One Identity Manager 9.1.3

LDAP Connector for CA Top Secret Reference Guide

Contents

Initializing and configuring the LDAP connector for CA Top Secret

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

Detailed information about this topic

Prerequisites

- The IBM mainframe must have CA LDAP Server for z/OS installed and configured.

- An LDAP service account must be created on your Top Secret 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 Admin user.

NOTE: Before attempting to connect to the CA LDAP Server with the Top Secret LDAP 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 Top Secret LDAP connector has been verified for synchronization against the IBM mainframe running CA Top Secret r16.0 or later.

Operating constraints

- There is an eight-character limit for user and group names on Top Secret.
- There is an eight-character limit for passwords on Top Secret.

How to initialize and configure the Top Secret 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 Top Secret

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. On the **Choose target system** page, select **Top Secret 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 the **Test** button to make sure the server is accessible.

d. 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 Top Secret system.

c. Click **Test** to check that the credentials are valid.

The schema is loaded from the Top Secret system.

9. Ignore the **Define virtual classes** page. Click **Next**.

10. On the **Search options** page:

a. In the **Base DN** drop-down, and select the correct base DN for your system.

b. Ignore the **Use partitioned search** check box.

11. Ignore the **Modification capabilities** page. Click **Next**.

12. Ignore the **Auxiliary class assignment** page. Click **Next**.

13. Ignore the **System attributes** page. Click **Next**.

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 Top Secret schema loads into your One Identity Manager system. 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 must be defined for the attribute mappings.

Table 1: System variables

Name	Value
IdentDomain	The name of your Top Secret domain: for example, `TOPSECRET1`
UserLocation	Parent DN of your Top Secret user container: for example, `tssadmingrp=acids,host=topsecret1,o=mycompany,c=com`
GroupLocation	Parent DN of your Top Secret group container: for example, `tssadmingrp=groups,host=topsecret1,o=mycompany,c=com`
ProfileLocation	Parent DN of your Top Secret profile container: for example, `tssadmingrp=profiles,host=topsecret1,o=mycompany,c=com`

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

Related topics

- Domain filter setting on page 7
- User mapping information on page 8
- Group mapping information on page 12
- Profile mapping information on page 17

Domain filter setting

A domain filter must be created to identify information that has been retrieved from the Top Secret database to keep it separate from other imported data.

To create a domain filter:

1. Update the One Identity Manager schema so that all entries are included.

   a. In the Synchronization Editor, open your Top Secret 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, `Top Secret Domain`
Distinguished name	Distinguished name of the domain: for example, `host=topsecret1,o=mycompany,c=com`
Domain	Domain name: for example, `TOPSECRET1`
Structural object class	Structural object class representing the object type: enter **DCOBJECT**

d. Save the changes.

3. In the Synchronization Editor, open your Top Secret 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 Top Secret and the standard One Identity Manager database table called `LDAPAccount`.

- Set up a new mapping from `LDAPAccount(all)` to `tssacid(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 Top Secret user attributes on page 9
- Property mapping rules on page 9
- Object matching rules on page 12

Mandatory Top Secret user attributes

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

- objectclass
- tssacid
- name
- Department
- userPassword

Related topics

Property mapping rules

- CanonicalName ← vrtEntryCanonicalName

  `vrtEntryCanonicalName` is a virtual property, set to the canonical name of the object in the connector. Select the **Ignore case sensitivity** check box.

  Sample value:

  `COM/MYCOMPANY/TOPSECRET1/ACIDS/USER1234`

- cn ←→ tssacid

  On the Top Secret system, `tssacid` is the user ID. Select the **Ignore case sensitivity** check box.

  Sample value:

  `USER1234`

- DistinguishedName ← vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector. Once this mapping rule is created, edit the mapping rule by clicking on it. Select the **Ignore case sensitivity** check box.

  Sample value:

  `tssacid=USER1234,tssadmingrp=acids,host=topsecret1,o=mycompany,c=com`

- ObjectClass ←→ objectClass

  The `objectClass` attribute (multi-valued) on the Top Secret system. Select the **Ignore case sensitivity** check box.

  Sample value:

`TSSACID`

- StructuralObjectClass ← vrtStructuralObjectClass

    `vrtStructuralObjectClass` on the Top Secret system defines the single object class for the object type. Select the **Ignore case sensitivity** check box.

