How to initialize and configure the AS/400 LDAP connector](#) on page 5
- [Domain filter setting](#) on page 7
- [System variables](#) on page 6
- [User mapping information](#) on page 8
- [Group mapping information](#) on page 13
- [AS/400 attributes](#) on page 19

Prerequisites

- The AS/400 computer must have IBM AS/400 Directory Services installed and configured.
- A service account must be created on your AS/400 server that has the appropriate permissions to administer users and groups on this platform:
 - Security administrator (*SECADM) special authority rights
 - Object management (*OBJMGT) rights over the user profile accounts that are to be managed

- Use (*USE) rights over the user profile accounts that are to be managed
- Service account set up as a projected user

NOTE: Before attempting to connect to the AS/400 Directory Services LDAP server with the One Identity Manager connector, first check that the LDAP server is running correctly. This can be tested with any LDAP browser, for example, the LDP.exe tool from Microsoft. For more information, see your *LDAP browser documentation*.

Platform support

The AS/400 LDAP connector has been verified for synchronization against os-400 V7R1 or later.

How to initialize and configure the AS/400 LDAP connector

NOTE: The following sequence describes how you configure a synchronization project if the Synchronization Editor is in expert mode.

To set up initial synchronization project for AS/400

1. Start the Synchronization Editor and log in.
2. From the start page, select **Start a new synchronization project**.
This starts the Synchronization Editor project wizard.
3. On the **Choose target system** page, select **AS/400 LDAP Connector**.
4. On the **System access** page, click **Next**.
5. On the **Create system connection** page, select **Create new system connection**.
6. On the system connection wizard start page, click **Next**.
7. On the **Network** page:
 - a. In the **Server** field, enter the DNS name or IP address of your mainframe server.
 - b. In the **Port** field, enter the port number.
 - c. Click **Test** to make sure the server is accessible.
 - d. IBM AS/400 Directory Services supports LDAP v3. Enter the number 3 in the **Protocol version**.
 - e. If SSL is to be used, select the **Use SSL** check box.
8. On the **Authentication** page:

- a. Set the **Authentication method** to **Basic**.
- b. In the **Credentials** section, enter the full DN and password of the administrator account on your AS/400 system.
- c. Click **Test** to check that the credentials are valid.

The schema is loaded from the AS/400 system.

9. Ignore the **Define virtual classes** page. Click **Next**.
10. On the **Search options** page:
 - a. In the **Base DN** drop-down list, select the correct base DN for your system. It should begin with **OS400-SYS=**.
 - b. Ignore the **Use paged search** check box.
11. Ignore the **Modification capabilities** page. Click **Next**.
12. Ignore the **Auxiliary class assignment** page. Click **Next**.
13. On the **System attributes** page, in the **Revision properties** section, clear the **createTimestamp** and **modifyTimestamp** entries by double-clicking them.
14. Ignore the **Select dynamic group attributes** page. Click **Next**.
15. Ignore the **Password settings** page. Click **Next**.
16. Click **Finish**.

This takes you back to the Synchronization Editor project wizard.
17. On the **One Identity Manager connection** page, enter the database connection data.

This loads the AS/400 schema into your One Identity Manager. Wait for this to complete.
18. On the **Select project template** page, select **Create blank project**.
19. On the **General** page, enter a display name for your synchronization project and set a scripting language if required.
20. Click **Finish**.
21. Select **Activate project**.

System variables

The following system variables need to be defined for the attribute mappings. For more detailed information about variables, see the *One Identity Manager Target System Synchronization Reference Guide*.

Table 1: System variables

Name	Value
IdentDomain	The name of your AS/400 domain, for example, AS400_001
UserLocation	Parent DN of your AS/400 user container, for example, CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM
GroupLocation	Parent DN of your AS/400 group container, for example, CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM

Related topics

- [Domain filter setting](#) on page 7
- [Property mapping rules](#) on page 10
- [Property mapping rules](#) on page 15

Domain filter setting

A domain filter needs to be created to identify information that has been retrieved from the AS/400 database to keep it separate from other imported data.

1. Update the One Identity Manager schema so that all entries are included.
 - a. In the Synchronization Editor, open your AS/400 project.
 - b. Select **Configuration > One Identity Manager connection**.
 - c. In the **General** section, click **Update schema**.
 - d. Click **Yes** in the next two dialogs.
 - e. Click **OK** when completed.
2. In the Manager
 - a. Select **LDAP > Domains**.
 - b. In the result list toolbar, click .

- c. On the **General** tab, enter the following general master data.

