



One Identity Manager 8.0.4

LDAP Connector for CA Top Secret Reference Guide

Copyright 2019 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 indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Initializing and Configuring the LDAP Connector for CA Top Secret	4
Pre-requisites	4
Platform Support	5
Operating Constraints	5
How to initialize and configure the Top Secret LDAP connector	5
System Variables	7
Domain Filter Setting	7
User Mapping Information	8
Mandatory Top Secret User Attributes	9
Property Mapping Rules	9
Object Matching Rules	11
Group Mapping Information	12
Mandatory Top Secret Group Attributes	12
Property Mapping Rules	13
Object Matching Rules	15
Synchronizing Top Secret Group Members	16
Appendix: Top Secret Attributes	17
About us	22
Contacting us	22
Technical support resources	22

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 enables a 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

- [Pre-requisites](#) on page 4
- [Platform Support](#) on page 5
- [Operating Constraints](#) on page 5
- [How to initialize and configure the Top Secret LDAP connector](#) on page 5
- [Domain Filter Setting](#) on page 7
- [System Variables](#) on page 7
- [User Mapping Information](#) on page 8
- [Group Mapping Information](#) on page 12
- [Appendix: Top Secret Attributes](#) on page 17

Pre-requisites

- 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 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 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 9.0 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. Select **Top Secret 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. 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.
9. The schema will be loaded from the Top Secret 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 the **Use partitioned search** check box.
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 Top Secret schema into your One Identity Manager system. 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
- [Group Mapping Information](#) on page 12

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 Top Secret domain e.g. TOPSECRET1
UserLocation	Parent DN of your Top Secret user container, e.g. tssad-mingrp=acids,host=topsecret1,o=mycompany,c=com
GroupLocation	Parent DN of your Top Secret group container, e.g. tssad-mingrp=groups,host=topsecret1,o=mycompany,c=com

Related Topics

- [Domain Filter Setting](#) on page 7
- [Property Mapping Rules](#) on page 9
- [Property Mapping Rules](#) on page 13

Domain Filter Setting

A domain filter needs to be created to identify information that has been retrieved from the Top Secret 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 Top Secret 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. Top Secret Domain
Distinguished name	Distinguished name of the domain e.g. host=topsecret1, - ,o=mycompany,c=com
Domain	Domain name e.g. 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 the category **Configuration | One Identity Manager connection**.
 - b. Select the **Scope view** and click **Edit scope**.
 - c. Select the object type LDAPDomain 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 Top Secret and the standard One Identity Manager database table called LDAPAccount.

- Set up a new mapping from LDAPAccount(a11) to tssacid(a11).

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 11

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](#) 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/TOPSECRET1/ACIDS/USER1234
- cn ←→ tssacid
On the Top Secret system, tssacid 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:
tssacid=USER1234,tssadmingrp=acids,host=topsecret1,o=mycompany,c=com
- ObjectClass ←→ objectClass
The objectClass attribute (multi-valued) on the Top Secret system. Activate the check box **Ignore case sensitivity**.
Sample value:
TSSACID

- StructuralObjectClass ← vrtStructuralObjectClass

vrtStructuralObjectClass on the Top Secret system defines the single object class for the object type.

Sample value:

TSSACID

- UID_LDPPDomain ← 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_LDPPDomain. 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:

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.

Sample value:

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

- vrtDep → Department

Create a new fixed value property on the One Identity Manager side of type "String" with the name of your department. Call the property vrtDept. Map this to Department on the Top Secret side.

- vrtName → name

Create a new variable on the One Identity Manager side of type "Format Defined Property" with name vrtName. Set its value to name=%CN%. Then map this to name on the Top Secret side.

Sample value:

name=USER123

- vrtRDN → vrtEntryRDN

Create a new variable on the One Identity Manager side of type "Format Defined Property" with name vrtRDN. Set its value to %CN%. Then map this to vrtEntryRDN on the Top Secret side.

Sample value:

USER123

- 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 on **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 TopSecret side of type "String" with no value called vrtEmpty. Map this to UID_LDAPContainer. This generates a property mapping rule conflict.

To solve 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 Top Secret User Attributes](#) on page 9
- [System Variables](#) on page 7
- [Object Matching Rules](#) on page 11
- Sample User Mapping

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 unchecked).

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
- [Sample User Mapping](#)

Group Mapping Information

This section shows a possible mapping between a user account 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 12
- [Property Mapping Rules](#) on page 13
- [Object Matching Rules](#) on page 15

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](#) on page 13
- [Object Matching Rules](#) on page 15

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/TOPSECRET1/GROUPS/GROUP123
- cn ←→ tssgroup
On the Top Secret system, tssgroup is the group ID.
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. Activate the check box **Ignore case sensitivity**.
Sample value:
TSSGROUP
- StructuralObjectClass ← vrtStructuralObjectClass
vrtStructuralObjectClass on the Top Secret system defines the single object class for the object type.
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 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:

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.

Sample value:

tssadmingrp=groups,host=topsecret1,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 %CN%. Then map this to vrtEntryRDN on the Top Secret side.