    Sample value:

    `TSSACID`

- UID_LDPDomain ← vrtIdentDomain

    Create a fixed-value property variable on the Top Secret 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:

    `TOPSECRET1`

- 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 Top Secret side. Select the **Ignore case sensitivity** check box.

    Sample value:

    `tssadmingrp=acids,host=topsecret1,o=mycompany,c=com`

- BusinessCategory ←→ Department

    The `Department` attribute defines the Top Secret department assigned to the user. Select the **Ignore case sensitivity** check box.

    Sample value:

    `TSSDEPT1`

- Description ←→ name

    The `name` attribute contains a description for the user. Select the **Ignore case sensitivity** check box.

    Sample value:

```
TEST USER
```

- vrtRDN → vrtEntryRDN

Create a new variable on the One Identity Manager side of type **Script Property** with the name `vrtRDN` and a data type of **String**. In the **Scripts** section, enter one of the following scripts in the **Read script** section, depending on whether your project is configured for C# or Visual Basic.

C# Script:

```
references VI.TSUtils.dll;

return (VI.TargetSystem.Base.Utils.LDAP.RDN.Create("cn", useOldValues ?
$cn[o]$ : $cn$).ToString()).Replace("cn=","tssacid=");
```

VB Script:

```
References VI.TSUtils.dll

Imports VI.TargetSystem.Base.Utils.LDAP

Dim name as String = ""

If useOldValues Then

name = $cn[o]$

Else

name = $cn$

End If

return RDN.Create("cn",name).ToString().Replace("cn=","tssacid=")
```

Then map `vrtRDN` to `vrtEntryRDN` on the Top Secret side.

Sample value:

```
tssacid=USER1234
```

- userPassword → userPassword

Used to change a user's password in Top Secret. 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 Top Secret user attributes on page 9
- Object matching rules on page 12

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 Top Secret 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. Do not mark this rule as case-sensitive. Leave the check box cleared.

Sample value:

`tssacid=USER1234,tssadmingrp=acids,host=topsecret1,o=mycompany,c=com`

Related topics

- Mandatory Top Secret user attributes on page 9
- Property mapping rules on page 9

Group mapping information

This section shows a possible mapping between a group in Top Secret and the standard One Identity Manager database table called `LDAPGroup`.

- Set up a new mapping from `LDAPGroup(all)` to `tssgroup(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 Top Secret group attributes on page 13
- Property mapping rules on page 13
- Object matching rules on page 16
- Synchronizing Top Secret group members on page 17

Mandatory Top Secret group attributes

When creating a group in the Top Secret database, the following LDAP attributes must be defined:

- objectclass
- tssgroup
- name
- Department
- User-Type

Related topics

Property mapping rules

- CanonicalName ← vrtEntryCanonicalName

  `vrtEntryCanonicalName` is a virtual property, set to the canonical name of the object in the connector. Select the **Ignore case sensitivity** check box.

  Sample value:

  `COM/MYCOMPANY/TOPSECRET1/GROUPS/GROUP123`

- cn ←→ tssgroup

  On the Top Secret system, `tssgroup` is the group ID. Select the **Ignore case sensitivity** check box.

  Sample value:

  `GROUP123`

- DistinguishedName ← vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector.

  Sample value:

  `tssgroup=GROUP123,tssadmingrp=groups,host=topsecret1,o=mycompany,c=com`

- ObjectClass ←→ objectClass

  The `objectClass` attribute (multi-valued) on the Top Secret system. Select the **Ignore case sensitivity** check box.

  Sample value:

  `TSSGROUP`

- StructuralObjectClass ← vrtStructuralObjectClass

  `vrtStructuralObjectClass` on the Top Secret system defines the single object class for the object type. Select the **Ignore case sensitivity** check box.

  Sample value:

  `TSSGROUP`

- UID_LDPDomain ← vrtIdentDomain

  Create a fixed-value property variable on the Top Secret side called`vrtIdentDomain` that is set to the value $IdentDomain$. Map this to `UID_LDPDomain`. This causes 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. Enable **Handle failure to resolve as error**.

  5. To close the Property Mapping Rule Conflict Wizard, click **OK**.

  Sample value:

  `TOPSECRET1`

- vrtParentDN → vrtEntryParentDN

  Create a virtual attribute on the One Identity Manager side equal to a fixed string representing the parent DN for the object that is being manipulated. Select the **Ignore case sensitivity** check box.