Table 2: Domain master data

Property	Description
Display name	Display name, for example, AS400 Domain 001
Distinguished name	Distinguished name of the domain, for example, OS400-SYS=AS4001.MYCOMPANY.COM
Domain	Domain name, for example, AS400_001
Structural object class	Structural object class representing the object type; enter DCOBJECT

- d. Save the changes.
3. In the Synchronization Editor, open your AS/400 project.
 - a. Select **Configuration > One Identity Manager connection**.
 - b. Select **Scope view** and click **Edit scope**.
 - c. Select the object type LDPDomain in the **Scope hierarchy** list and set the **Object filter** to Ident_Domain = '\$IdentDomain\$'.
 - d. Save the changes.

For more detailed information about scopes, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [System variables](#) on page 6

User mapping information

This section shows a possible mapping between a user account in AS/400 and the standard One Identity Manager database table called LDAPAccount. User and group information on the AS/400 is stored in the same container, so a filter needs to be set up to tell these apart.

- When creating the user mapping, add a new schema class as follows.

Table 3: Schema class settings

Property	Value
Schema type	os400-usprf
Display name	user_os400_usrprf
Class name	user_os400_usrprf
Select objects: Condition	os400_gid='*NONE'
Select objects: Ignore case	Activated

- Map the LDAPAccount (a11) schema class to this new schema class, user_os400_usrprf, for this user mapping.

For more detailed information about setting up mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Mandatory AS/400 user attributes](#) on page 9
- [Property mapping rules](#) on page 10
- [Object matching rules](#) on page 12
- [Sample user mapping](#) on page 13

Mandatory AS/400 user attributes

When creating a user in the AS/400 database, the following LDAP attributes must be defined:

- objectclass
- os400-profile

Related topics

- [Property mapping rules](#) on page 10
- [Object matching rules](#) on page 12

Property mapping rules

- CanonicalName ← vrtEntryCanonicalName
vrtEntryCanonicalName is a virtual property, set to the canonical name of the object in the connector.
Sample value:
AS4001.MYCOMPANY.COM/ACCOUNTS/USER1234
- cn ←→ os400-profile
On the AS/400 system, os400-profile is the user ID.
Sample value:
USER1234
- DistinguishedName ← vrtEntryDN
vrtEntryDN is a virtual property, set to the DN of the object in the connector. Once this mapping rule has been created, edit the mapping rule by clicking on it. Then select **Force mapping against direction of synchronization**.
Sample value:
os400-profile=USER1234,CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM
- ObjectClass ←→ objectClass
The objectClass attribute (multi-valued) on the AS/400 system. Enable **Ignore case sensitivity**.
Sample value:
TOP;OS400-USRPRF
- StructuralObjectClass ← vrtStructuralObjectClass
vrtStructuralObjectClass on the AS/400 system defines the single object class for the object type.
Sample value:
OS400-USRPRF
- UID_LDPDomain ← vrtIdentDomain
Create a fixed value property variable on the AS/400 side called vrtIdentDomain that is set to the value \$IdentDomain\$. Map this to UID_LDPDomain. This will cause a conflict, and the Property Mapping Rule Conflict Wizard opens automatically.

To resolve the conflict

1. In the Property Mapping Rule Conflict Wizard, select the first option and click **OK**.
2. On the **Select an element** page, select **Ident_Domain** and click **OK**.
3. Confirm the security prompt with **OK**.

4. On the **Edit property** page:
 - a. Clear **Save unresolvable keys**.
 - b. Select **Handle failure to resolve as error**.
5. To close the Property Mapping Rule Conflict Wizard, click **OK**.

Sample value:

AS400_001

- vrtParentDN → vrtEntryParentDN

Create a fixed-value property variable on the One Identity Manager side called vrtParentDN equal to a fixed string with value \$UserLocation\$. Map this to vrtEntryParentDN on the AS/400 side.

Sample value:

CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM

- vrtRDN → vrtEntryRDN

Create a new variable on the One Identity Manager side of type **Format Defined Property** with the name vrtRDN. Set its value to os400-profile=%CN%. Then map this to vrtEntryRDN on the AS/400 side.

Sample value:

os400-profile=USER1234

- userPassword → os400-password

Used to change a user's AS/400 password. A condition needs to be set on this rule to map the password only when there is a value to be copied.

To add a condition

1. Create the mapping.
2. Edit the property mapping rule.
3. Expand the **Condition for execution** section at the bottom of the dialog.
4. Click **Add condition** and set the following condition (a blank password is indicated by using two apostrophe characters).

Left.UserPassword<>' '

- UID_LDAPContainer ← vrtEmpty

This is a workaround needed to support group mappings. Create a new fixed-value variable on the AS/400 side of type **String** with no value called vrtEmpty. Map this to UID_LDAPContainer. This generates a property mapping rule conflict.

To resolve the conflict

- In the Property Mapping Rule Conflict Wizard, highlight **Select this option if you do not want to change anything** and click **OK**.

