

Dell™ One Identity Manager 7.1.3




LDAP Connector for CA ACF2™ Reference
Guide



© 2016 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and Dell™ One Identity Manager, Active Roles, Dell™ One Identity Password Manager, and Dell™ One Identity Cloud Access Manager are trademarks of Dell Inc. in the United States and/or other jurisdictions. Microsoft, Outlook, Active Directory, Azure, SharePoint, SQL Server, Forefront, Internet Explorer, Visual Studio, Windows Server, Windows PowerShell, Windows Vista and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. SAP, SAP R/3, SAP NetWeaver Application Server, SAP HANA, and BAPI are trademarks or registered trademarks of SAP AG (or an SAP affiliate company) in Germany and other countries. IBM, DB2, RACF, Notes, Domino and LotusScript are registered trademarks of International Business Machines Corporation. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Oracle, MySQL and Java are trademarks or registered trademarks of Oracle and/or its affiliates. UNIX is a registered trademark of The Open Group. Mono is a registered trademark of Novell, Inc. Apache and Apache HTTP Server are trademarks of The Apache Software Foundation. Firefox is a registered trademark of the Mozilla Foundation. Safari is a registered trademark of Apple Inc. Chrome and Google are trademarks or registered trademarks of Google Inc., used with permission. CA ACF2 and CA Top Secret are trademarks or registered trademarks of CA Technologies Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Legend

-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

One Identity Manager LDAP Connector for CA ACF2™ Reference Guide
Updated - November 2017
Version - 7.1.3

Contents

Initializing and Configuring the LDAP Connector for CA ACF2™	4
Pre-requisites	4
Platform Support	5
Operating Constraints	5
How to initialize and configure the ACF2 LDAP connector	5
System Variables	6
Domain Filter Setting	7
User Mapping Information	8
Mandatory ACF2 User Attributes	8
Property Mapping Rules	8
Object Matching Rules	10
Sample User Mapping	11
Appendix: ACF2 Attributes	12
About Dell	19
Contacting Dell	19
Technical support resources	19

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

- [Pre-requisites](#) 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 6
- [User Mapping Information](#) on page 8
- [Appendix: ACF2 Attributes](#) on page 12

Pre-requisites

- The IBM mainframe must have the CA LDAP Server for z/OS installed and configured. It is recommended to remove the search size limit on the CA LDAP Server. This is done 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 which 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 Admin user.

NOTE: Before attempting to connect to the CA LDAP Server with the One Identity Manager connector, it is recommended to first check that the CA 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 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's project wizard.
3. Select **ACF2 LDAP Connector** on the **Choose target system** page.
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 on the **Test** button to make sure 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 to be used, check the **Use SSL** 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.
9. The schema will be loaded from the ACF2 system.

10. Ignore the **Define virtual classes** page. Click **Next**.
11. 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**.
12. Ignore the **Modification capabilities** page. Click **Next**.
13. Ignore the **Auxiliary class assignment** page. Click **Next**.
14. On the **System attributes** page, in the **Revision properties** section, deselect the "createTimestamp" and "modifyTimestamp" entries by double clicking on them.
15. Ignore the **Select dynamic group attributes** page. Click **Next**.
16. Ignore the **Password settings** page. Click **Next**.
17. Click **Finish**.
This takes you back to the Synchronization Editor's project wizard.
18. Enter the database connection data on the **One Identity Manager connection** page.
19. This will load the ACF2 schema into your One Identity Manager. Wait for this to complete.
20. On the **Select project template** page, select **Create blank project**.
21. On the **General** page, enter a display name for your synchronization project and set a scripting language if required.
22. Click **Finish** to complete the project wizard.
23. Select **Activate project** to activate the 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 Dell One Identity Manager Target System Synchronization Reference Guide.

Table 1: System variables

Name	Value
IdentDomain	The name of your ACF2 domain e.g. MAINFRAME2
UserLocation	Parent DN of your ACF2 user container, e.g. acf2admingrp=lids,host=mainframe2,o=mycompany,c=com

Related Topics

- [Domain Filter Setting](#) on page 7
- [Property Mapping Rules](#) on page 8

Domain Filter Setting

A domain filter needs to 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 the category **Configuration | One Identity Manager connection**.
 - c. Then in the "General" section on the right-hand side, click **Update schema**.
 - d. Click on **Yes** in the next two dialog boxes.
 - e. Click **Ok** when completed.
2. In the Manager
 - a. Select the category **LDAP | Domains**.
 - b. In the result list toolbar, click .
 - c. Enter at least the following general master data on the **General** tab.

Table 2: Domain Master Data

Property	Description
Display name	Display name e.g. ACF2 Domain
Distinguished name	Distinguished name of the domain e.g. host=mainframe2,o=mycompany,c=com
Domain	Domain name e.g. MAINFRAME2
Structural object class	Structural object class representing the object type, enter <code>DCOBJECT</code>

- d. Save the changes.
3. In the Synchronization Editor, open your ACF2 project.
 - a. Select the category **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 Dell 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 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 Dell One Identity Manager Target System Synchronization Reference Guide.

Detailed information about this topic

- [Mandatory ACF2 User Attributes](#) on page 8
- [Property Mapping Rules](#) on page 8
- [Object Matching Rules](#) on page 10
- [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 8
- [Object Matching Rules](#) on page 10

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. Then check the box marked **Force mapping against direction of synchronization**.