  Sample value:

  `tssadmingrp=groups,host=topsecret1,o=mycompany,c=com`

- vrtRDN → vrtEntryRDN

  Create a new variable on the One Identity Manager side of type **Script Property** with the name `vrtRDN` and a data type of **String**. In the **Scripts** section, enter one of the following scripts in the **Read script** section, depending on whether your project is configured for C# or Visual Basic.

  C# Script:

  ```
  references VI.TSUtils.dll;

  return (VI.TargetSystem.Base.Utils.LDAP.RDN.Create("cn", useOldValues ?
  $cn[o]$ : $cn$).ToString()).Replace("cn=","tssgroup=");
  ```

  VB Script:

  ```
  References VI.TSUtils.dll
  ```

```
Imports VI.TargetSystem.Base.Utils.LDAP

Dim name as String = ""

If useOldValues Then

name = $cn[o]$

Else

name = $cn$

End If

return RDN.Create("cn",name).ToString().Replace("cn=","tssgroup=")
```

Then map `vrtRDN` to `vrtEntryRDN` on the Top Secret side.

Sample value:

`tssgroup=GROUP123`

- Description ← → name

The `name` attribute contains a description for the group. Select the **Ignore case sensitivity** check box.

Sample value:

`TEST GROUP`

- UID_LDAPContainer ← vrtEmpty

This is a workaround needed to support group mappings. Create a new fixed-value variable on the Top Secret side of type **String** with no value called `vrtEmpty`. This is mapped 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 ← → uniqueMember

This mapping is used to synchronize group membership information.

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 the following M:N schema types:

   a. Add an entry for `LDAPAccountInLDAPGroup`. Set the left box to `UID_LDAPGroup` and the right box to `UID_LDAPAccount`. Set the **Primary Key Property** to `DistinguishedName`.

   b. Add an entry for `LDAPGroupInLDAPGroup`. Set the left box to `UID_LDAPGroupChild` and the right box to `UID_LDAPGroupParent`. 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 Top Secret schema property to `uniqueMember`.

- vrtType → User-Type

Create a new fixed-value property on theOne Identity Manager side of type **String** with the value `GROUP`. Call the property `vrtType`. Map this to `User-Type` on the Top Secret side. Select the **Ignore case sensitivity** check box.

- SeeAlso ←→ Department

The `Department` attribute defines the Top Secret department assigned to the group. A suitable string attribute on the One Identity Manager side to store this value is `SeeAlso`. Select the **Ignore case sensitivity** check box.

Sample value:

TSSDEPT1

Related topics

- Mandatory Top Secret group attributes on page 13
- Object matching rules on page 16

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 Top Secret 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:

tssgroup=GROUP123,tssadmingrp=groups,host=topsecret1,o=mycompany,c=com

Related topics

- Mandatory Top Secret group attributes on page 13
- Property mapping rules on page 13

Synchronizing Top Secret group members

The members of a Top Secret group can be found in the group's `uniqueMember` attribute. This is a multi-valued attribute that contains a list of all group members (`tssacids`). The CA LDAP Server does not allow this attribute to be updated directly, but it can be updated via the connector. When the connector receives a request to update a group's `uniqueMember` attribute, it performs all necessary LDAP calls behind the scenes to synchronize group members.

How the connector performs group member synchronization

When the connector receives a request to update a group's `uniqueMember` attribute, it first performs an LDAP search to find out what the group's current `uniqueMember` attribute contains. It then compares the attribute with the supplied update and creates a list of users that need to be added or deleted in order to perform the synchronization.

For each user to be added, the connector sends an LDAP modify request for the user (`tssacid`) object to add the group via the user's `groups` attribute. This adds the user to the group, and the CA LDAP Server then automatically updates the group's `uniqueMember` attribute to include the new user.

Similarly, for each user deleted, the connector sends an LDAP modify request for the user (`tssacid`) object to delete the group via the user's `groups` attribute. This removes the user from the group and the CA LDAP Server then automatically updates the group's `uniqueMember` attribute to remove the user.

Once this is done, the `uniqueMember` attribute for the group will match the value that was passed into the connector, effectively synchronizing the two values. This approach is used in the sample group mapping in this document.

Related topics

- Group mapping information on page 12

Profile mapping information

This section shows a possible mapping between a profile in Top Secret and the standard One Identity Manager database table called `LDAPGroup`.