Related topics

- [Mandatory AS/400 user attributes](#) on page 9
- [System variables](#) on page 6
- [Object matching rules](#) on page 12
- [Sample user mapping](#) on page 13

Object matching rules

- DistinguishedName (primary rule) vrtEntryDN
vrtEntryDN is a virtual property, set to the DN of the object in the connector. This forms a unique ID to distinguish individual user objects on the AS/400 system.

To convert this mapping into an object matching rule

1. Select the property mapping rule in the rule window.
2. Click  in the rule view toolbar.
A message appears.
3. Click **Yes** to convert the property mapping rule into an object matching rule and save a copy of the property mapping rule.
4. Open the new object matching rule in the top window and clear the **Case sensitive** check box.

Sample value:

os400-profile=USER1234,CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM

Related topics

- [Mandatory AS/400 user attributes](#) on page 9
- [Property mapping rules](#) on page 10
- [Sample user mapping](#) on page 13

Sample user mapping

The following figure shows the user mapping in operation.

 Object matching rules

       

Schema property in One Identity Manager	Information	Schema property in the target system
DistinguishedName	Primary rule	vrtEntryDN

 Property mapping rules

    

Schema property in One Identity Manager		Information	Schema property in the target system
CanonicalName	←		vrtEntryCanonicalName
cn	←		→ os400-profile
DistinguishedName	←		vrtEntryDN
ObjectClass	←		→ objectClass
StructuralObjectClass	←		vrtStructuralObjectClass
UID_LDAPContainer	←		vrtEmpty
VRT_UID_LDAPDomain	←		vrtIdentDomain
UserPassword	←	?	→ os400-password
vrtParentDN			→ vrtEntryParentDN
vrtRDN			→ vrtEntryRDN

Group mapping information

This section shows a possible mapping between a group profile in AS/400 and the standard One Identity Manager database table called LDAPGroup. User and group information on the AS/400 is stored in the same container, so a filter needs to be set up to tell these apart.

- When creating the group mapping, add a new schema class as follows.

Table 4: Schema class settings

Property	Value
Schema type	os400-usprf
Display name	group_os400_usrprf
Class name	group_os400_usrprf
Select objects: Condition	os400_gid<>*NONE'
Select objects: Ignore case	Activated

- Map the LDAPGroup (a11) schema class to this new schema class, group_os400_usrprf, for this group mapping.

For more detailed information about setting up mappings, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Mandatory AS/400 group attributes](#) on page 14
- [Property mapping rules](#) on page 15
- [Object matching rules](#) on page 17
- [Sample group mapping](#) on page 17

Mandatory AS/400 group attributes

When creating a group in the AS/400 database, the following LDAP attributes must be defined:

- objectclass
- os400-profile
- os400-groupmember (this is not mandatory but if omitted, a user profile will be created instead)

Related topics

- [Property mapping rules](#) on page 15
- [Object matching rules](#) on page 17

Property mapping rules

- CanonicalName ← vrtEntryCanonicalName
vrtEntryCanonicalName is a virtual property, set to the canonical name of the object in the connector.
Sample value:
AS4001.MYCOMPANY.COM/ACCOUNTS/GROUP123
- cn ←→ os400-profile
On the AS/400 system, os400-profile is the group ID.
Sample value:
USERGRP
- DistinguishedName ← vrtEntryDN
vrtEntryDN is a virtual property, set to the DN of the object in the connector.
Sample value:
os400-profile=GROUP123,CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM
- ObjectClass ←→ objectClass
The objectClass attribute (multi-valued) on the AS/400 system. Select the **Ignore case sensitivity** check box.
Sample value:
TOP;OS400-USRPRF
- StructuralObjectClass ← vrtStructuralObjectClass
vrtStructuralObjectClass on the AS/400 system defines the single object class for the object type.
Sample value:
OS400-USRPRF
- vrtParentDN → vrtEntryParentDN
Create a fixed value property variable on the One Identity Manager side called vrtParentDN equal to a fixed string with the value \$GroupLocation\$. Map this to vrtEntryParentDN on the AS/400 side.
Sample value:
CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM
- vrtRDN → vrtEntryRDN
Create a virtual attribute on the One Identity Manager side equal to the CN value. Then map this to vrtEntryRDN on the AS/400 side.
Sample value:
os400-profile=GROUP123

- UID_LDAPContainer ← vrtEmpty

This is a workaround needed to support group mappings. Create a new fixed value variable on the AS/400 side of type **String** with no value called vrtEmpty. Map this to UID_LDAPContainer. This generates a property mapping rule conflict.

To resolve the conflict

- In the Property Mapping Rule Conflict Wizard, highlight **Select this option if you do not want to change anything** and click **OK**.