Sample value:

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

- `ObjectClass` ← → `objectClass`

The `objectClass` attribute (multi-valued) on the ACF2 system. Activate the check box **Ignore case sensitivity**.

Sample value:

```
ACF2LID
```

- `StructuralObjectClass` ← `vrtStructuralObjectClass`

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

Sample value:

```
ACF2LID
```

- `UID_LDPDomain` ← `vrtIdentDomain`

Create a fixed value property variable on the ACF2 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 solve 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. Deactivate **Save unresolvable keys**.
 - b. Activate **Handle failure to resolve as error**.
 - c. 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 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 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 on **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 8
- [System Variables](#) on page 6
- [Object Matching Rules](#) on page 10
- [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 8
- [Property Mapping Rules](#) on page 8
- [Sample User Mapping](#) on page 11

Sample User Mapping

The following figure shows the above 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	←	→ acf2lid
DistinguishedName	←	vrtEntryDN
ObjectClass	←	→ objectClass
StructuralObjectClass	←	vrtStructuralObjectClass
VRT_UID_LDAPDomain	←	vrtIdentDomain
UserPassword	?	→ userPassword
vrtParentDN		→ vrtEntryParentDN
vrtRDN		→ vrtEntryRDN

Appendix: 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
AllowJOBFROMStmtUsage
AuthSubmissionPgm
AutomaticDump
BatchJobAuthority

Attribute Name

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

EUARoutine5

EUARoutine6

EUARoutine7

EUARoutine8

ExpirePassword

FullName

GeneralIDMSAccess

Attribute Name

GeneralIMSAccess

GeneralTSOAccess

GeneralVAXAccess

GeneralVMAccess

GeneralVM-ESAAccess

GenerateDumps

GroupName

HasAccesToSystem

HomeDirectory

IdleTime

IDMSListVersion

IDMSMusassOpts10-2

IDMSMusassStartPgm

IDMSSignonClist

InvalidPswdDate

InvalidPswdTime

KerberosCruV

KerberosVios

LastUpdatedDateTime

LDAPDirectorySync

LidExpireDate

LIDTEMP

LIDZMAX

LIDZMIN

LinuxName

LogAccessOutsideShift

LogActiveLibBatchAccess

LogActiveLibBatchAccessVios

LotusName

MaintPrivilege

MaxAddrSpaceSize

MaxCPUTime

Attribute Name

MaxDataSpacePages

MaxDaysBetweenPswdChange

MonitorLogon

MonitorLogonSecurityAlert

MountDevices

MusassDefaultLid

MusassID

MusassInfoCall

MusassLid

MusassUpdateAuth

NonCancelPrivilege

NovellName

NumericUserID

PasswordForExtract

PCFControl

Phone

PrefixTSOMessages

PromptForMissingParms

PswdChgDateTime

PswdEntrySource

PSWD-MIX

PSWD-MX8

PSWD-UPP

PswdViolations

PTICKET

ReadAccessToAll

ReceiveTSOMailMsgs

ReceiveTSOMessages

ReceiveTSONotices

RecentPswdViolations

RestrictedLogonid

RsrcRuleMustValidate

Attribute Name

RuleKeyPrefix

ScopeList

SecurityViolations

ShellProgram

SMSDefaultValues

SpecifyTSOAcctNum

SpecifyTSOLogonSize

SpecifyTSOLogonTime

SpecifyTSOLogonUnit

SpecifyTSOMsgClass

SpecifyTSOOutputDest

SpecifyTSOPerformance

SpecifyTSOProcedure

SpecifyTSORecover

StartedTaskAccess

SubmitJobThruAPFOnly

SuspendedLid

SynchronizedLogonNode

SYSPEXCL

TargetNodes

TraceAllEvents

TraceTSOCommands

TSOAccountPriv

TSOAccountRequired

TSOCommandListModule

TSOConsole

TSODefaultAccount

TSODefaultPerformance

TSODefaultProcedure

TSODefaultRegionSize

TSODefaultTime

TSODefaultUnit

Attribute Name

TSODelChar

TSOFullScreenLogon

TSOHoldClass

TSOLineDelChar

TSOMailIndexRecordPtr

TSOModalMsgs

TSOMsgClass

TSOMsgPause

TSOOperator

TSOPrefix

TSOProcedureRequired

TSORecover

TSORegionSizeMax

TSOSubmitAuthority

TSOSubmitClass

TSOSysoutClass

TSOSysoutDest

UnicenterTNGSync

UseProtectedPrograms

UserCancelled

UserIdentificationString

userPassword

UserWhoSetCancel

UsingLID

ValidateRestrictAccess

ValidateTSOAccount

ValidateTSOProcedure

VMAutologAll

VMAutologNoPswd

VMAutologOnly

VMBypassDialValidation

VMDefaultAccount

Attribute Name

VMDiagnose84

VMGroupLogonId

VMIdleMinutes

VMIssueD4Diagnose

VMLastLogonId

VMNoSpoolFoundAction

VMOptionalGroupId

VMPVMAccess

VMSAFDiagnose

VMSFS

VMSRFAccess

VMSRFAccessFromVSE

VMSyntaxErrorAction

VMTargetDiagnose

VMTargetDiagnoseReset

VMTempRuleMustExit

VMValidateAccounting

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.quest.com.

Contacting Dell

For sales or other inquiries, visit <http://quest.com/company/contact-us.aspx> or call +1 949 754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <https://support.quest.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. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to <http://quest.com/trials>.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer