



One Identity Manager 9.2

LDAP Connector for CA ACF2 Reference Guide

Copyright 2023 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/trademark-information.aspx. 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.**

One Identity Manager LDAP Connector for CA ACF2 Reference Guide
Updated - 29 September 2023, 04:42

For the most recent documents and product information, see [Online product documentation](#).

Contents

| | |
|--|-----------|
| Initializing and configuring the LDAP connector for CA ACF2 | 4 |
| Prerequisites | 4 |
| Platform support | 5 |
| Operating constraints | 5 |
| How to initialize and configure the ACF2 LDAP connector | 5 |
| System variables | 7 |
| Domain filter setting | 7 |
| User mapping information | 8 |
| Mandatory ACF2 user attributes | 9 |
| Property mapping rules | 9 |
| Object matching rules | 11 |
| Sample user mapping | 11 |
| Appendix: ACF2 attributes | 13 |
| About us | 21 |
| Contacting us | 21 |
| Technical support resources | 21 |

Initializing and configuring the LDAP connector for CA ACF2

This document describes how to initialize and configure the ACF2 LDAP connector into an existing One Identity Manager system. This enables One Identity Manager to access, read, and update data stored in an ACF2 database on an IBM mainframe.

Detailed information about this topic

- [Prerequisites](#) on page 4
- [Platform support](#) on page 5
- [Operating constraints](#) on page 5
- [How to initialize and configure the ACF2 LDAP connector](#) on page 5
- [Domain filter setting](#) on page 7
- [System variables](#) on page 7
- [User mapping information](#) on page 8
- [ACF2 attributes](#) on page 13

Prerequisites

- The IBM mainframe must have the CA LDAP Server for z/OS installed and configured. It is recommended that you remove the search size limit on the CA LDAP Server. You can do this by editing the configuration file `slapd.conf` on the server. Set the `sizelimit` value to unlimited as follows.

For versions of CA LDAP Server version 14 or earlier

```
sizelimit 0
```

For versions of CA LDAP Server version 15 or later

```
sizelimit unlimited
```

- An LDAP service account must be created on your ACF2 server that has the appropriate permissions to administer users and groups on this platform. The account must be given sufficient privileges so that the profiles being administered fall within the scope of the administrator user.

NOTE: Before attempting to connect to the CA LDAP server with the One Identity Manager connector, first check that the CA LDAP server is running correctly. You can test this with any LDAP browser, for example, the LDP.exe tool from Microsoft. For more information, see your *LDAP browser documentation*.

Platform support

The ACF2 LDAP connector has been verified for synchronization against the IBM mainframe running CA ACF2 version 9.0 or later.

Operating constraints

- There is an eight-character limit for user names on ACF2.
- There is an eight-character limit for passwords on ACF2.

How to initialize and configure the ACF2 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 ACF2

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 **ACF2 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** ensure the server is accessible.
 - d. The CA LDAP server for z/OS supports LDAP v3. Enter the number 3 in the **Protocol version**.
 - e. If SSL is 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 ACF2 system. The account DN can take the format CN=<account id> or acf2lid=<account id>.
 - c. Click **Test** to check that the credentials are valid.

The schema is loaded from the ACF2 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.
 - b. Ignore **Use partitioned search**.
 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 ACF2 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**.

Related topics

- [Domain filter setting](#) on page 7
- [User mapping information](#) on page 8

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 ACF2 domain, for example, MAINFRAME2 |
| UserLocation | Parent DN of your ACF2 user container, for example, acf2admingrp=lids,host=mainframe2,o=mycompany,c=com |

Related topics

- [Domain filter setting](#) on page 7
- [Property mapping rules](#) on page 9

Domain filter setting

A domain filter must be created to identify information that has been retrieved from the ACF2 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 ACF2 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 complete.
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, ACF2 Domain |
| Distinguished name | Distinguished name of the domain, for example, host=mainframe2,o=mycompany,c=com |
| Domain | Domain name, for example, MAINFRAME2 |
| Structural object class | Structural object class representing the object type; enter DCOBJECT |

- d. Save the changes.
3. In the Synchronization Editor, open your ACF2 project.
 - a. Select **Configuration > One Identity Manager connection**.
 - b. Select the **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 7

User mapping information

This section shows a possible mapping between a user account in CA ACF2 and the standard One Identity Manager database table called LDAPAccount.