- Set up a new mapping from `LDAPGroup(all)` to `tssprofile(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 Top Secret profile attributes

When creating a profile in the Top Secret database, the following LDAP attributes must be defined:

- objectclass
- tssprofile
- name
- Department
- User-Type

Related topics

Property mapping rules

- CanonicalName ← vrtEntryCanonicalName

  `vrtEntryCanonicalName` is a virtual property, set to the canonical name of the object in the connector. Select the **Ignore case sensitivity** check box.

  Sample value:

  `COM/MYCOMPANY/TOPSECRET1/PROFILES/PROFILE1`

- cn ←→ tssprofile

  On the Top Secret system, `tssprofile` is the profile ID. Select the **Ignore case sensitivity** check box.

  Sample value:

  `PROFILE1`

- DistinguishedName ← vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector.

  Sample value:

```
tssprofile=PROFILE1,tssadmingrp=profiles,host=topsecret1,o=mycompany,c=com
```

- ObjectClass ←→ objectClass

The `objectClass` attribute (multi-valued) on the Top Secret system. Select the **Ignore case sensitivity** check box.

Sample value:

`TSSPROFILE`

- StructuralObjectClass ← vrtStructuralObjectClass

`vrtStructuralObjectClass` on the Top Secret system defines the single object class for the object type. Select the **Ignore case sensitivity** check box.

Sample value:

`TSSPROFILE`

- UID_LDPDomain ← vrtIdentDomain

Create a fixed-value property variable on the Top Secret side called `vrtIdentDomain` that is set to the value $IdentDomain$. Map this to `UID_LDPDomain`. This causes 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. Enable **Handle failure to resolve as error**.
5. To close the Property Mapping Rule Conflict Wizard, click **OK**.

Sample value:

`TOPSECRET1`

- vrtParentDN → vrtEntryParentDN

Create a virtual attribute on the One Identity Manager side equal to a fixed string representing the parent DN for the object that is being manipulated. Select the **Ignore case sensitivity** check box.

Sample value:

`tssadmingrp=profiles,host=topsecret1,o=mycompany,c=com`

- vrtRDN → vrtEntryRDN

Create a new variable on the One Identity Manager side of type **Script Property** with the name `vrtRDN` and a data type of **String**. In the **Scripts** section, enter one of the following scripts in the **Read script** section, depending on whether your project is configured for C# or Visual Basic.

C# Script:

```
references VI.TSUtils.dll;

return (VI.TargetSystem.Base.Utils.LDAP.RDN.Create("cn", useOldValues ?
$cn[o]$ : $cn$).ToString()).Replace("cn=","tssprofile=");
```

VB Script:

```
References VI.TSUtils.dll

Imports VI.TargetSystem.Base.Utils.LDAP

Dim name as String = ""

If useOldValues Then

name = $cn[o]$

Else

name = $cn$

End If

return RDN.Create("cn",name).ToString().Replace("cn=","tssprofile=")
```

Then map `vrtRDN` to `vrtEntryRDN` on the Top Secret side.

Sample value:

`tssprofile=PROFILE1`

- Description ← → name

The `name` attribute contains a description for the profile. Select the **Ignore case sensitivity** check box.

Sample value:

`TEST PROFILE`

- UID_LDAPContainer ← vrtEmpty

This is a workaround needed to support membership mappings. Create a new fixed-value variable on the Top Secret side of type**String** with no value called `vrtEmpty`. This is mapped 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 ← → uniqueMember

This mapping is used to synchronize profile membership information.

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 the following M:N schema types:

a. Add an entry for `LDAPAccountInLDAPGroup`. Set the left box to `UID_LDAPGroup` and the right box to `UID_LDAPAccount`. Set the **Primary Key Property** to `DistinguishedName`.

b. Add an entry for `LDAPGroupInLDAPGroup`. Set the left box to `UID_LDAPGroupChild` and the right box to `UID_LDAPGroupParent`. 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 Top Secret schema property to `uniqueMember`.

- vrtType → User-Type

    Create a new fixed-value property on theOne Identity Manager side of type **String** with the value `PROFILE`. Call the property `vrtType`. Map this to `User-Type` on the Top Secret side. Select the **Ignore case sensitivity** check box.