- vrtMember ↔ os400-groupmember

Synchronizing this attribute on the AS/400 will manage the group memberships for the user.

1. Create a new virtual entry on the One Identity Manager side of type **Members of M:N schema types** with the name vrtMember. Select the **Ignore case** and **Enable relative component handling** check boxes.
2. Add an entry for LDAPAccountInLDAPGroup(a11). Set the left box to UID_LDAPGroup and the right box to UID_LDAPAccount. Set the **Primary Key Property** to DistinguishedName.
3. Create a new mapping rule of type **Multi-reference mapping rule**. Set the rule name to **Member** and the mapping direction to **Both directions**. Set the One Identity Manager schema property to vrtMember and the AS/400 schema property to os400-groupmember.

- UID_LDPDomain ← vrtIdentDomain

Create a fixed-value property variable on the AS/400 side called vrtIdentDomain that is set to the value \$IdentDomain\$. Map this to UID_LDPDomain. This will cause a conflict and the Property Mapping Rule Conflict Wizard opens automatically.

To resolve the conflict

1. In the Property Mapping Rule Conflict Wizard, select the first option and click **OK**.
2. On the **Select an element** page, select **Ident_Domain** and click **OK**.
3. Confirm the security prompt with **OK**.
4. On the **Edit property** page:
 - a. Clear **Save unresolvable keys**.
 - b. Select **Handle failure to resolve as error**.
5. To close the Property Mapping Rule Conflict Wizard, click **OK**.

Sample value:

AS400_001

Related topics

- [Mandatory AS/400 group attributes](#) on page 14
- [System variables](#) on page 6

- [Object matching rules](#) on page 17
- [Sample group mapping](#) on page 17

Object matching rules

- DistinguishedName (primary rule) vrtEntryDN
vrtEntryDN is a virtual property, set to the DN of the object in the connector. This forms a unique ID to distinguish individual user objects on the AS/400 system.

To convert this mapping into an object matching rule

1. Select the property mapping rule in the rule window.
2. Click  in the rule view toolbar.
A message appears.
3. Click **Yes** to convert the property mapping rule into an object matching rule and save a copy of the property mapping rule.

Sample value:

os400-profile=GROUP123,CN=ACCOUNTS,OS400-SYS=AS4001.MYCOMPANY.COM

Related topics

- [Mandatory AS/400 group attributes](#) on page 14
- [Property mapping rules](#) on page 15
- [Sample group mapping](#) on page 17

Sample group mapping

The following figure shows the group mapping in operation.

Object matching rules



Schema property in One Identity Manager	Information	Schema property in the target system
DistinguishedName	Primary rule	vrtEntryDN

Property mapping rules



Schema property in One Identity Manager	Information	Schema property in the target system
CanonicalName	←	vrtEntryCanonicalName
cn	←	→ os400-profile
DistinguishedName	←	vrtEntryDN
vrtMember	←	→ os400-groupmember
ObjectClass	←	→ objectClass
StructuralObjectClass	←	vrtStructuralObjectClass
UID_LDAPContainer	←	vrtEmpty
VRT_UID_LDAPDomain	←	vrtIdentDomain
vrtParentDN		→ vrtEntryParentDN
vrtRDN		→ vrtEntryRDN

Appendix A

AS/400 attributes

The following table lists the AS/400 attributes that are made available to One Identity Manager by the AS/400 LDAP connector. User and group objects in the AS/400 Directory Server are treated at the same level.

Table 5: List of AS/400 attributes

Attribute name
os400-acgcde
os400-astlvl
os400-atnpgm
os400-audlvl
os400-ccsid
os400-chridctl
os400-cntryid
os400-curlib
os400-dlvry
os400-docpwd
os400-dspsgninf
os400-eimassoc
os400-gid
os400-groupmember
os400-grpaut
os400-grpauttyp
os400-grpprf
os400-homedir

Attribute name

os400-laspStorageInformation

os400-inlmnu

os400-inlpgm

os400-invalidSignonCount

os400-jobd

os400-kbdbuf

os400-langid

os400-lclpwdmgt

os400-lmtdevssn

os400-locale

os400-maxstg

os400-msgq

os400-objaud

os400-outq

os400-owner

os400-password

os400-passwordExpirationDate

os400-passwordLastChanged

os400-previousSignon

os400-profile

os400-prtdev

os400-ptylmt

os400-pwdexp

os400-pwdexpitv

os400-setobatr

os400-sev

os400-spcaut

os400-spcenv

os400-status

Attribute name

os400-storageUsed

os400-storageUsedOnlasp

os400-supgrpprf

os400-text

os400-uid

os400-usrcls

os400-usropt

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

Contacting us

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

Technical support resources

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

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

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