- Set up a new mapping from LDAPAccount(all) to acf2lid(all).

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

Detailed information about this topic

- [Mandatory ACF2 user attributes](#) on page 9
- [Property mapping rules](#) on page 9

- [Object matching rules](#) on page 11
- [Sample user mapping](#) on page 11

Mandatory ACF2 user attributes

When creating a user in the ACF2 database, the following LDAP attributes must be defined:

- objectclass
- acf2lid
- userPassword

Related topics

- [Property mapping rules](#) on page 9
- [Object matching rules](#) on page 11

Property mapping rules

- CanonicalName ← vrtEntryCanonicalName
vrtEntryCanonicalName is a virtual property, set to the canonical name of the object in the connector.
Sample value:
COM/MYCOMPANY/MAINFRAME2/LIDS/USER1234
- cn ← → acf2lid
On the ACF2 system, acf2lid 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. Select the **Force mapping against direction of synchronization** check box.
Sample value:
acf2lid=USER1234,acf2admingrp=lids,host=mainframe2,o=mycompany,c=com
- ObjectClass ← → objectClass
The objectClass attribute (multi-valued) on the ACF2 system. Select the **Ignore case sensitivity** check box.
Sample value:

ACF2LID

- StructuralObjectClass ← vrtStructuralObjectClass

vrtStructuralObjectClass on the ACF2 system defines the single object class for the object type.

Sample value:

ACF2LID

- UID_LDPODomain ← vrtIdentDomain

Create a fixed value property variable on the ACF2 side called vrtIdentDomain that is set to the value \$IdentDomain\$. Map this to UID_LDPODomain. 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:

MAINFRAME2

- vrtParentDN → vrtEntryParentDN

Create a fixed-value property variable on the One Identity Manager side called vrtParentDN equal to a fixed string with the value \$UserLocation\$. Map this to vrtEntryParentDN on the ACF2 side.

Sample value:

acf2admingrp=lids,host=mainframe2,o=mycompany,c=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 acf2lid=%CN%. Then map this to vrtEntryRDN on the ACF2 side.

Sample value:

acf2lid=USER1234

- userPassword → userPassword

Used to change a user's ACF2 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<>' '
```


Related topics

- [Mandatory ACF2 user attributes](#) on page 9
- [System variables](#) on page 7
- [Object matching rules](#) on page 11
- [Sample user mapping](#) on page 11

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 ACF2 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:

```
acf2lid=USER1234,acf2admingrp=lids,host=mainframe2,o=mycompany,c=com
```

Related topics

- [Mandatory ACF2 user attributes](#) on page 9
- [Property mapping rules](#) on page 9
- [Sample user mapping](#) on page 11

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 | vrEntryDN |

Property mapping rules



| Schema property in One Identity Manager | Information | Schema property in the target system |
|---|-------------|--------------------------------------|
| CanonicalName | ← | vrEntryCanonicalName |
| cn | ← | → acf2lid |
| DistinguishedName | ← | vrEntryDN |
| ObjectClass | ← | → objectClass |
| StructuralObjectClass | ← | vrStructuralObjectClass |
| VRT_UID_LDPPDomain | ← | vrIdentDomain |
| UserPassword | ← ? | → userPassword |
| vrParentDN | | → vrEntryParentDN |
| vrRDN | | → vrEntryRDN |

Appendix A

ACF2 attributes

The following table lists the ACF2 attributes that are made available to One Identity Manager by the ACF2 LDAP connector.

Table 3: List of ACF2 attributes

| Attribute name |
|------------------------|
| AccessCount |
| AccessDate |
| AccessRileMustValidate |
| AccessShiftName |
| AccessSource |
| AccessSourceName |
| AccessTime |
| AccessZoneName |
| ACF2AccountPriv |
| ACF2AuditPriv |
| ACF2CICSSecurity |
| ACF2ConsultPriv |
| ACF2DynamicPrivileges |
| ACF2LeaderPriv |
| acf2lid |
| ACF2RefreshPriv |
| ACF2SecurityPriv |
| ActiveDate |

Attribute name

AllowJOBFROMStmtUsage

AuthSubmissionPgm

AutomaticDump

BatchJobAuthority

BulkDataTransfer

BypassCmdLimiting

BypassManVioProcessing

BypassMusassAccessStats

BypassStepMustComplete

BypassTapeLabelLimited

BypassTapeLabelProcessing

BypassTSOCmdList

CancelDate

CICSAccess

CICSControlRecSYSID

CICSMultipleSignons

CICSOpClass

CICSOpId

CICSPriority

CICSRsrcAccessKey

CICSSecKey1-3

CICSSecKeyLast5

CICSTargetUsage

DDBHomenode

DoNotStoreACF2Rules

EUARoutine1

EUARoutine2

EUARoutine3

EUARoutine4

Attribute name

EUARoutine5

EUARoutine6

EUARoutine7

EUARoutine8

ExpirePassword

FullName

GeneralIDMSAccess

GeneralIMSAccess

GeneralTSOAccess

GeneralVAXAccess

GeneralVMAccess

GeneralVM-ESAAccess

GenerateDumps

GroupName

HasAccesToSystem

HomeDirectory

IdleTime

IDMSCListVersion

IDMSMusassOpts10-2

IDMSMusassStartPgm

IDMSSignonClist

InvalidPswdDate

InvalidPswdTime

KerberosCruV

KerberosVios

LastUpdatedDateTime

LDAPDirectorySync

LidExpireDate

LIDTEMP

Attribute name

LIDZMAX

LIDZMIN

LinuxName

LogAccessOutsideShift

LogActiveLibBatchAccess

LogActiveLibBatchAccessVios

LotusName

MaintPrivilege

MaxAddrSpaceSize

MaxCPUTime

MaxDataSpacePages

MaxDaysBetweenPswdChange

MonitorLogon

MonitorLogonSecurityAlert

MountDevices

MusassDefaultLid

MusassID

MusassInfoCall

MusassLid

MusassUpdateAuth

NonCancelPrivilege

NovellName

NumericUserID

PasswordForExtract

PCFControl

Phone

PrefixTSOMessages

PromptForMissingParms

PswdChgDateTime

Attribute name

PswdEntrySource

PSWD-MIX

PSWD-MX8

PSWD-UPP

PswdViolations

PTICKET

ReadAccessToAll

ReceiveTSOMailMsgs

ReceiveTSOMessages

ReceiveTSONotices

RecentPswdViolations

RestrictedLogonid

RsrcRuleMustValidate

RuleKeyPrefix

ScopeList

SecurityViolations

ShellProgram

SMSDefaultValues

SpecifyTSOAcctNum

SpecifyTSOLogonSize

SpecifyTSOLogonTime

SpecifyTSOLogonUnit

SpecifyTSOMsgClass

SpecifyTSOOutputDest

SpecifyTSOPerformance

SpecifyTSOProcedure

SpecifyTSORecover

StartedTaskAccess

SubmitJobThruAPFOnly

Attribute name

SuspendedLid

SynchronizedLogonNode

SYSPEXCL

TargetNodes

TraceAllEvents

TraceTSOCommands

TSOAccountPriv

TSOAccountRequired

TSOCommandListModule

TSOConsole

TSODefaultAccount

TSODefaultPerformance

TSODefaultProcedure

TSODefaultRegionSize

TSODefaultTime

TSODefaultUnit

TSODelChar

TSOFullScreenLogon

TSOHoldClass

TSOLineDelChar

TSOMailIndexRecordPtr

TSOModalMsgs

TSOMsgClass

TSOMsgPause

TSOOperator

TSOPrefix

TSOProcedureRequired

TSORecover

TSORegionSizeMax

Attribute name

TSOSubmitAuthority

TSOSubmitClass

TSOSysoutClass

TSOSysoutDest

UnicenterTNGSync

UseProtectedPrograms

UserCancelled

UserIdentificationString

userPassword

UserWhoSetCancel

UsingLID

ValidateRestrictAccess

ValidateTSOAccount

ValidateTSOProcedure

VMAutologAll

VMAutologNoPswd

VMAutologOnly

VMBypassDialValidation

VMDefaultAccount

VMDiagnose84

VMGroupLogonId

VMIdleMinutes

VMIssueD4Diagnose

VMLastLogonId

VMNoSpoolFoundAction

VMOptionalGroupId

VMPVMAccess

VMSAFDiagnose

VMSFS

Attribute name

VMSRFAccess

VMSRFAccessFromVSE

VMSyntaxErrorAction

VMTargetDiagnose

VMTargetDiagnoseReset

VMTempRuleMustExit

VMValidateAccounting

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