- SeeAlso ←→ Department

    The `Department` attribute defines the Top Secret department assigned to the profile. A suitable string attribute on the One Identity Manager side to store this value is `SeeAlso`. Select the **Ignore case sensitivity** check box.

    Sample value:

    TSSDEPT1

Related topics

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 Top Secret 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:

    tssprofile=PROFILE1,tssadmingrp=profiles,host=topsecret1,o=mycompany,c=com

Related topics

Synchronizing Top Secret profile memberships

The members of a Top Secret profile can be found in the profile's `uniqueMember` attribute. This is a multi-valued attribute that contains a list of all profile members (`tssacids`). The CA LDAP Server does not allow this attribute to be updated directly, but it can be updated via the connector. When the connector receives a request to update a profile's `uniqueMember` attribute, it performs all necessary LDAP calls behind the scenes to synchronize profile members.

How the connector performs profile member synchronization

When the connector receives a request to update a profile's `uniqueMember` attribute, it first performs an LDAP search to find out what the profile's current `uniqueMember` attribute contains. It then compares the attribute with the supplied update and creates a list of users that need to be added or deleted in order to perform the synchronization.

For each user to be added, the connector sends an LDAP modify request for the user (`tssacid`) object to add the group via the user's `groups` attribute. This adds the user to the profile, and the CA LDAP Server then automatically updates the profile's `uniqueMember` attribute to include the new user.

Similarly, for each user deleted, the connector sends an LDAP modify request for the user (`tssacid`) object to delete the profile via the user's `groups` attribute. This removes the user from the profile and the CA LDAP Server then automatically updates the profile's `uniqueMember` attribute to remove the user.

Once this is done, the `uniqueMember` attribute for the profile will match the value that was passed into the connector, effectively synchronizing the two values. This approach is used in the sample profile mapping in this document.

Related topics

Top Secret attributes

The following table lists the Top Secret user, group and profile attributes that are made available to One Identity Manager by the Top Secret LDAP connector.

Table 3: List of Top Secret user, groups, and profile attributes

Attribute name
Acid-All
Acid-Audit
Acid-Create
Acid-Defnode
Acid-Info
Acid-Maintain
AcidMatchlim
Acid-Report
Acid-XAuth
AdminAcid
AdministeringAcid
AdministeringDate
AdministeringSMFid
AdministeringTime
AdminListData
AdminMisc1
AdminMisc2
AdminMisc3

Attribute name
AdminMisc4
AdminMisc5
AdminMisc6
AdminMisc7
AdminMisc8
AdminMisc9
AdminSuspend
AllowLocalIPWPhrase
APPC-Sysout-AcctNum
APPC-Sysout-Addr1
APPC-Sysout-Addr2
APPC-Sysout-Addr3
APPC-Sysout-Addr4
APPC-Sysout-Bldg
APPC-Sysout-Dept
APPC-Sysout-Name
APPC-Sysout-Room
Audit-Attr
AuthoritytoGraphicMonitorFacility
AutoOwnDatasetHLQ
Available-Cmds-per-Facility
Bypass-Dsn-Check
Bypass-Job-Submission-Check
Bypass-Limited-Cmd-Facility-Check
Bypass-Minidisklink-Check
Bypass-Resource-Check
Bypass-Volume-Check
CICS-Auto-Transaction
CICS-Oper-Class

Attribute name
CICS-Oper-Identification
CICS-Oper-Property
CICS-Security-Key
CICS-Time-Out
Console-Auth
ConsoleIdentifier
Created-Date
Created-Time
DCESegmentFlags
Default-Remote-Nodes
Department
Division
DUF-Extract
DUF-Update
EIMProfile
EncryptedKey
EncryptionType
ExpireNow
ExpirePassPhraseNow
Expires
For-Number-of-Days
Globally-Admin-Profile
groupmemberOf
Groups
HomeCell
IMS-Multi-Sys-Coupling
InitialCommand
Installation-Data
InstallationExitSuspended

Attribute name
KerberosName
Language-Pref
Last-Access-Count
Last-Accessed-From-CPU
LastLoginDTS
Last-Used-Date
Last-Used-Facility
Last-Used-Time
LDAP-Destinations
LDAPUser
LinuxEntries
LinuxName
ListData-Acids
ListData-Admin
ListData-All
ListData-Basic
ListData-Cics
ListData-Instdata
ListData-LCF
ListData-Names
ListData-Password
ListData-Profile
ListData-PWVIEW
ListData-Resource
ListData-SessKey
ListData-SMS
ListData-Source
ListData-Tso
ListData-WorkAttr

Attribute name
ListData-XAuth
ListofScopeClasses
LotusName
M1-All
M1-Instdata
M1-LCF
M1-LTime
M1-Noats
M1-RDT
M1-Suspend
M1-TSSSim
M1-User
M2-All
M2-APPCLU
M2-DLF
M2-SMS
M2-Target
M2-TSO
M2-WorkAttr
M3-ALL
M3-SDT
M4-ALL
M4-CERTAUTH
M4-CERTCHEK
M4-CERTEXPO
M4-CERTGEN
M4-CERTLIST
M4-CERTSITE
M4-CERTUSER

Attribute name
M4-KERBUSER
M5-ALL
M5-DCLADMIN
M5-DCLIST
M5-MLSADMIN
M8-All
M8-LISTAPLU
M8-ListRDT
M8-ListSDT
M8-ListSTC
M8-MCS
M8-NOMVSDF
M8-PWMAINT
M8-Remasusp
M9-All
M9-Bypass
M9-Console
M9-Generic
M9-Global
M9-Mastfac
M9-Mode
M9-STC
M9-Trace
Master-Facility
MaxAddrSpaceSize
MaxCPUTime
MaxDataSpacePages
MaxFilesPerProcess
Maximum-Non-Shared-Memory-Space

Attribute name
Maximum-Shared-Memory-Space
MaxProcess
MaxPthreadsCreated
MaxTicketLife
MCS-Alternate-Grp
MCS-Authirized-Cmds
MCS-Auto-Cmds
MCS-Cmd-Target-System
MCS-Delete-Oper-Cmds
MCS-Display-Format
MCS-Keyword
MCS-Log-Cmds
MCS-Migration-ID
MCS-Monitor
MCS-Msgs-Queue-Storage
MCS-Msgs-Received
MCS-Receive-ConsoledZero-Message
MCS-Receive-HardCopy-Messages
MCS-Receive-Unknown-ConsoleID-Messages
MCS-Routing-Code
MCS-Undelivered-Msgs
memberOf
MLSDfltSecLabel
MLSSecLabels
Modified-Date
Modified-Time
Multi-Region-Optimized-Signon
name
No-Automatic-Dsn-Protection

Attribute name

No-Automatic-Terminal-Signon
No-OMVS-Default-User
No-Password-Chg
NovellName
No-Vthresh-Suspend
objectClass
OMVS-Dflt-Group
OMVS-Group-ID
OMVS-Home-Subdir
OMVS-Program
OMVS-User-ID
Operating-Mode
PassPhrase
PasswordSuspended
Physical-Security-Key
Policy-Profiles
PrincipalNameofUser
Profile-After
Profile-Before
Profile-First
Profile-Names
Profile-Until-Date
ProgramIdentifierinOtherDomain
PWPhrase
ReceiveUnsolicitedMessages
Refresh
RestrictedAccess
Restricted-Cmds-per-Facility
SecurityCheckIdentifier

Attribute name
SMS-Application-ID
SMS-Data-Class
SMS-Mgmt-Class
SMS-Storage-Class
Source-Reader
StringFormofUUID
Target-Notes-for-Cmds
Terminal-Lock-Time
Time-Zone
Trace-ACID-Activity
TSO-Hold-Class
TSO-Job-Class
TSO-Logon-Account
TSO-Logon-Command
TSO-Logon-Proc
TSO-Max-Region-Size
TSO-Message-Class
TSO-Multiple-Passwords
TSO-Options
TSO-Output-Destination
TSO-Performance-Grp
TSO-Region-Size
TSO-Sysout-Class
TSO-Unit
TSO-User-Data
tssacid
tssgroup
tssprofile
UIDGIDRange

Attribute name
uniqueMember
Until-Date
User-Access
UserDefFields
UserHomeCellUUID
userPassword
userPassword-Expire
userPassword-Interval
userPasswordPhraseInterval
User-Suspend
User-Type
Using-Acid
ViolationsSuspended
VSE-IES-Dflt-Usercat
VSE-IES-Fld1
VSE-IES-Fld2
VSE-IES-Init
VSE-IES-Synm-ModelID
VES-IES-Type
Wait-for-Synchronous-Processing
Zone

About us

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