Sample value:

GROUP123

- vrtName → name

Create a new variable on the One Identity Manager side of type "Format Defined Property" with name vrtName. Set its value to name=%CN%. Then map this to name on the Top Secret side.

Sample value:

name=GROUP123

- 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 solve 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 ↔ memberOf
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 name vrtMember. Activate the boxes to **Ignore case** and **Enable relative component handling**.
 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 memberOf.
- vrtType → User-Type
Create a new fixed value property on the One Identity Manager side of type "String" with the value GROUP. Call the property vrtType. Map this to User-Type on the Top Secret side.
 - vrtDept → Department
Create a new fixed value property on the One Identity Manager side of type "String" with the name of your department. Call the property vrtDept. Map this to Department on the Top Secret side.


Related Topics

- [Mandatory Top Secret Group Attributes](#) on page 12
- [Object Matching Rules](#) on page 15
- Sample Group Mapping

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 12
- [Property Mapping Rules](#) on page 13
- [Sample Group Mapping](#)

Synchronizing Top Secret Group Members

The members of a Top Secret group can be found in the group attribute called `memberOf`. This is a multi-valued attribute that contains a list of all the group's 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 `memberOf` attribute, it performs all the necessary LDAP calls behind the scenes to perform the synchronization of the group members.

How the Connector Performs Group Member Synchronization

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

For each user to be added, the connector creates an LDAP object of type `tssacidlist` for the group that contains the new user's name. This adds the user to the group and the CA LDAP Server then automatically updates the group's `memberOf` attribute to include the new user.

Similarly, for each user to be deleted, the connector removes the LDAP object of type `tssacidlist` for the group associated with the user to be deleted. This removes the user from the group and the CA LDAP Server then automatically updates the group's `memberOf` attribute to remove the user.

Once all this has been done, the `memberOf` attribute for the group will then match the value that was passed in to the connector, effectively synchronizing the two values. This approach has been used in the sample group mapping that appears in this document.

Related Topics

- [Group Mapping Information](#) on page 12

Appendix: Top Secret Attributes

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

Table 3: List of Top Secret User and Groups Attributes

Attribute Name
AcidRecordSize
AdminAcid
AdminListData
AdminMisc1
AdminMisc2
AdminMisc3
AdminMisc4
AdminMisc5
AdminMisc6
AdminMisc7
AdminMisc8
AdminMisc9
AdminSuspend
APPC-Sysout-AcctNum
APPC-Sysout-Addr1
APPC-Sysout-Addr2
APPC-Sysout-Addr3
APPC-Sysout-Addr4

Attribute Name

APPC-Sysout-Bldg

APPC-Sysout-Dept

APPC-Sysout-Name

APPC-Sysout-Room

Audit-Attr

Bypass-Dsn-Check

Bypass-Job-Submission-Check

Bypass-Limited-Cmd-Facility-Check

Bypass-Minidisklink-Check

Bypass-Resource-Check

Bypass-Volume-Check

CICS-Oper-Class

CICS-Oper-Identification

CICS-Oper-Priority

CICS-Security-Key

Console-Auth

Created-Date

Default-Remote-Nodes

Department

Division

DUF-Extract

DUF-Update

Expires

For-Number-of-Days

Globally-Admin-Profile

groupmemberOf

IMS-Multi-Sys-Coupling

Installation-Data

InstallationExitSuspended

Attribute Name

Language-Pref

Last-Access-Count

Last-Accessed-From-CPU

Last-Used-Date

Last-Used-Facility

Last-Used-Time

LDAP-Destinations

LDAPUser

LinuxName

LotusName

Master-Facility

MaxAddrSpaceSize

MaxCPUTime

MaxDataSpacePages

MaxFilesPerProcess

MaxProcesses

MaxPthreadsCreated

MCS-Alternate-Grp

MCS-Authorized-Cmds

MCS-Auto-Cmds

MCS-Cmd-Target-System

MCS-Delete-Oper-Cmds

MCS-Display-Format

MCS-Keywords

MCS-Log-Cmds

MCS-Migration-ID

MCS-Monitor

MCS-Msgs-Queue-Storage

MCS-Msgs-Received

Attribute Name

MCS-Routing-Code

MCS-Undelivered-Msgs

memberOf

Modified-Date

Modified-Time

Multi-Region-Optimized-Signon

name

No-Automatic-Dsn-Protection

No-Automatic-Terminal-Signon

No-OMVS-Default-User

NovellName

No-Vthresh-Suspend

OMVS-Dflt-Group

OMVS-Group-ID

OMVS-Home-Subdir

OMVS-Program

OMVS-User-ID

Operating-Mode

PasswordSuspended

Physical-Security-Key

SMS-Application-ID

SMS-Data-Class

SMS-Mgmt-Class

SMS-Storage-Class

Source-Reader

Target-Nodes-for-Cmds

Terminal-Lock-Time

Time-Zone

Trace-ACID-Activity

Attribute Name

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

Until-Date

Until-Access

userPassword

userPassword-Expire

userPassword-Interval

User-Suspend

User-Type

Using-Acid

ViolationSuspended

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 or other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

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